

## Chapter 5

# Defend the Network and Infrastructure

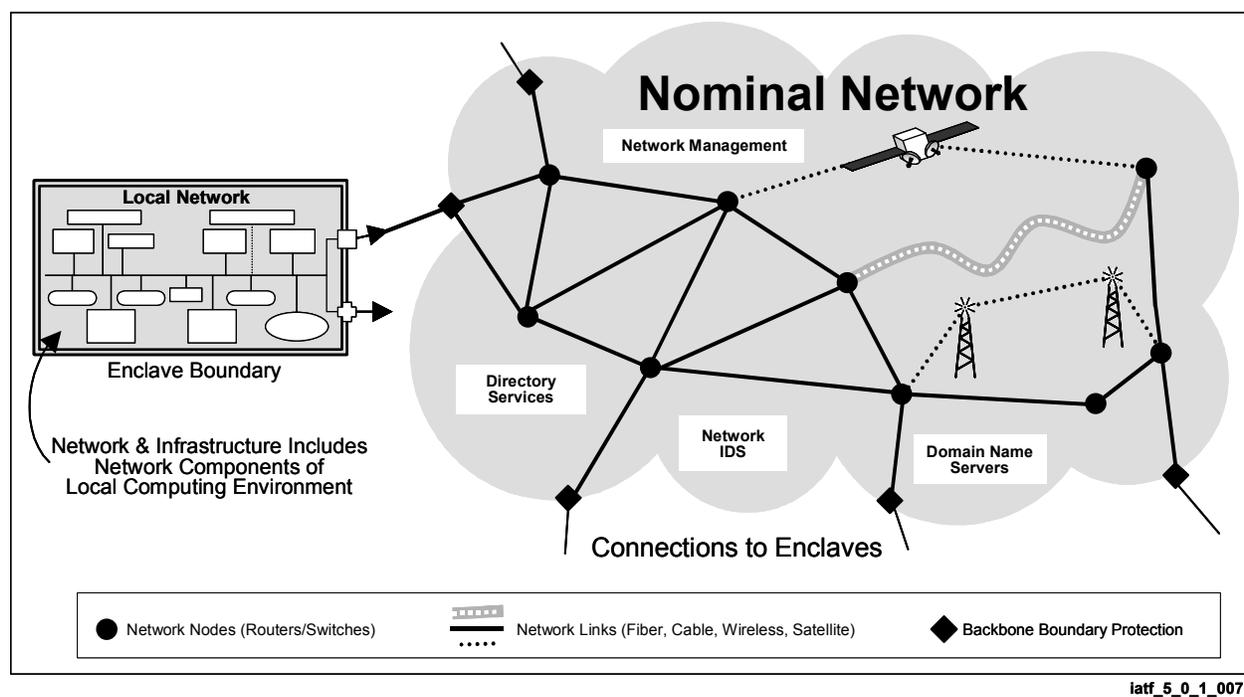
---

Networks provide a transport mechanism for user traffic and for the availability of user information. Networks and their supporting infrastructures must protect against denial-of-service attacks that could prevent user information from being transmitted. The supporting infrastructure consists of the management systems and any other systems that support network operation.

The network supports three distinct types of traffic: user, control, and management. User traffic is simply the information that users are transmitting over the network. Networks have the responsibility to provide separation of user traffic. Isolation of individual user connections must be maintained to ensure reliable delivery of information. Additionally, confidentiality services *may* be provided by the network, either by government encryptors, for classified traffic, or through commercial encryption embedded in network components, for unclassified traffic.

Control traffic is any information transferred between network components that is necessary for establishing user connections. Control traffic provided by a signaling protocol, such as Signaling System 7 (SS7), includes addressing, routing information, and signaling. Proper addressing by the network infrastructure is essential for user traffic to be directed to the intended destination. Routing information must be protected to ensure that the user information will be properly transferred and that the path that user information takes is not manipulated. Similarly, signaling must be protected to ensure that user connections are established properly.

The third type of network traffic, management traffic, is any information that configures network components or information initiated from a network component that informs the network infrastructure on the status of the network component. Management protocols include Simple Network Management Protocol (SNMP), Common Management Information Protocol (CMIP), Hypertext Transfer Protocol (HTTP), rlogin and Telnet command line interfaces, or other proprietary management protocols. Network management traffic protection is essential to ensuring that network components are not modified by unauthorized users. If management of a network component is compromised, that component can be configured to perform any function the attacker wishes. Simply being able to view configuration information on a network component may give an attacker knowledge of network connections, addressing schemes, or other potentially sensitive information. Figure 5-1 illustrates the network and infrastructure in the high level Defense Information Infrastructure (DII) context. Some of the networks illustrated are controlled by government organizations, while others are controlled by commercial entities such as the public switched telephone network (PSTN) and the Internet.



**Figure 5-1. Defend the Network and Infrastructure**

Today, commercial carriers provide over 95 percent of all the transmission service for all communications of the Federal Government and industry. In addition, most of the large civil government networks provided by General Services Administration (GSA), Federal Aviation Administration (FAA), Department of Transportation, etc., outsource the management of their networks. In light of this reliance on commercial control networks, all organizations should adopt a two-pronged approach—starting at the highest level—to defend their networks. First, organizations should ensure that they have established clear service level agreements (SLA) with their commercial carrier that specify metrics for reliability, priority, and access control. Commercial carriers view network security as a business issue. Therefore, they will not simply add security features. For them, a business case must be made; the customer must ask for these services. Second, organizations should recognize that during transmission, their data may be essentially unprotected. It is incumbent upon the *owner* of the information to implement security services, such as encryption for confidentiality, at the user level. Historically, few organizations outside of the Department of Defense (DoD) and the Intelligence Community (IC)—have developed strategies and encrypted data sent over commercial lines. In the past few years, however, services such as Pretty Good Privacy (PGP) have grown in use by government and industry organizations.

The general information assurance (IA) strategy for defending the network and infrastructure is to use approved wide area networks (WAN) to transport classified data among and between DoD and IC elements when feasible, and then to use National Security Agency (NSA)-approved—e.g., Type 1—encryptors, in-line network encryptors (INE), or traditional bulk encryptors to protect classified data transported over networks. To protect sensitive data exchanged among unclassified local area networks (LAN), the strategy is to use commercial

solutions that satisfy published criteria; are validated by an approved, independent laboratory; are properly configured; and are accredited for use by an approval process such as the DoD Information Technology Security Certification and Accreditation Process (DITSCAP).

For voice networks, a number of strategies are in use. DoD's protection strategy is to use approved common user networks when available, or NSA-approved subscriber voice terminals otherwise. The strategy for DoD tactical networks is to use NSA-approved tactical radios, tactical subscriber terminals, or INEs to protect classified information transmissions. Law enforcement organizations use encrypted communications in the field, generally following National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) publications on encryption standards. Other civil agencies involved in tactical operations, such as responding to natural disasters, generally use commercial off-the-shelf (COTS) communications with no encryption. They are migrating to digital phones, which are less likely to be compromised. However, this move is motivated by market changes rather than any requirement to have more secure communications. The most critical requirements for emergency response functions are availability and reliability, not confidentiality.

To achieve interoperability between government and commercial networks, the strategy is to include denial-of-service protection measures in all SLAs for commercial leased network services. For DoD owned and operated networks, the strategy is to provide a number of measures to ensure network availability. These measures include mechanisms that ensure the positive control of network elements; Public Key Infrastructure (PKI)-enabled authentication and access control for remote management of all critical network elements; authentication and integrity protection for all network management transactions; and enclave boundary protection for centers that manage the control of DoD WANs.

The Defend the Network and Infrastructure chapter of the IATF consists of several sections. The Availability of Backbone Networks section considers data communications networks (e.g., Internet Protocol [IP] and asynchronous transfer mode [ATM]); and issues with secure network management. The Wireless section considers the security issues associated with cellular service, pagers, satellite systems, and wireless LANs. The System High Interconnections and Virtual Private Networks (VPN) section addresses secure connectivity between systems operating at the same sensitivity level via backbone networks. A future section dealing with secure voice transmission will cover voice over the PSTN, voice over Integrated Services Digital Network (ISDN), and voice over data networks. A future section on multiple security layers will address issues with using a single backbone to transmit information of the same classification level, but of varying compartments.

**UNCLASSIFIED**

Defend the Network and Infrastructure  
IATF Release 3.1 —September 2002

**This page intentionally left blank.**

## 5.1 Availability of Backbone Networks

Reliance on commercial providers of network services has been increasing, primarily owing to increased competition after the Telecommunications Act of 1996 and the exponential demand for bandwidth. While most private sector organizations traditionally relied on commercial providers for almost all of their network services, Government took a different view. Many government organizations, especially the Department of Defense (DoD) and the Intelligence Community (IC), held to the paradigm that they had to operate and maintain the entire communication system, including all of the long-haul communication transport systems.

With the move to more cost-effective commercial service providers, government organizations have had to join private sector organizations in seeking to influence the network security industry. The overall strategy for the public and private sector should be first, to educate—organizations should understand the different aspects of network security and determine their own requirements—and second, they should seek to participate in standards activities to influence standards, protocols, and operations.

This section of the framework focuses specifically on improving the availability<sup>1</sup> of the long-haul transport systems to meet the operational requirements even if the long-haul transport systems are under an information warfare attack.

### 5.1.1 Target Environment

This section of the framework focuses on backbone networks (BN). The most common examples of a commercial BN are the terrestrial-based voice systems and the Internet. In the DoD, the most common data BN is the Defense Information Systems Network (DISN). The framework looks to encompass a wider range of systems than data wide area networks (WAN) (including wireless systems, satellite systems, video teleconferencing systems, and voice systems). BNs hereafter refer to this entire range of communication systems.

Typically, BNs are known by a single name, such as the Internet or the DISN. However, these networks are constructed of a range of technologies and transport systems. Although the separations between BNs and other parts of the communication systems are neither simple nor clean, useful characteristics can be described in terms of a generalized model of a BN. We can decompose our model of the BN into nine focus areas:

- Network-to-network communication.
- Device-to-device communication.
- Device management and maintenance.
- User data interface.
- Remote operator-to-Network Management Center (NMC) communication.

---

<sup>1</sup> The backbone security service is limited to availability for two reasons. First, backbones may be acquired through commercial service provisioning thus restricting the acquisition office from dictating special security services. Second, the communication models used in today's systems dictate the other security services, such as confidentiality and data integrity, to be handled by the end system and not the backbone network.

## UNCLASSIFIED

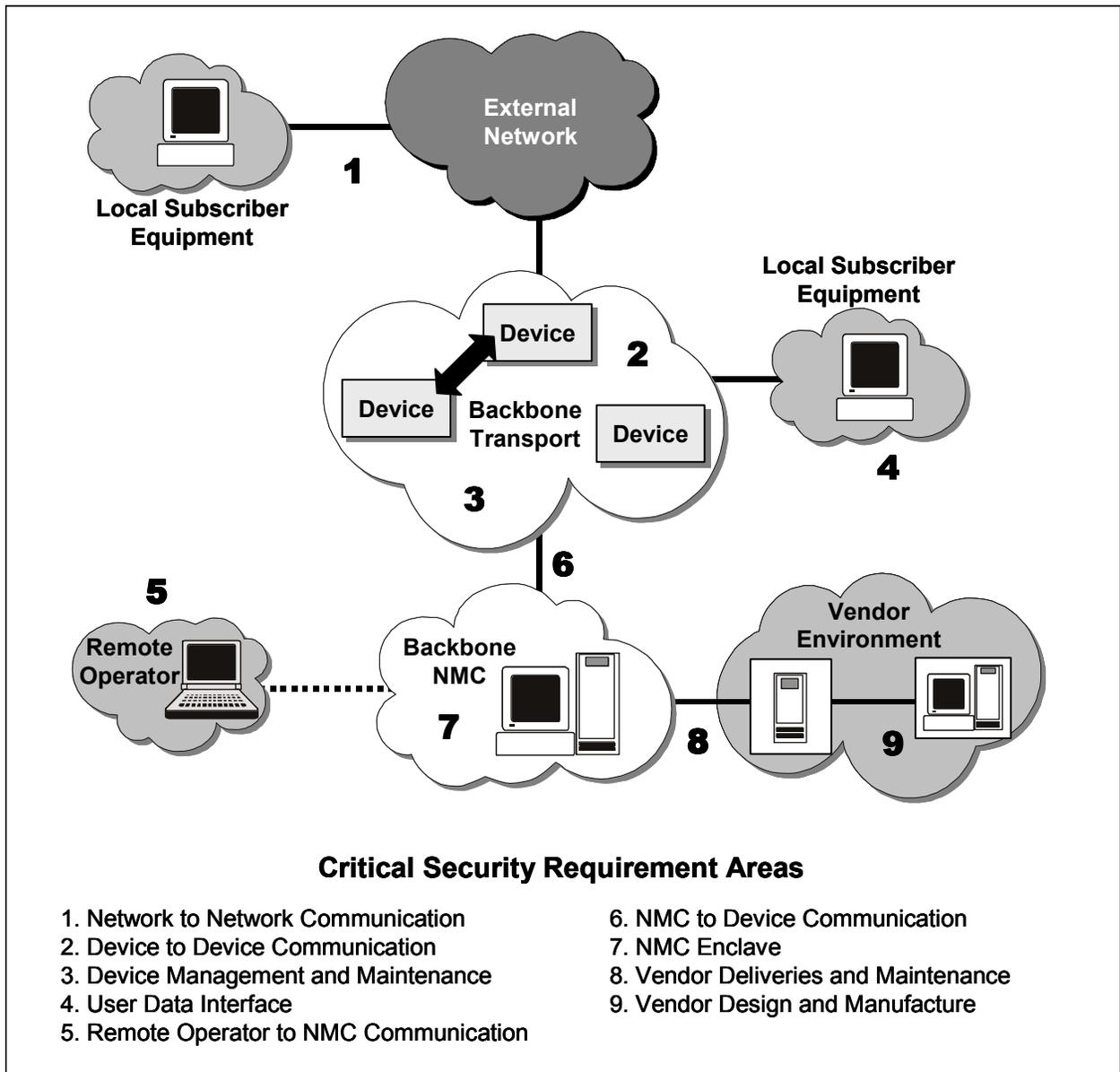
Availability of Backbone Networks  
IATF Release 3.1—September 2002

- NMC-to-device communication.
- NMC enclave.
- Vendor deliveries and maintenance.
- Vendor design and manufacture.

The availability of a BN is closely connected to the communications between networks, network devices such as routers and switches, and the network management's centers and the devices they manage. Additionally, the NMCs and network devices must be protected. We performed an Information Systems Security (INFOSEC) Information System Security Engineering (ISSE) analysis of the model components for five network cases. The remainder of this section presents the backbone availability model and security issues related to the analysis.

The following provides an expanded description of the nine backbone availability model components identified in the model depicted in Figure 5.1-1.

- 1) Network-to-Network Communication.** There are two classes of network traffic or data of concern here. One data class is the user traffic or user data that traverses this interface. The other data class, control traffic, is the communications required between the backbone transport devices and the external network devices. It is necessary to distinguish between two classes. Typically, the device-to-device communication is a well-defined protocol providing network-specific data necessary to transport the user data. The user data will be entering and exiting the backbone transport network. This is one of the BN boundary interfaces that allows the ISSE to define the inside and the outside of the BN.
- 2) Device-to-Device Communication.** This area considers the internal communications between devices that are components of the BN itself. Generally, BNs require continual information exchange of this management and control traffic among devices to provide optimum performance and to support on-line maintenance and troubleshooting.
- 3) Device Management and Maintenance.** This area focuses on configuration and parameter adjustments required to maintain the individual devices on the BN, the network management traffic. Typically, each device has a unique set of operational requirements and specifications that must be controlled by the NMC or maintenance personnel for that device to remain an active node on the network.
- 4) User Data Interface.** The user data interface is the means by which user data enters and exits the BN. This may occur at any connection supporting user connectivity including user networks represented by the Local Subscriber Environment (LSE) and other networks connected to user networks represented by the external network. These interfaces should be resistant to cyber attacks from the user connections.



iatf\_5\_1\_1\_0011

Figure 5.1-1. Backbone Availability Model

- 5) Remote Operator-to-NMC Communication.** The primary concern with this area is the operator's physical security, e.g., where the equipment, usually a laptop computer, is being used, and what protection is afforded to the equipment. In addition to those security concerns, there is the connection into the NMC and the type of security needed to protect it. When this area is needed to support operational requirements, it increases the complexity of analyzing the NMC, so perimeter security considerations regarding access to the NMC should be analyzed.
- 6) NMC-to-Device Communication.** Addressing this area allows analysis of the perimeters of the backbone transport and the NMC, recognizing the NMC requires

## UNCLASSIFIED

connectivity to the devices making up the backbone transport for all of the management operations. The connectivity may occur through in-band or out-of-band signaling using either primary or secondary channels. This provides opportunity to access the BN devices, and the NMC equipment and data, plus it exposes network management data.

- 7) **NMC Enclave.** The concern in this area stems from the concept that network management is critically important to the availability of the BN and should be operated separately from, what has been called in this section, user data. The management equipment and data require security protection from attack so they may successfully perform their mission, which is to manage the BN. Considering this as a local network environment will permit the ISSEs to take full advantage of virtually every other section of this framework document.
- 8) **Vendor Deliveries and Maintenance.** This area is more complex than Figure 5.1-1 depicts. The NMC may receive equipment or software to be prepared for installation in the backbone transport. It is possible that the vendor will be called on to provide product service and maintenance directly to the backbone transport devices. The NMC may receive the information from the vendor either indirectly, e.g., by the postal system, or directly on line through a network connection. The ability to ensure the validity of the information and equipment received plays an important role in the availability of the BN.
- 9) **Vendor Design and Manufacture.** This area covers the entire manufacturing process from development to production to delivery of the end item, whether it is a device or software. Security must be applied over all of this so that what “comes out of the box” can be trusted to operate properly. Security must also be designed into the product so that many of the security requirements raised in the other eight areas can be achieved.

Now that the BN focus areas have been described, it is useful to return and discuss its generalized use and operations. One of the general characteristics of the BN is that it has an inside and an outside. The user community generally connects from outside of the *backbone transport* portion of the BN. All internal connections are either between internal parts of the backbone transport or with the *backbone NMC*. By extension, the NMC is considered to be inside the BN. In today’s environment of searching for cost reduction while improving user services, a BN will likely interoperate with one or more *external networks* in addition to the user community it supports. The external networks are typically deemed untrustworthy with respect to the BN being analyzed.

Another characteristic of a BN is that it is viewed by users as a means to an end for their missions. The user’s requirement is normally to communicate with another entity, not the BN itself. In other words, the user information travels across the backbone but does not stop there. In Figure 5.1-1, the users are represented by the LSE clouds. The security concerns of the LSE are addressed elsewhere in this framework, e.g., Chapter 6, Defend the Enclave Boundary/External Connections.

In this model, the backbone transport devices are managed and operated remotely by the NMC using commercial off-the-shelf (COTS) or government off-the-shelf (GOTS) network management systems. The NMC devices are separate and distinct from the backbone transport devices. It should be noted that the NMC component of the BN architecture is fundamentally the same as an LSE. Though the purpose and function may be different, the NMC architecture takes advantage of the appropriate security guidance provided throughout the rest of this document.

Generally, the NMC must be operational 24 by 7 (24 hours a day, 7 days a week). Because of that need, NMCs may support remote operator connectivity, represented in Figure 5.1-1 by the remote operator. It is common practice to provide remote access to system experts so they do not have to be physically present at the NMC at all times. A remote operator is similar to a generic remote user and some of the security considerations are the same. Please refer to Section 6.2, Remote Access. However, a remote operator has a significant difference. A remote user connects into the backbone network either from a special service provision—e.g., roaming user dial-up service—or from some external network or LSE connection. The remote user is considered to be *outside* the BN. In contrast, a remote operator—who connects into the backbone NMC via a similar manner—is considered to be *inside* the BN.

In the full life cycle of a BN, new capabilities and features are constantly being incorporated into the devices that compose it. Occasionally new devices or components are installed to replace or upgrade the existing devices or to expand the network and its capabilities. The security concerns associated with this evolution are represented in Figure 5.1-1 by the vendor environment and interface. A common practice in the network industry is to develop the devices and the product software/firmware and then ship these new components to the field in the same manner used by any computer-based product. One method that is often used is to post the product software on an Internet Web site for customer downloading. This distribution approach is open to compromise. To maximize the availability of the BN, it is necessary to have trust (in a security sense) in the entire life-cycle process of the BN and its components.

## 5.1.2 Consolidated Requirements

The fundamental requirement for availability of BNs is that they are required to be present and functioning properly when the missions require them. The President's Commission on Critical Infrastructure Protection acknowledges the importance of solving this problem with the following: "The critical infrastructures [including Information and Communications Industries] are central to our national defense and our economic power, and we must lay the foundations for their future security ..." [1] Specific requirements are identified below.

### Functional Requirements

- BNs must provide an agreed level of responsiveness, continuity of service and resistance to accidental or intentional corruption of the communications service. (The agreement is between the owners of the network and the users of the network.)

## UNCLASSIFIED

Availability of Backbone Networks  
IATF Release 3.1—September 2002

- BNs are not required to provide security services of user data (such as confidentiality and integrity)—that is the user's responsibility.
- BNs must protect against the delay, misdelivery, or nondelivery of otherwise adequately protected information.
- BNs, as a part of the end-to-end information transfer system, must provide the service transparently to the user.
- As part of the transparency requirement, the BN must operate seamlessly with other backbones and local networks.

### 5.1.2.1 Security Requirements

#### Access Control

- Access controls must be used to differentiate access to the network devices between users' access for transport of data and administrator access for network management and control. For example, access controls must enforce user's access to status information versus configuration information.
- Access controls must limit access to the NMC.

#### Authentication

- Network devices must authenticate the source of all communications from other network devices, such as routing messages.
- Network devices must authenticate all connection requests from network management personnel.
- Network management systems must authenticate network management personnel prior to being granted access.
- The NMC must authenticate the source of all communications entering the NMC from external networks.
- The NMC must authenticate the source of vendor-supplied material.
- The NMC must authenticate the source of vendor-supplied software. For example, new releases of operating systems must be authenticated prior to being implemented across the network.
- The NMC must authenticate all dial-in users prior to granting them access to the NMC.

## Availability

- Hardware and software resources (such as user agents and servers) must be available to users.
- The service provider must provide a high grade of system availability for users.

## Confidentiality

- The confidentiality of key material must be protected.
- The network management system shall provide confidentiality of routing information, signaling information, and network management traffic to provide traffic flow security.

## Integrity

- The integrity of communications between network devices must be protected.
- The integrity of the hardware and software in network devices must be protected.
- The integrity of communications between network devices and the NMC must be protected.
- The integrity of vendor-supplied hardware and software must be protected.
- The integrity of dial-in communications to the NMC must be protected.

## Nonrepudiation

- Network personnel must not be able to repudiate changes to the configuration of network devices.
- Vendors must not be able to repudiate vendor supplied or developed hardware or software.

### 5.1.2.2 Networking Environments

Please refer to Section 5.3, System High Interconnections and Virtual Private Networks (VPN) of the framework, where these requirements have been addressed in detail.

### 5.1.2.3 Interoperability Requirements

BNs must be able to securely interoperate with other BNs and local subscriber environments. This requirement includes the secure exchange of network management information and routing data.

## 5.1.3 Potential Attacks and Potential Countermeasures

As with the Requirements for Network Environments section above, please refer to the corresponding System High Interconnections and VPNs, Potential Attacks, Section 5.3, for substantial, related material. The reader should note that this section has a somewhat different focus from that of Section 5.3. This section is focused on attacks against network management operations and against BN infrastructure devices. In addition, this section focuses specifically on user data and information in terms of availability and delivery service capability in the presence of the attacks discussed below.

Threats to network availability can be grouped into three general threat categories as discussed below.

- **Loss of Available Bandwidth.** The threat category occurs because every network has a limited amount of network bandwidth. Attacks can reduce the amount of available bandwidth, limit network resources for legitimate users, and decrease the network's availability. These attacks generally do not impact the operational control of the network. The network is operating as designed and the NMC retains control over the network infrastructure. This category applies to model components 1, 2, 4, and 6 in Figure 5.1-1.
- **Disruption of Network Management Communications.** This threat category impacts the normal operation of the network. Intrinsicly, every network must move information from one user to another over network communication channels. Attacks in this category threaten the normal flow of information through the network by disrupting the communication channels. Examples include shutting down circuits or providing erroneous routing information. These attacks focus on the network management traffic used to control the flow of information across the network. The network is not operating as expected due to the misdirection of the flow of information, but the NMC still has some control over the infrastructure. This category applies to model components 1, 2, and 6 in Figure 5.1-1.
- **Loss of Network Infrastructure Control.** This threat category is the most severe. These attacks represent a loss of control over the network infrastructure. Once the network managers have lost control over the network infrastructure, or over the NMC, they are no longer able to provide the intended network services and, in fact, the network assets are conceivably at risk of being used to support the attacker's goals. This category applies to Critical Security Requirement Areas (CSRA) 3, 7, and 9 in Figure 5.1-1, in terms of loss of control of the BN. The attacks may also occur via any of the other model components in Figure 5.1-1.

Each threat category represents a potential loss of network availability. However, the severity of the attack is related to the loss of control of the network, since control represents the ability of the network managers to respond to an attack. These categories are then considered within the

context of the major threat categories discussed in Chapter 4, Technical Principles, of the framework.

The remainder of this section discusses the relationship of these three general threat categories and the classes of attacks described in Section 4.2, Adversaries, Threats, (Motivations/ Capabilities), and Attacks. Where appropriate, countermeasures for specific attacks are highlighted below. The countermeasures are consolidated in the section that follows.

### 5.1.3.1 Passive Attacks

Passive attacks monitor and collect information as they traverse the network. Previously, BN providers did not consider the passive intercept of network management data as a threat to the network except as a means of gathering information for a more serious active attack. An example was intercepting fixed identifications (ID) and passwords to support a subsequent attack on the control of the network infrastructure. Now, BN providers are viewing passive attacks with growing concern. Providers are considering the overall network topology as sensitive information, with its protection from passive attacks needed to mitigate potential disruption of network management communications.

It remains to be seen which way the commands, status, and the rest of the network infrastructure management traffic will be viewed in the future, but it seems BN providers are working hard to improve security. This is demonstrated prominently in the latest release of the Simple Network Management Protocol version 3 (SNMP v3), which has significant security section additions over earlier versions of SNMP. This class applies to model components 1, 2, 4, 5, and 6 in Figure 5.1-1.

### 5.1.3.2 Active Attacks

Active attacks represent the classic attack by an outsider<sup>2</sup> on the network. In the case of the backbone availability model, the outsider is represented by a “user of the network” or by an adversary connected through an external network connection (as opposed to the insider who is the manager or administrator of the network). All three general threat categories identified above in Section 5.1.3, Potential Attacks and Potential Countermeasures, can be realized; the following discusses the general threat categories relative to this class. These attacks apply to model components 1, 2, 4, 5, and 6 in Figure 5.1-1.

**Loss of Available Bandwidth Attacks.** Network bandwidth represents the network’s ability to transfer information. Loss of available bandwidth attacks (the first general attack category discussed above) consumes network bandwidth, preventing legitimate network users from exchanging information. Three common available bandwidth attacks are the following.

---

<sup>2</sup> Note that the Availability of Backbone Networks section of the framework views insiders and outsiders from the view of backbone networks. Thus, insiders are those authorized to control and manage the network; outsiders include both authorized users of the network (who do not have privileges to effect the control of the network) and potential adversaries that do not have authorized access.

## UNCLASSIFIED

Availability of Backbone Networks  
IATF Release 3.1—September 2002

- 1) Jamming attacks are usually the easiest to detect and possibly the hardest to counter for a network backbone. For example, in a jamming attack an adversary transmits noise in the electromagnetic spectrum of the network preventing the flow of information. Two examples are between a satellite and a ground station or between cells of a wireless network.

A variety of countermeasures—e.g., frequency hopping and redundancy via an alternative media such as terrestrial-based hard-wired systems—for these attacks have been developed for military applications. These countermeasures are usually not implemented in commercial backbone BNs because of cost and other constraints. These attacks apply to model components 1, 2, 4, and possibly 6 in Figure 5.1-1.

- 2) Flooding attacks consume network bandwidth by “burying” the network with processing communications in excess of network capability. Everyone is familiar with the problems with the phone system over holidays or during disasters where everybody tries to use the limited resource at the same time. Active cyber flooding attacks produce the same result using spurious communications traffic. This attack is difficult to counter since the network managers can rarely distinguish legitimate traffic from spurious traffic. The two most common countermeasures are to support a preemption capability, which allows specified users the right to specific bandwidth regardless of other demands on the system, or to limit the bandwidth available through any access point onto the network. This attack is typically applied at model components 1, 2, and 4 in Figure 5.1-1.
- 3) Theft of service attacks may be the subtlest of the available bandwidth attacks. These attacks consume bandwidth, but they appear as normal operations. Attackers pose as legitimate users, establish a connection, and use the network to transfer their information. Most of the time, network managers do not realize bandwidth is being stolen until valid users receive their bill and claim that they did not make specific calls.

A typical countermeasure is to require the users to authenticate themselves to the network before being granted access to network services. Another countermeasure relies on audit techniques. For example, the system could maintain a profile of users’ normal activities and trigger an alarm when the network detects abnormal activity. This attack applies to model components 1 and 4 in Figure 5.1-1. It is also possible at model components 2 and 6.

**Disruption of Network Management Communications Attacks.** These are active attacks that disrupt network communications, intending to interfere with the flow of information across the network by attacking the control commands to the infrastructure devices. By way of contrast, bandwidth availability attacks do not impact the normal operation of the network. They consume bandwidth, limiting the availability of the network but not modifying the command and operation of the infrastructure devices. Network managers are still able to control the network, but the network is receiving misinformation causing a disruption in service. For example, Internet Protocol (IP) routing networks pass network topology data between the routers. This data allows the routers to move a user’s information across the network. If this data is modified,

the routers no longer deliver the user's information as expected, reducing the availability of the network.

Attacks in this category are specific to the BN and how it establishes and maintains the communication pathways to transfer a user's data. For example, voice networks rely on Signaling System 7 (SS7) to manage voice circuits. An attack on this network is to insert a message signaling "one of the users hanging up the phone" resulting in the circuit being dropped. Asynchronous transfer mode (ATM) networks establish virtual circuits to transfer a user's data. An example of a disruption attack on an ATM network would be to transmit an operations, administration, and maintenance (OA&M) cell telling a switch to shut down the virtual circuit. Analysis of this area of attack considers model components 1, 2, 4, 5, and 6 in Figure 5.1-1.

Two countermeasures are available to protect against disruption attacks. First, all network management traffic should originate within the network. This countermeasure requires the network edge devices to check all traffic entering the network to ensure that no network management traffic enters the network from the outside. This approach is referred to as establishing a security perimeter, an enclave boundary, on the system. Second, the integrity and the authenticity of network management traffic should be verified. For instance, a digital signature could be incorporated into the network management traffic. This mechanism could also be used to protect against a replay of valid network management traffic with the incorporation of time stamps or sequence numbers into the signed network management traffic.

**Loss of Network Infrastructure Control Attacks.** The most severe attacks are those against the network operators' control of the network infrastructure. Three ways of attacking control of the network infrastructure are the following.

- 1) Network control attacks directed at the communications between the network operators and the network devices.** These attacks seek to isolate the network operators from the network devices. For example, network operators may access their network through a single connection point into the network. If this point is compromised the network operators cannot access the network.

The best countermeasure is to provide redundant access to the network, allowing the free flow of information from the network managers and their devices. This countermeasure has implications later in this discussion for another control attack.

- 2) Network control attacks directed at network devices.** These attacks focus on getting access to, and thereby control of, the device. For example, most network managers remotely manage their devices and use Telnet or other communications protocols to log into the device. Once the network operator has access, the device can be re-configured, including changing the password used to log into the device. An adversary may choose several ways to gain this control. One example is for an adversary to actively attack the access control using password-sniffing programs. Two possible countermeasures for this attack are to strongly authenticate network management requests prior to granting them access to the device or to set up a protected channel, such as an encrypted VPN, between the network operator management station and the device.

- 3) **Network control attacks directed at the NMC.** If the NMC is rendered inoperable, the network operators are unable to access, let alone manage the network. Every communications path into the NMC serves as a potential attack path. Viruses are an example of these attacks. Viruses could destroy the contents of the memory of the network management devices. Several types of countermeasures are available to protect the NMCs against these attacks. Network guards or firewalls can be used to monitor the communications entering the NMC. These devices can prevent unauthorized communications and check incoming traffic for viruses and other threats to the NMC. A second type of countermeasures is procedural. Policies and procedures should be implemented to support the restoration of the NMC or establishment of redundant NMCs.

### 5.1.3.3 Insider Attacks

The insider threat considers an insider to be any user or network management operator of the system who knowingly or unknowingly causes the reduction of the availability of the BN. Insider attacks are initiated by personnel responsible for managing the network. The majority of these personnel are located in the NMC. In the analysis of BNs there are two “insiders.” There are the operators of the network represented in the model by the backbone NMC. The model recognizes a special case of management personnel: the personnel that operate remotely from the NMC and require additional scrutiny. There are also the developers and producers of the network components, represented in the model by the vendor design and manufacture. Specific insider attacks relevant to BN availability include the following.

- Backbone NMC insider has direct access to the NMC management assets. These users have legitimate reasons for accessing and configuring network assets. These users have the ability to launch subtle attacks on the network, by supplying misinformation to the network assets, or blatant attacks by transferring control of the network assets to an outsider.
- The most effective countermeasures rely on strong procedural mechanisms and strong accountability. Procedural mechanisms can be implemented to separate critical network functions, such as the configuration, maintenance, and provisioning of network assets from noncritical functions, e.g., general e-mail and Web-surfing. Audit mechanisms can be implemented to review the execution of network operations.
- Remote operators are a special case of the backbone NMC insider. These operators are generally on-call experts who help troubleshoot network problems. These operators pose as big a threat as the normal backbone insider does, but their identity cannot be confirmed by procedural mechanisms, and their commands can be compromised during transmission.
- A common countermeasure is to employ a secure modem to protect the remote operator’s dial-up connection. Regardless of the type of remote connection, the identity of the remote operator should be authenticated and the integrity of the transmitted data protected. Analysis of this area of attack considers CSRA 5 in Figure 5.1-1.

- Vendors and producers that develop software control many if not all of these devices. Commercial software is not typically developed with the strict configuration control that is associated with the development of trusted software. Therefore, there is a potential that malicious code can be embedded in the software. This code can support a range of attacks on the network infrastructure including the destruction of the system configuration information, the generation of spurious command information, and the loss of control of the network devices. This threat recognizes the malicious intent of the code inserted into the operating system; another aspect that must be considered is development software that could be exploited. Software developers are infamous for inserting “backdoors” and other features that allow to easy access to the system they are working on. If these undocumented features are not removed before the software is released, they could be exploited by an outsider to gain control of the system.
- The most effective countermeasures to this threat are procedural mechanisms. These mechanisms include the implementation of a strong software engineering process, which identifies the requirements for every software module and reviews the implementation, and strong configuration management. Analysis of this area of attack considers model component 9 in Figure 5.1-1.

### 5.1.3.4 Distribution Attacks

Distribution attacks alter the hardware and software provided by the vendors (commercial or government) as the mechanism to attack the network. These attacks are not limited to the vendor’s personnel, but include the delivery cycle as the hardware and software moves from the vendor to the NMC. The distribution threat needs to consider the movement of new software releases from the vendor to the installation in the network backbone. A common distribution mechanism is to provide a Web server that users access to download the new releases. Currently, users cannot distinguish legitimate material from modified material.

An effective countermeasure is to apply digital signatures to the material allowing the network managers to verify the integrity and authenticity of the information. Analysis of this area of attack considers model component 8 in Figure 5.1-1.

## 5.1.4 Technology Assessment

BNs are not limited to a single technology. Typically, a BN is constructed using a variety of technologies. For instance, the DISN uses IP routers to connect subscribers to the BN. Connectivity between routers is provided by commercial leased lines, satellite links, or ATM switches. This section assesses each of the common technologies used to construct a BN and addresses the available security features.

The technology assessment cannot be limited to the routers and switches used to pass data across the network; it also needs to look at the technologies used to manage the networks. In some instances, a single technology or technique can be used for a number of different types of devices, such as SNMP or Telnet. Alternatively, a single or proprietary protocol may be used to

manage the network devices. This section looks at the security features in network management protocols for Data Networks-IP Router Networks. Later releases of the framework will look at the security features of Multimedia networks and ATM networks.

### **5.1.4.1 Data Networks IP Router Networks**

IP networks are prevalent in today's commercial and government environments. IP network devices used in the wide-area infrastructure must have security features which promote a more robust and secure environment. IP is a connectionless packet oriented protocol that requires security considerations that are different than other technologies used for WANs. IP is a shared media so information that is addressed to a particular destination is readable by multiple network elements. Connections between peers may traverse multiple nodes or hops in the network. For security, this means that a network element does not know its immediate neighbors. Security services, i.e., authentication, access control; must be performed on a per packet basis, because a packet received on a port of an IP router may have originated almost anywhere in the network. Additionally, because IP packets are variable in length, security relevant information may be included with each IP packet.

#### **IP Transactions**

There is network control and management traffic within wide-area IP networks that is required for the BN to function properly. Through the manipulation of these communications, an attacker may modify the operation of the network to accomplish his goals. Because IP is a very dynamic environment, packets may be misdirected, directed through specific routers, or service may be selectively or globally denied. The following sections describe the IP network communications that require security enhancements and which security services can provide protection.

#### **Domain Name Server**

IP networks are dependent upon translating high-level domain names to IP addresses. This service is dependent upon the information stored on local and regional Domain Name Servers (DNS) to be accurate. Without accurate translation between domain names and IP addresses, IP packets cannot be properly routed through the network. Connections will either not be established, or established to end systems other than the intended end systems. The DNS query contains address information that must be translated as well as the responses to previous translation requests.

The integrity of this transaction is essential to establishing communications with the intended end system. The information on the DNS server, as well as the DNS query must not be modified by an unauthorized operator. One of the basic design philosophies of DNS is that DNS information is public and should be provided to all inquirers. Therefore there should be no attempt to implement an access control policy for DNS. Authentication and integrity are critical for an inquirer to know that they have contacted an authorized DNS server, and that the information retrieved from the DNS server is accurate.

## Internet Control Message Protocol

To report errors and unexpected error conditions, or to support network functionality, Internet Control Message Protocol (ICMP) is included with all IP implementations. ICMP poses several unique problems. ICMP messages may be viewed by any node within the network, and it is local policy for each node to act or not act on an ICMP message that it has seen. Additionally, ICMP is an IP layer protocol and does not ride on top of Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). ICMP messages terminate directly at the operating system kernel and are not passed up the protocol stack.

ICMP messages should not be encrypted because all nodes in the network must be able to view them. ICMP messages must only be acted upon when they are received from an authenticated source. Additionally, ICMP messages must also pass an integrity check, to verify that they have arrived as intended. However, there are no security solutions implemented or under development to solve the problem of unauthorized ICMP messages. The recommended approach for local enclaves is to filter on ICMP messages and to only allow those ICMP messages that are critical to operations. This approach does not eliminate the risk of ICMP unauthorized ICMP messages, but it does reduce the risk. In WANs this approach is not viable. The WAN may need to transport ICMP messages between enclaves. To meet customer requirements for supporting network services, filtering on ICMP messages is not an option.

## Routing Messages

An essential part of any IP network, is a dynamic routing mechanism to efficiently transfer packets through out the network. The accuracy of these routing messages as well as the routing tables stored on routers is essential. This accuracy ensures that the routes that the connections take through the network are not denied and make effective use of network resources. Protecting a router's routing table is critical to preserving the availability of the network.

Integrity mechanisms are required for the routing updates sent between routers. This will ensure that routing updates are not modified as they travel through the network. Internal to the routers, an integrity mechanism is also required. Routing tables must be protected against unauthorized modification to ensure that they contain an accurate representation of the network. Additionally, an authentication mechanism is required to ensure that routing updates are not being injected into the network from an unauthorized source.

## Boot Protocol/Dynamic Host Control Protocol

The Boot Protocol (BOOTP) protocol is used when a network device powers up and needs to determine its IP address and possibly its hardware address. If a BOOTP message is intercepted en route to the BOOTP server, an attacker may respond with their own reply. This may cause the network device to download the incorrect memory image, which could have improper configuration information. The Dynamic Host Control Protocol (DHCP) extends this capability to allow dynamic IP addressing. Addresses of other necessary network elements, i.e., location of DNS server, location of timeserver; may be contained in a reply to a DHCP request.

The security services required to protect BOOTP and DHCP messages are authentication and integrity. Integrity ensures that BOOTP and DHCP replies are not modified while traversing the network. It is also important for the BOOTP/DHCP server to authenticate itself to the network device to ensure that an attacker is not masquerading as the BOOTP/DHCP server. Configuration information received in a BOOTP/DHCP response must be received from an authorized server.

## Network Management

Perhaps the most critical area for WAN availability is network management. IP devices must be configured properly and must be resistant to malicious or unintentional tampering in order to provide network services. There are several physically different methods of managing an IP device. These are:

- **Inband.** Network manager connects to the network device using the same communication channels used for user traffic. The protocols used for this may be SNMP, Telnet, or HyperText Transfer Protocol (HTTP) for Web based management.
- **Ethernet Port.** Network managers connect to the network device using an Ethernet network physically separated from the network used for user traffic. This requires an additional network infrastructure to support management traffic. The protocol used for this may be Telnet, or HTTP for Web based management.
- **Local Port.** Network managers connect to the network device via a local port, i.e., RS-232 port, on the device using a laptop or similar computer. This method usually requires the network manager to be in close proximity to the network device. The protocol used for this may be Telnet, or HTTP for Web-based management.
- **Modem Port.** Network managers connect to the network device remotely using a modem interface on the device. Communications are usually over the Public Switched Telephone Network (PSTN) and operators may dial in from remote locations. The protocol used for this may be Telnet, or HTTP for Web-based management.

There are several security services that apply to secure network management. The first line of defense for network management is authentication. Administrators must first authenticate themselves to the network device to prove they are who they claim to be. Closely coupled to authentication is access control. Once an administrator's identity has been proven, their privileges must be determined. There should be several administrative roles on each device, each role with its own set of privileges. This allows each administrator to perform their job duties, but does not grant global privileges to each administrator. An audit log that links administrators to events and the time those events were performed is important. Such an audit log provides a mechanism for determining if a security violation has occurred, who is responsible, and suggests precautions for preventing similar events in the future. Finally integrity is important to ensure that communications between network managers and network devices are not altered while traversing the network. It is critical that configuration files on the devices are not modified by unauthorized personnel.

Traffic flow security for network management traffic may be of concern to some organizations. Network management traffic contains addresses of network components, or other information that may be sensitive. Providing confidentiality for network management traffic will provide protection for information while in transit through the network.

## 5.1.5 Framework Guidance

Our analysis of BN availability has resulted in some general guidance. This guidance is applicable to all of the network technologies that should be implemented to protect the availability of these networks:

- **Protection of Network Management Communications.** While the content of network management traffic is not considered critical, the integrity and authenticity is critical. Digital signatures or some form of secure hashes should be incorporated into all critical network management traffic. These communications also include the vendor-supplied software used to manage the network assets. If traffic flow security or disclosure of information within the network management traffic is a concern, confidentiality should be provided.
- **Separation of Network Management Data.** Backbone availability is not dependent on the protection of user data, but it is dependent on the protection of network management traffic. Countermeasures should be employed to isolate network management traffic from user data. One mechanism is to use an out-of band or dedicated communication channel, such as SS7. The value of separating management traffic from user traffic is to allow the infrastructure to provide the appropriate protection to the user data while impacting network performance only minimally. Network management data should be separated from the user data, and should be protected cryptographically. There are several means available for providing this protection, including encryption, digital signing, and cryptographic checksums.
- **Protection of the NMC.** The NMC is the critical element for maintaining control of the network. As long as the NMC can access the network, the network managers can respond to attacks. The NMC should be protected using the appropriate procedural and physical controls, and network security devices. A security device commonly employed today is a firewall. The NMC should consider constraining its operations to the management of the network. Permitting duties or capabilities beyond that which is necessary to manage the network provides a potential point of attack against the NMC.
- **Configuration Management.** System owners and operators should adopt formal configuration management practices. Strong configuration management allows network managers to restore network operations quickly and effectively after an attack. Configuration management supports the proper implementation of new releases of network software and the implementation of security upgrades. Strong configuration management also protects new releases of network software as the vendors develop them. Finally, it supports rigorous security design and analysis of the system.

The following section provides guidance for the protection of IP data networks. As technology assessments are completed for the other data networks, matching guidance will be incorporated into the framework.

## **5.1.5.1 IP Data Network Guidance**

### **Routing Security**

There are commercial implementations of cryptographic checksums applied across routing update messages.

### **Address Space**

Some government sponsored WANs may have the requirement to protect the addresses of the network elements. To accomplish this static routes must be configured between the WAN and each adjoining network. Network Address Translation (NAT) must be configured at the wide area border node to hide the addressing scheme of the WAN. Conversely, the local network may have the requirement to hide their address from the WAN. In this case NAT must also be configured at the local border node.

In the case of a public carrier network as the WAN, the addressing scheme may not be able to be protected.

### **Filtering**

Filtering, as it is traditionally thought of, is generally not applicable to WANs. Services cannot be filtered because it is likely that every service will be required by at least one user network. However, filtering is applicable to the area of network management. Each network device should contain a list of identifiers that describe the administrators with configuration/viewing privileges on that device. This has historically been done on IP address. IP addresses are easily spoofable. Another mechanism in addition to IP addresses is required to determine which administrators are capable of modifying/configuring each device.

### **IP Security**

IP Security (IPSec), as defined in RFC 1825, is a set of protocols supporting the secure exchange of packets at the IP layer. To achieve this, IPSEC employs two cryptographic security mechanisms: the Authentication Header (AH) and the Encapsulating Security Payload (ESP). These IP-layer security mechanisms may be used together or separately. IPSec is currently being incorporated into vendor products. IPSec functionality should be available in commercial IP network elements.

While IPSec is a suitable set of protocols for providing confidentiality for user traffic, it was not designed to provide security for intra-network communications. IPSec may be used to

implement some VPN scenarios required for segregation of user traffic over the WAN. IPSec is not viewed as being able to provide security to achieve WAN availability.

## Network Management

**Inband.** Inband network management is performed using SNMPv1. There are no security features inherent to SNMPv1. All Management Information Base (MIB) information must be considered accessible to an SNMP agent. Devices typically employ IP address filtering to limit the management stations that may configure/manage the devices. While it is recommended that this feature be used in WANs, it is not sufficient to prevent unauthorized access to network resources. IP address spoofing is common and easily implementable. The recommended approach to inband network management is SNMPv3. SNMPv3 provides confidentiality, integrity, and authentication, and timeliness functionality to inband management.

**Ethernet Port.** Constructing a separate Ethernet network to provide network management is a secure method of network management. It is a physically separate network, which provides a larger degree of control of the network management network. However, for WANs, this approach is not practical. The network elements are geographically disperse and it not feasible to construct another WAN for management. If Ethernet port management is not being used, it is recommended that the network device be configured to disallow network management connections through the Ethernet port.

**Local Port.** It is critical that IP network elements can be securely accessed through a local port. This is often the network's configuration method if the BN element cannot be reached through the network. Physical security of the devices is important to protect the local port. If an attacker does not have physical access to the device they cannot be successful. Authentication and access controls are also critical. There should be several different administrative roles on the network elements. When administrators authenticate themselves to a device, they must assume a role with well-defined privileges.

## UNCLASSIFIED

Availability of Backbone Networks  
IATF Release 3.1—September 2002

### References

1. “The President’s Commission on Critical Infrastructure Protection - Report Summary”,  
[http://www.info-sec.com/pccip/pccip2/report\\_index.html](http://www.info-sec.com/pccip/pccip2/report_index.html)

## 5.2 Wireless Networks Security Framework

The Wireless Networks Security Framework section has been added as an element of the Information Assurance Technical Framework (IATF) to discuss the security of new wireless communications technologies. This section is incorporated because the IATF addresses many security concerns and secure infrastructure elements that also affect wireless communications. Exposure of wireless communications in the radio frequency (RF) transmission environment, and the portability of computer processing and storage that wireless connectivity provides, add another set of vulnerabilities to the vulnerabilities of wired network systems. This section will present the areas of security where wireless communication presents additional vulnerabilities, different customer requirements, and different, although related, security concerns.

Wireless network protection addresses the need to ensure security of user communications where one or more links in the communications channel traverse a wireless link. “Wireless” is defined as the set of services and technologies that does not include more traditional legacy radio communications such as land mobile radio (LMR) and military point-to-point and netted military satellite communications (MILSATCOM). RF systems are addressed separately because the government legacy systems were typically designed for specific applications and included required security mechanisms. The new wireless technologies are commercially based and are not built to specifications for government applications, although the number of government applications for such systems is increasing rapidly. Security measures for new wireless systems must be developed in conjunction with the equipment manufacturers and service providers involved in the wireless industry.

“Wireless,” in this context, defines a set of commercially developed systems and products, and a system infrastructure, that transfers personal communications from wired to RF transmission environments. Wireless communications often are provided as a service to the user where the user does not own the communication infrastructure. These systems often do not require user licensing or user spectrum management (at least in the United States). Typically, wireless systems use low-power transmission and/or spectrum-spreading techniques in short-range communications environments. The characteristics used herein to define wireless are—

- RF communications in commercial and unlicensed frequency bands
- Low-power, short-range communications systems using enhanced processing and multiple transmitters to achieve range when required
- Commercially owned and operated communications infrastructure (there are exceptions)
- Commercial standards
- Vendor proprietary protocols
- Mobility of users and communications.

## UNCLASSIFIED

Wireless Networks Security Framework  
IATF Release 3.1—September 2002

As we describe the technologies and applications involved in wireless systems, the reader will note that there are exceptions to each of these characteristics. Wireless communications, rather than being a set of discrete technologies, applications, and implementations, actually form a continuum of capabilities that connect across the boundaries of the system definitions we provide. Wireless technologies also, in most cases, rely heavily on the wired network and telecommunications infrastructures for their interfaces and proper function. These interconnections are significant in discussion of security.

Wireless equipment may be used by travelers or telecommuters to remotely access their local area networks (LAN), enclaves, or enterprise computing environments. However, most remote access situations involve connecting through wired telephone or commercial data networks. Discussion in this section of the framework focuses on wireless communication networks in general, regardless of the systems being accessed through the network. As digital wireless telephony, two-way paging, wireless LANs (WLAN), and other wireless technologies gain strength in the marketplace, both government and industry users are becoming increasingly reliant on wireless communications for their daily activities. With this in mind, these devices must operate in untrusted, highly mobile, and potentially hostile environments.

There will be some overlap between the options presented here and those presented in other portions of the IATF because the majority of wireless communications networks in use today tie into a larger, wired network with additional security concerns. Previous sections of the IATF have addressed the data network portion of these wired concerns in great detail, and references are made throughout this chapter to those IATF sections, as applicable. Securing wireless communications across network segments implies a unique set of challenges that must be addressed within this framework document in order to provide layered security services, as outlined in the defense-in-depth strategy.

In today's marketplace, the consumer has access to a wide variety of wireless devices, including digital wireless phones, mobile satellite circuit-switched and packet services, WLANs, pagers, and wireless private branch exchange (PBX)/local loop devices. Each device interacts differently with existing wired networks, often through a private gateway or a service provider's network equipment. Additionally, different users have different connectivity and communications security needs. Information protection mechanisms can provide authentication and confidentiality but definitely add to the cost of the equipment. Therefore, before purchasing any wireless communications equipment, users should make a decision regarding connectivity needs and the sensitivity of the information that will traverse their wireless network. Based on these decisions, appropriate protection mechanisms can be selected to meet user needs.

This section examines several categories of wireless technology, addressing the functional requirements, security requirements, and mechanisms involved at each point in the communications and processing links. Security requirements will focus primarily on the following areas: identification and authentication (I&A), access control, data confidentiality, data integrity, and availability. These requirements for wireless systems do not replace those discussed in earlier sections. Instead, they are the same as the security requirements presented for wired networks but may have differing emphasis due to RF exposure, and differing implementation requirements. For example, if a (Unclassified but Controlled) WLAN is

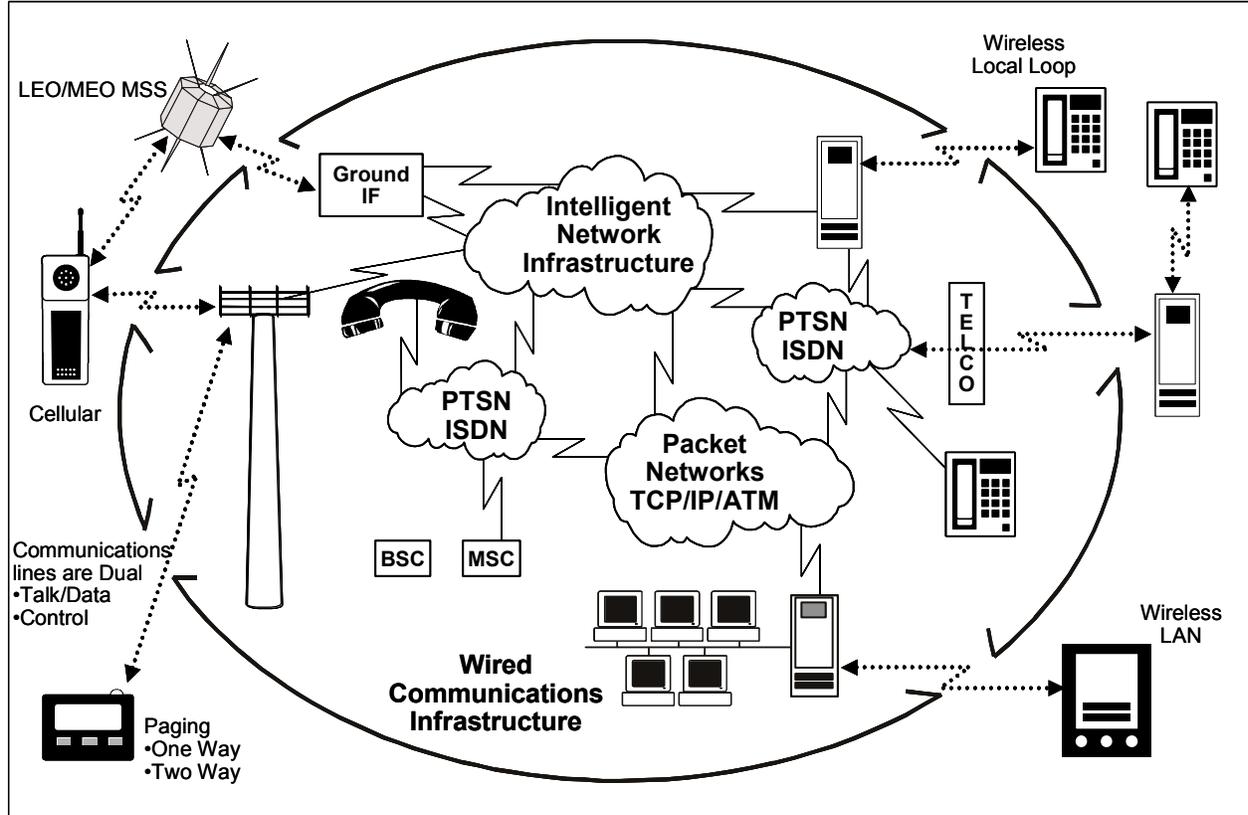
connected to a public network such as the Internet, the requirements discussed in Sections 5.3, 6.1, 6.2, and 6.3 are fully valid. RF transmission of sensitive or classified data adds other variables to the equation in terms of ensuring that the message is received by only the intended recipient, detecting location of users, and combating denial of service—caused by techniques such as jamming. In such situations, a wireless network connection will often expand virtual private networks (VPN), protection of network access (PNA), remote access, and even multilevel security (MLS). Typically, wireless systems connect to their wired counterparts at the same security level as the wired system, although the use of end-to-end confidentiality can permit users to “tunnel” through the wired system at any level of classification without mixing different classification levels. The provision of security mechanisms for High-to-Low, Low-to-High, and need-to-know is entrusted to processors within the system just as it is with wired components.

In developing the security solutions framework for wireless communications, we have subdivided commercial wireless communications into topical areas based on differences in application and implementation technology. Admittedly, there is overlap as providers merge applications to provide new services and maximize customer base (e.g., paging over cellular phones in Personal Communications System [PCS] networks). The wireless topics covered here are divided into the following areas:

- Cellular telephone
- Low Earth orbit (LEO)/medium Earth orbit (MEO) satellite telephone networks
- WLAN
- Paging (one-way and two-way)
- Wireless telephone (wireless PBX, wireless local loop [WLL], and cordless telephone).

Figure 5.2-1 shows a combination of the wireless services attached to a set of wired infrastructures. It depicts a boundary around the various wired information transfer services that includes both data network systems and circuit-switched systems, which typically provide voice communications. Each type of wireless implementation effectively creates a hole in the wired infrastructure boundary because it exposes information in the system to the RF medium where signals can be much more readily detected and intercepted than in wired communications systems.

Figure 5.2-1 demonstrates that security measures implemented in the wired infrastructure can be negated by wireless connections. For example, a user community might have a wired VPN that is secured using a combination of encryption, access controls, and firewalls to create a security boundary, shown as the oval in the figure. The connection of wireless components to the VPN (e.g., wireless LAN, cell phones) can expose the VPN users and their data to over-the-air signal intercept. Such interception is readily accomplished. The wireless assets, if not properly implemented, thus punch holes in the security boundary. These holes are depicted as the breaks in the oval in the figure.



iatf\_5\_2\_1\_0005

**Figure 5.2-1. Wireless Extension of the Wired Infrastructure**

Wireless technology and capabilities are moving so rapidly that continuous updates to this document will be required to attempt to stay abreast of increased bandwidths, new modes of wireless operations, new product and service offerings, and the aggregation of services. As wireless technology services are enhanced, new vulnerabilities and user risks will be introduced.

Throughout this section, comparisons are made between several different types of wireless networks and their wired counterparts. New threats and new vulnerabilities in the wireless arena add a different dimension in security requirements and considerations for designers and consumers. Some of the vulnerabilities and risks described in this section of the IATF are common to both wired and wireless networks and communications media. This section will emphasize areas of risk that are increased by the use of wireless communications media. The framework will highlight critical gaps in current government and commercial security technologies.

## 5.2.1 Cellular Telephone

As technologies have advanced, cellular applications and terminology have become confused. Originally, “cellular” referred to a dialed analog voice telephone call technology that made use of distributed transceivers in line-of-sight communications with connections to the circuit-

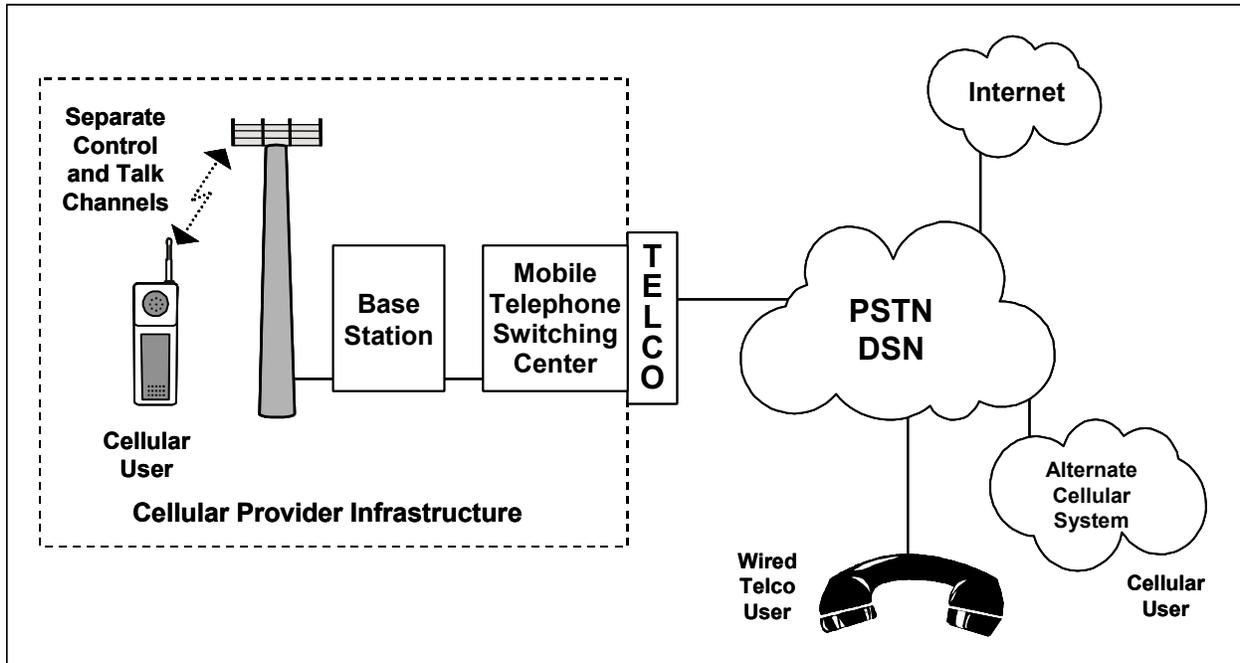
switched wired infrastructure. The term “cellular” no longer means the same thing for everybody because it is evolving into a digital pipeline that can be used for virtually any voice- or data-based service (bandwidth limitations notwithstanding). Cellular systems operate primarily in the 800–900 MHz range and the 1.8–1.9 GHz range using either Time Division Multiple Access (TDMA) narrowband or Code Division Multiple Access (CDMA) wideband RF modulation. These distinctions of frequency and modulation do not substantially modify the services offered by cellular providers but are in some cases germane to the security of the systems. All cellular systems provide an over-the-air control channel from the cellular base station in addition to multiple user “talk” channels. This arrangement means that the bulk of the system control is out of band with reference to user channels.

In recent years, the cellular telephone market has seen tremendous growth around the world. With the transition to digital cellular telephony and the advent of the new PCS, the wireless telephone system has become a major part of both the Defense Information Infrastructure (DII) and the National Information Infrastructure (NII) for mobile users. Moreover, users desire similar functionality with wireless telephones to the functionality they have become accustomed to with standard wired telephones, including call forwarding, conference calling, and secure calling. Specialized militarized systems have been developed where vehicle transportable cell base stations are used as cellular telephone communications hubs. The user instruments that support cellular communications have grown increasingly capable in mobility, processing, storage, and communications capability. This aggregation of capabilities provides enhanced user functions, but also increases the risk of loss of sensitive information, denial of service, and spoofing of user messages and identities.

### 5.2.1.1 Target Environment

This framework examines the standard wireless telephone environment, described as an end user with a hand-held telephone, roaming throughout a cell-based infrastructure owned or at least controlled by a cellular service provider. As shown in Figure 5.2-2, the cell towers connect through a base station to their mobile telephone switching center (MTSC), which provides connection to the public switched telephone network (PSTN) or if service is procured, to the Defense Switched Network (DSN).

Figure 5.2-2 can be broken into three major sections: the user environment, the service provider network, and the public network. The user environment consists of the hand-held phone and associated user, and the traffic and control channels. The service provider network infrastructure includes all equipment and connections from the cellular transmitter through the base station and on to the MTSC. The MTSC is the gateway to the PSTN or DSN for wired routing of calls. The PSTN includes connections to wired users, the Internet, and other mobile network providers. Each segment varies in the levels of privacy and availability provided to the user.



iatf\_5\_2\_2\_0006

Figure 5.2-2. Cellular Telephone Environment

## 5.2.1.2 Consolidated Requirements

Users of wireless networks require functionality from their wireless equipment similar to what they get from their wired counterparts. Wireless telephony is certainly no exception. In discussing the following capabilities and postulated functional requirements, particular attention is paid to functions associated with connecting a wireless user to an existing wired network.

### 5.2.1.2.1 Functional Requirements

- Users/User Equipment
  - Should provide maximum portability and mobility for the user.
  - Must have individual identification (ID), e.g., unique phone number.
  - Must provide unique ID of user instrument.
  - Must be able to provide location to the service provider system, e.g., Emergency 911 (E911).
  - Must have service availability within full assigned area of provider network.
  - Must ensure confidentiality of control channel and voice/data channel information.
  - Must provide protection for information stored and processed in user equipment.
  - Must provide user with maximum allowable access to needed information and services.
  - Must be compatible with different signaling protocols for operation in different locations when outside home network.

- Must interface with wired and wireless user communities.
- Should provide certificate and key management and distribution interfaces for authentication of users.
- Should maximize user instrument operating time (battery life).
- Geolocation is both a benefit provided by cellular systems (under certain circumstances) and a risk for cellular users when the function is not desired. Federal law for E911 service requires geolocation of users for emergency situations. At the same time, the greater precision of the geolocation and the availability of that information in the cellular system put other users at risk during clandestine operations.
- Service Provider
  - Provide high grade of system availability for users.
  - Provide high-quality voice and error-free data services for users.
  - Protect user information (e.g., ID and location) within the cellular infrastructure.
  - Provide priority service for critical users.
  - Provide capability for user communities to manage allocation of user services.
  - Manage security of user provisioning and location information.
  - Protect against the full range of network attacks (e.g., cloning, eavesdropping, impersonation).
  - Provide signaling technologies that are compatible with multiple user instruments.
  - Provide protection against jamming and other denial-of-service attacks.
- Interface to Public Network
  - Provide minimal operational impact on user and phone performance.
  - Provide accurate billing method.
  - Provide dedicated connections from mobile telephone switch to telco.
  - Provide wired telco services (e.g., caller ID).
  - Provide standard interface with telco systems.

### 5.2.1.2.2 Networking Environments

- The networking environment in a wireless telephone network is not as clearly defined as it is in a computer network. One of the significant differences between a cellular network and a computer network is the level of access provided to a user. Local access to a computer network can provide universal access to all systems connected to that network. Access on a cellular network is much more limited for the end user, that is, access to a selected called party. However, with the increased use of the data capabilities of digital wireless telephony, a cellular network may begin to resemble the more familiar computer network. Wireless telephones should offer conference calling, as well as the ability to broadcast data to one or many recipients simultaneously.
- The networking environment should maximize the user's ability to use the service within the full boundaries of the service area. Fading and interference characteristics vary depending on site structures and modulation techniques. Users should investigate these

characteristics for different providers in areas of critical operations for service continuity before selecting a provider.

### 5.2.1.2.3 Interoperability Requirements

- Service providers and associated handsets should not force users to use any nonstandard protocols, modes of operation, or procedures that would prohibit interoperability with external users or systems with which users desire to communicate.
- Different cellular infrastructures currently make certain handsets inoperable in many areas around the world. In addition to the varying protocols, frequency allocations differ globally. While equipment is being manufactured to operate in different frequency bands, switching between protocols like TDMA and CDMA is more challenging. From a network security standpoint, users must carefully consider how transmitted signals affect detectability, availability, power control, jamming, and interception. Based on these considerations, the proper technology should be available to meet the user's needs. Regardless of the primary digital multiple access technique used, cellular handsets that can revert to a more universal system like Advanced Mobile Phone Service (AMPS) are extremely useful when the mobile user is outside of his or her normal area. However, AMPS is gradually being replaced and will not be widely available in the future. Future cell phones will be equipped to handle multiple types of more modern protocols.

### 5.2.1.2.4 Anticipated Future Requirements

- Convergence of technologies is demanding access to Internet services from the wireless telephone. Manufacturers have begun providing this service with a combination of wireless telephone and personal digital assistants (PDA). Increases in channel bandwidth to (in excess of) 100 Kbps have made Internet connection a viable reality.
- Wireless phones will require operation with a smart card or a Subscriber Identity Module (SIM) card for such future technologies as electronic commerce. These cards are also referred to as tokens. A token can be implemented in hardware or software, depending on the required assurance level for the transmitted information.
- Tokens will help cellular phones provide digital signatures, as well as end-to-end confidentiality of information. The security features required for electronic commerce can also be used to implement security features for sensitive and classified traffic.
- The ability to use a single-user instrument for different types of cellular protocols (and other wireless capabilities such as mobile satellite service [MSS], paging, WLAN, cordless phone services, and wireless computer synchronization) is now coming on line. Universal handsets will be available in the near future. This will reduce the cost of confidentiality and other security mechanisms because the security will not need to be implemented for multiple protocols, but could rather become a user application that is independent of the network for end-to-end security requirements.

- The number of communications modes and interfaces described in the previous paragraph will require some common form of authentication and other common security solutions.
- Increased information transmission over the user and control channels will require enhanced security for those connections. For example, caller ID is now becoming available, and E911 will carry very specific geolocation information over the RF path.

### 5.2.1.3 Potential Attacks

The primary concerns of the cellular service provider are theft of service and denial of service. While different types of users may or may not be concerned about the confidentiality of the information transmitted and received by their wireless phone, commercial service providers definitely want to ensure that the cellular system prevents unauthorized use of their service by a nonpaying customer and that the cellular service is functional for paying customers. Confidentiality of the information is typically a secondary objective for the service provider, but a primary concern for business and government users.

#### 5.2.1.3.1 Passive

- Eavesdropping operations were relatively simple with analog AMPS handsets. The change to digital technologies has increased the difficulty of passive eavesdropping, but devices can be readily modified to provide channel scanning and intercept capabilities. Without a true encryption scheme, passive means can result in a major attack.
- Geolocation by an adversary via direction finding, cell location, or E911 requirements.
- Traffic analysis via dialed phone numbers and caller ID.
- Spoofing. Attacker intercepts data, splices in information, and retransmits the message as if originator of the message.

#### 5.2.1.3.2 Active

- As shown in Figure 5.2-2, a distinction must be made between the voice/information channel and the control channel. Interception of control channel information is a bigger threat to service providers, while users are typically more concerned with the confidentiality of the “talk” channel.
- Denial of service by jamming or altering control channel data can be a threat to users and service providers in cellular networks because of the vulnerability of control channel information when it is transmitted over the air. Such attacks typically require physical access to a provider’s network equipment, although outsider spoofing can modify the control channel.

- Outsider control of the transmit power of the user hand-held device allows an attacker to conduct locating and tracking operations against a target. Also, an attacker could cause denial of service by limiting the output power of a user's handset below what is required to maintain a connection.

### **5.2.1.3.3 Insider**

- Duplicate smart cards or SIM cards (copy user token).
- Steal information on user identification and user traffic via control channel intercept.
- Modify control parameters of the system infrastructure.
- Modify user's phone.

### **5.2.1.3.4 Distribution**

- Hardware or software modification in transit could be used as a first step in a complete attack by which an adversary eventually could cause the system to send data or allow access by way of electronic connections to information for which he or she is not authorized. These attacks, however, are not the emphasis within this section.
- The distribution attack is enhanced by the fact that user instruments are becoming increasingly modular. Thus, a user capability is assembled from parts that were distributed separately. Such components include storage devices (disks, flash prom) and communications devices (e.g., PC card modems, wireless modems, and WLAN cards) that could spread viruses and open undesirable communications channels.

### **5.2.1.3.5 Other**

- Theft of portable user devices containing sensitive information and user programs is also a risk. The increasing integration of processing and communications elements in mobile systems can make the theft of user equipment very destructive because of the storage volume and aggregation of information on that equipment.

## **5.2.1.4 Potential Countermeasures**

Sufficient countermeasures must be implemented to provide privacy, authentication, and message integrity in accordance with the level of information being transmitted. Type 1 security, primarily for the DII community, requires countermeasures that provide the maximum possible security for message traffic. Sensitive information requiring Type 2/3 security requires less stringent countermeasures. In order to maintain a secure infrastructure, the Government must overlay a supporting system infrastructure to incorporate authentication and key management and other countermeasures for each level of information as appropriate. Chapter 8, Supporting Infrastructure, is dedicated entirely to discussion of supporting secure infrastructure, and Section 8.1.5.14, Attacks and Countermeasures, covers attacks and countermeasures in more detail.

### **5.2.1.4.1 Encryption**

The primary security requirement for cellular phones, as with any RF transmission system, is protection of user information over the air. There are two primary modes for protection. The first is encryption to secure the information and transmission security (e.g., signal spreading or hopping) to protect the channel and possibly to provide protection against signal detection. Information on the control channel is also user related at times in that it provides information on location, privileges, called party, and calling party. Such information is very valuable for traffic analysis. A second important requirement for users is I&A of the parties in a communications session.

The Federal Bureau of Investigation is presently promoting a law that will prohibit sale of encryption devices for use within the United States that do not provide key recovery services to support Communications Assistance to Law Enforcement Act access. Although the law has not been implemented, it appears that cellular service providers are slow to implement encryption services until the implications of a key recovery law are known. However, the techniques and standards for certificate and key management and encryption exist within the data network world to permit firmware or software encryption to be implemented for sensitive communications. Encryption algorithms can be embedded or implemented on the same tokens that provide user identification and privileges.

Inband signaling is also a target for encryption to prevent traffic analysis. For instance, encryption of dialing and data digit signals sent over the RF network must be considered, as well as caller ID information that precedes a received communication. This will help secure credit card transactions, personal identification numbers (PIN), other account numbers that are entered to access commercial dial-up services, and the identities of calling and called parties.

### **5.2.1.4.2 I&A**

SIM cards and other small token form factors may provide the best countermeasure to enable user and user terminal authentication (and security management). If a phone is stolen, for example, the user can notify the service provider, who then deactivates the SIM card in the stolen phone. The phone can even be programmed to flash “Stolen Handset” to notify the thief that the handset is useless. The same measures that providers use to prevent theft of service from the provider can be adapted to provide I&A security services. For increased security, service providers can permit user groups to control access of their own individual members using software tools that the service providers use to provision systems. The same provisioning capabilities can be expanded to include information such as security clearances, access to keying and other security management infrastructure (SMI) services, and restriction of services within the limits of the overall provisioned (and paid for) service.

### **5.2.1.4.3 Availability and Integrity**

The availability and integrity of communications are largely a function of the protocols used by the service provider to connect calls, to provide reliable communications channels, and to service

an optimal number of customers. As with any telephone system, busy channels are possible, although a busy system (rather than called party busy) is much more likely in cellular systems depending on the number of subscribers within a given cell or coverage area. To maximize the number of users in a given area, the RF power output is often controlled for provider and/or user equipment on a dynamic basis to within a tolerable channel error rate for digital voice communications. Error correction codes are then used to correct the errors that would not be tolerable for data communications. To enhance both availability and integrity, a caller priority technique could be implemented to eliminate busy connections for critical calls and to reduce the number of concurrent general user calls processed within a given cell area in support of emergency operations.

### 5.2.1.5 Technology Assessment

Within the wireless telephone market, current technology is more than adequate to permit insertion of required security into most applications, but few security measures have been implemented. As discussed earlier, the best available security technologies use some sort of token (physical component or inserted code) to provide authentication, access control, and data confidentiality. Lessons can be learned from the use of SIM cards with Global System for Mobile Communications (GSM) phones in the European market, where a user must have both a SIM card and a password (passwords are optional) in order to operate the telephone. Hardware or software tokens can be issued to every individual requiring sensitive communications who will use a wireless telephone in the future. Regardless of which protocol is used in a mobile telephone, the technology is available to ensure that these tokens provide continued high performance and ease of use for the mobile user, as well as providing a mechanism for implementing the required security. For U.S. government applications, cellular end-to-end secure handsets are under development to satisfy Department of Defense (DoD) and other government high-security requirements. Currently, the DoD is fielding Type 1 secure CDMA and GSM phones.

To manage the approval and provision of tokens and security privileges, an SMI infrastructure is required. Presently, the software cryptography implemented in some systems provides protection only for the lowest levels of assurance.

Communications bandwidths (typically less than 20 Kbps) are not yet sufficient to support efficient public key distribution capabilities over the cellular communications channels, but the picture is changing in two ways. High bandwidth cellular services (over 100 Kbps) will be coming on line within the next several years, and new techniques for key and certificate distribution based on elliptic curve cryptography will provide more efficient transfer mechanisms. In combination, these capabilities will minimize call setup times and reduce the airtime cost of security to the point where a more widespread user base will consider the use of public key capabilities.

## 5.2.1.6 Usage Cases

Other sections of this framework have addressed several cases involving connecting equipment at one classification level to equipment at the same or a different classification level across both trusted and untrusted networks. These cases are clearly an IATF issue but also apply in the wireless domain. However, use of wireless equipment interfacing with a wired network does not significantly change the cases that were previously discussed. In general, some level of communications security is recommended for any equipment where there is a connection to a potentially hostile or unknown environment. In the case of cellular communications, all transmissions can be thought of as connecting to an unknown environment because of the nature of RF transmissions and the ease of signal intercept. Thus, the descriptions of each of the specific cases addressed in this framework remain unchanged for the wireless environment. Cellular calls are treated herein as having the same levels of classification as the wired systems to which they are connected. An exception involves the use of high-grade end-to-end confidentiality of the wireless service so that the user is independent of the classification level of the wireless or wired networks to which he or she is connected.

The cellular user scenario to be discussed is the voice phone call from/to a cellular portable phone system. Although the scenario appears to be quite simple, the actions required for the establishment and conduct of the call are quite complex. This “simple” example involves only a voice phone call; that is, it involves no data, pager, or other service that might be available under services such as PCS.

Three types of connections are addressed in this scenario:

- The cellular user calls a plain old telephone service (POTS) user.
- The cellular user calls another cellular user (same or different provider).
- The cellular user calls a satellite telephone user (e.g., Iridium phone).

The risks to users under the three scenarios are similar in terms of over-the-air exposure, but there are differences in denial of service and quality of service that must be considered. The risks presented below will call out the specific situation under which a certain risk or degradation in service occurs.

It is important to note that any communication over commercial facilities opens up a large number of paths for the call control and user voice information to follow. The user has little to say about what path his or her information will take or where important information related to the user will reside. As shown in Figure 5.2-2, for cellular voice calls the paths that can be taken by a call are varied.

Before the user ever gets to the point of making a telephone call, the user has to establish service with a cellular provider. When the service is established, the parameters are set for local service areas and roaming areas, as well as for billing-related items (e.g., free call minutes). All of these parameters are checked before calls can be completed. The user privileges can be checked rapidly by the provider through the use of the wireless intelligent network (WIN) that provides a

## UNCLASSIFIED

separate control system for the networks (separate from the cellular user channels themselves). User-related information is readily available within the cellular control infrastructure.

There are several important security-related elements to consider in making cellular phone calls:

- **Service Is Not Assured.** In an emergency and during peak usage periods, call overload can lead to denial of service for individual phone calls. Spurious or intentional signals sent by third parties can cause calls to hang up. A moving user can experience dead spots within the service area. In certain locations, such as urban areas, call coverage can be very spotty due to electronic and physical interference. Transition of calls between cells is not assured. Since cellular systems are implemented based on user population, many areas with low population density may not have cellular service at all.
- **User Is Identified.** As soon as a cellular phone is turned on within a service area (a call need not be made), the user is identified to the entire system. The user ID is broadcast within the cell in response to interrogation from the cellular system over-the-air signaling channel.
- **User Location Becomes Known.** As soon as a cellular phone is turned on within a service area (a call need not be made), the location of the user is identified to the entire system. The user is located to within a fraction of the cell area (typically several square miles).
- **User's Information Is Exposed Over the Air.** Both the signals transmitted from the user and the signals from the other party to the call are available over the air within the cell site. The equipment required for third parties to intercept calls is inexpensive. Nothing more than a standard cell phone is required to accomplish the interception. There are multiple hacker Web sites that provide information on how to convert a cell phone into an interception-scanning device. The use of high-gain antennas (also cheap and readily available) can extend the interception capability well beyond the cell site itself.
- **An Adversary Can Readily Deny Service.** Cellular signals can be readily jammed and are subject to interference also. Several vendors make intentional jammers to prevent cell phone operation on a given premises.
- **CDMA Technology Provides Lower Signal Exposure.** CDMA transmissions are less readily intercepted than TDMA transmissions, but CDMA transmissions are not, by any means, invulnerable.
- **Intelligibility of Calls May Be Poor.** Basic cell phones that use analog user channels can suffer from noise. Digital channels use low data rate voice encoding that can suffer quality loss through conversions from digital to analog and back in the telephone and cellular networks.
- **Users Can Be Spoofed.** Through theft of equipment or reprogramming of IDs, third parties can adopt the identity of a user and make misrepresented calls.

- **User Cellular Telephone Instruments Are Vulnerable.** As equipment becomes more sophisticated, more information is stored within the cell phones themselves. Several cellular phone models include a palmtop computer as part of the instrument. A stolen cellular instrument may contain much more sensitive information than the user's ID.

## 5.2.1.7 Framework Guidance

### User Advisory

- Cellular phones are adequate for general-purpose traffic but are typically unsuited for high reliability requirements. Numerous government organizations and law enforcement agencies use cellular telephones for general-purpose traffic but use specialized security devices and private networks (e.g., LMR) for critical communications.
- Several cellular providers offer over-the-air encryption of user information, but the security is applied only for the air link, not through the telephone network. In all cases, except the use of National Security Agency (NSA)-endorsed Type 1 instruments, commercial cellular encryption is not suited for classified information exchange. Discretion in sensitivity of information transmitted is necessary.
- Digital telephone services are somewhat more private than analog systems. Requirements for interception of analog conversations are trivial, whereas a small degree of sophistication must be applied to intercept digital connections. Also, digital connections are more readily secured through encryption, should the option be available. Use of digital cellular phones is recommended.
- Use of CDMA technology is preferable to use of TDMA from a signal interception viewpoint.
- Users must protect their cellular phone instruments from theft or loss. The cost of the instrument may be trivial compared to the value of information contained on the instrument.

### Desired Security Solution

- Users within the NII and the DII require reliable service with assurance of data integrity and confidentiality, as well as protection from handset cloning and misidentification.
- Any cellular/PCS network should provide over-the-air security (at a minimum) for both voice and control channel information.
- End-to-end security for user conversations and data transfers is required for U.S. Government sensitive and classified operations.
- Users should be protected from RF attacks and traffic flow analysis attacks.

- Systems should provide capabilities for users to be restricted to absolute need in the use of options available within the systems (e.g., caller ID), thus minimizing the amount of traffic-related information sent over the air.

## **Best Commercially Available Solution**

- The best current solutions involve using a PCS phone or a GSM phone with a SIM card to provide user I&A.
- Cellular providers have adopted RF signature evaluation techniques to find stolen cellular user instruments.
- Network providers currently secure billing information through the cellular and PSTN networks.
- GSM standards provide for encryption of user channels within the provider secure infrastructure (i.e., as far as the wired telco interface). This encryption is from the cellular phone to the base station only and is not sufficient to protect classified or sensitive information.

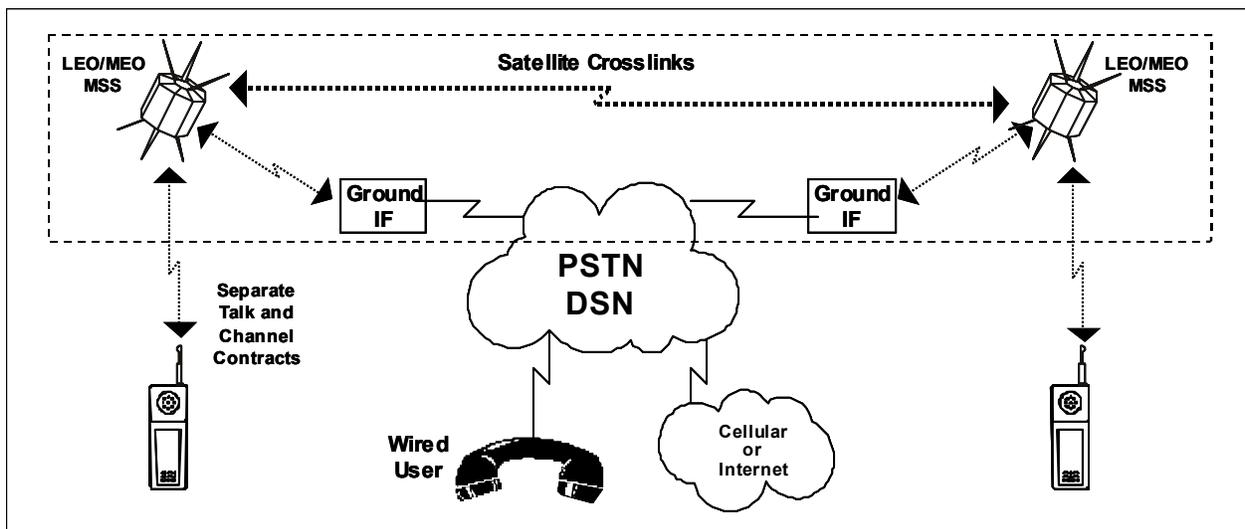
## **Technology Gaps**

- Adequate security mechanisms to implement Type 1 security for U.S. government classified operations, for example, insertable or software-based high-grade encryption.
- Protocol-sensitive encryption techniques to protect multiple data protocol types.
- SMI within the service provider network to include user security privilege establishment, maintenance, and distribution.
- User-operated control and provisioning systems to allow rapid reconfiguration of user privileges to modify services in emergency quick-response operations.
- Modified modulation techniques for spread spectrum systems (e.g., CDMA) to decrease the effect of electronic jamming and reduce the probability of detection for covert users.

## **5.2.2 Low Earth Orbiting/Medium Earth Orbiting Satellite Telephone Networks**

LEO and MEO satellite telephone networks, often referred to as MSS, are the next stage in worldwide, portable telephone connectivity. Unlike the cellular/PCS systems discussed earlier in this section, these handsets will provide telephone connectivity from anywhere in the world where the subscriber elects to pay for service. The traditional cell structure and roaming environment changes significantly with these networks because the cells are now moving and the users are remaining relatively stationary compared with the faster moving LEO satellites.

LEO satellites circle the planet many times each day at orbit altitudes of 300 to 1,000 miles. The engineering is very complex because these systems cover large areas with many small, low-powered satellites. Currently, only two satellite services are scheduled to be partially available now or in the near future: Iridium and Globalstar. In one case, there will actually be handoffs between the satellites, as shown in Figure 5.2-3. Advantages of these services will include worldwide coverage, the ability to use portable phones, and automatic searching for a terrestrial (cellular) service before switching to the satellite. Many MSS phones scheduled for commercial use operate with local digital cellular networks as well as with the satellite network. Because of the present high per-minute cost of satellite communications, the phone will/should first try to access a local cellular system when making a call. If no cellular service is available, the satellite service is used.



latf\_5\_2\_3\_0007

Figure 5.2-3. Mobile Satellite Subscriber Environment

### 5.2.2.1 Target Environment

The target environment is very similar to the cellular case where a user is making or receiving a phone call from a portable mobile user instrument to another portable instrument, to a wired telecommunications user, or to a cellular telephone. In this environment, the user and recipient can be anywhere in the world.

As previously presented for the cellular case, the elements of Figure 5.2-3 can be broken into three major sections: the user environment, the service provider network, and the public network. The user environment consists of the hand-held phone and associated user, as well as the talk and control channels. The service provider network infrastructure includes all equipment and connections from the satellites and earth stations, the satellite control infrastructure, and the ground entry points that interface with the PSTN. The public network includes connections to wired users, the Internet, and other mobile network providers.

## 5.2.2.2 Consolidated Requirements

The following requirements are proposed for government utilization of MSS capabilities.

### 5.2.2.2.1 Functional Requirements

- Global coverage area for call transmission and reception.
- Continuation of call connection from satellite to satellite.
- User and recipient I&A.
- Voice and data confidentiality and data integrity.
- Transmission of voice and data.
- User geolocation capability (both beneficial and a vulnerability).
- Long user instrument lifetime (battery power).
- Accurate and timely billing procedures.

### 5.2.2.2.2 Networking Environments

- Cross-connected satellite constellation for primary call handling (vendor or service provider proprietary protocols).
- Data transmission capabilities of up to 19.6 Kbps currently for e-mail and other short message services.
- Interconnection to PSTN, cellular networks, and data networks.
- Worldwide paging services also available through LEO satellite networks.

### 5.2.2.2.3 Interoperability Requirements

- User instruments that can be used with the MSS system and with cellular telephone systems.
- Interfaces with all PSTN systems worldwide.
- Sufficient digital voice quality to traverse the PSTN and be intelligible in cellular systems.

### 5.2.2.2.4 Anticipated Future Requirements

- Increased bandwidth to support data transfer.
- Increased voice quality for conferencing.
- Reduced cost of user instrument to expand availability.
- Support for SMI functions.

## 5.2.2.3 Potential Attacks

### 5.2.2.3.1 Passive

- Largely the same as for cellular RF emission vulnerabilities.
- Interception of data from the satellite downlink transmission can be accomplished from anywhere in the satellite footprint (larger space than for cellular). The only drawback for the adversary in this case is the volume of information to be processed.

### 5.2.2.3.2 Active

- Denial-of-service attacks by electronic jamming.
- Like attacks on cellular systems, network attacks through LEO/MEO satellite systems are somewhat limited in scope. An adversary cannot access the entire telephone network simply by intercepting one telephone call. In other words, local access does not allow universal system access as it would in the case of a LAN connected to the Internet.

### 5.2.2.3.3 Insider

- Modification of handsets before delivery to customer.
- Duplicate handset and user ID information can be loaded into a second phone (nonsimultaneous use).
- User location information available to service provider.

## 5.2.2.4 Potential Countermeasures

Many of the countermeasures discussed in the Cellular/PCS section also apply to satellite telephones. Theft of service will most likely be the primary goal of any hacker on the MSS telephone network. Theft of information and eavesdropping will likely be a secondary concern for providers, but will be critical to certain government users. Service providers must ensure that control channel information is secure, and procedures must be in place to provide user I&A in order to prevent theft of service. Providers must also permit the use of end-to-end confidentiality mechanisms to protect user information.

With a cellular structure, creating some type of SMI incorporating key management and other countermeasures is easier within a country. Any SMI used in the LEO network must fit into more of a global management structure. However, as costs drop and satellite telephony becomes more popular, usage by customers within both the DII and the NII will likely increase. Before these telephones become useful for customers in the DII transmitting sensitive information,

sufficient countermeasures must be implemented to provide privacy, authentication, and message integrity in accordance with the level of information being transmitted.

Use of some sort of token or smart card with the telephone handsets can also be integrated into the satellite network. As with cellular systems, SIM cards may provide the best countermeasure to enable user authentication and key management. Only authorized users will be able to access the satellite network. Also, if a phone is stolen, the user can notify the service provider, who then deactivate the SIM card in the stolen phone. The phone can even be programmed to flash “Stolen Handset” to notify the thief that the handset is useless.

### **5.2.2.5 Technology Assessment**

As of this writing, service has been initiated on both the Iridium and the Globalstar networks. Proposed technologies include dual-mode (GSM/MSS) handsets, voice and data transmission, paging, facsimile, and position location. Iridium will use a combination of Frequency Division Multiple Access (FDMA) and TDMA multiple access technologies, while Globalstar uses CDMA. Type 1 secure handset for end-to-end confidentiality in the Iridium network has been developed.

### **5.2.2.6 Usage Cases**

As stated for cellular usage cases, other sections of this framework have addressed several cases involving connecting equipment at one classification level to equipment at the same or a different classification level across both trusted and untrusted networks. These cases are clearly an IATF issue and also apply in the MSS domain. In the case of wireless communications, all transmissions can be thought of as connecting to an unknown environment because of the nature of RF transmissions and the ease of signal intercept. Thus, the descriptions of each of the specific cases addressed in this framework remain unchanged for the wireless environment.

The sample case of an MSS call can be treated in a very similar manner to that of the cellular call scenario described earlier. If we take the earlier cellular case of calls to another MSS telephone, a wireline-connected standard telephone, or a cellular telephone, the cellular vulnerabilities presented in Section 5.2.1.6, Usage Cases, exist with some modifications, as described below:

- In most cases, the MSS user must preregister with the service provider for specific roaming access areas outside of home territory.
- The extended satellite footprint makes user information more available to interception since the terrestrial range over which the RF signal is broadcast is on the order of several hundred miles.
- For at least one MSS service (i.e., Iridium), user coverage is global. In other cases (e.g., Globalstar/ICO), far north and south latitudes are not covered.
- Transmission rates are typically lower for MSS services than for cellular services. Since digital voice rates are reduced, voice quality is reduced. Connections across MSS and

cellular systems may suffer degradation in voice quality to the point where user voice recognition is not possible.

## 5.2.2.7 Framework Guidance

### User Advisory

- The risks for users in using MSS services are similar to those for cellular. The range of interception for MSS calls is increased, but the risk of geolocation is reduced. Keep messages short for both security and financial reasons.
- There is insufficient data concerning the operability of MSS systems to make definitive statements on system availability and loading. Request provider information on call completion rates.
- The development of instruments and protocols for high-grade end-to-end confidentiality has begun. If you are addressing user requirements for your organization, contact NSA for status of efforts.

### Desired Security Solution

Ideally, an MSS telecommunications network will provide confidentiality for both talk channel and control channel information. Users within the Government require reliable service with some assurance of data integrity and confidentiality, as well as protection from spoofing and misidentification (e.g., handset cloning). Integration of the smart card technology used in GSM phones with the satellite phone handsets could help provide adequate protection for users.

### Best Commercially Available Solution

Currently, the Iridium and Globalstar networks are operational with some commercial-grade encryption available over the air link. The only Type 1 solution today is the Iridium Security Module (ISM) for Iridium. The ISM provides handset-to-handset encryption and handset-to-STU/3 encryption through a red gateway. The primary security needs for satellite telephone services are end-to-end confidentiality for user information and the protection of caller and calling party identification.

### Technology Gaps

- Adequate security mechanisms to implement Type 1 or Type 2 security.
- SMI within the service provider network.
- Protection of stored information in user instruments.

- As wireless telephones increase in complexity and become more like personal computers, user handsets will require a way to provide secure data storage using SIM cards or other types of tokens.

## 5.2.3 Wireless Local Area Network

WLANs are quickly gaining popularity in multiuser environments. A WLAN can be used as a stand-alone network, or as is most often the case, it can be used to increase the range, flexibility, and user mobility of a larger network. WLANs are typically implemented with personal computer (PC) cards inserted into network processors, and can also be implemented in portable devices such as hand-held computers. A WLAN uses the same transmission (Ethernet is typical) and data protocols (e.g., Internet Protocol [IP]) as its wired equivalent but provides a lower bandwidth (e.g., 1-11 Mbps versus 10-100 Mbps for Ethernet). The typical implementation for RF communications is a collision avoidance direct-sequence spread-spectrum or frequency-hopped protocol under the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard. Members of a WLAN communicate one at a time as on an Ethernet rather than in an overlay of signals as occurs in CDMA cellular systems. Multiple WLAN nets can then be overlaid in the same location and frequency range by using different spreading or hopping sequences. WLAN members have a connection distance measured in the range of 100 to 1,000 feet, depending on the environment, e.g., office building, and open space.

WLANs have gained entrance into the marketplace primarily in the vertical markets of health-care, retail, manufacturing, warehousing, and academe. These markets have leveraged the productivity gains of using hand-held terminals and notebook computers to transmit real-time information to centralized hosts for processing. Primarily, WLANs provide an advantage when mobility, scalability, and installation speed, simplicity, and flexibility are important requirements. An interesting example of a large-scale WLAN integration is the Fox Tower building in Portland Oregon. The Fox Tower will feature connectivity to a high-speed fiber-optic network, including satellite transmission, digital phone lines, WLANs, video, and high-speed digital subscriber line access, to every tenant on every floor, regardless of each tenant's current technology capacity. This is an example of the architecture providing information technology infrastructure in a flexible, scalable plan to minimize the cost of constantly upgrading the system infrastructure as tenants move or change technology.

### 5.2.3.1 Target Environment

The WLAN provides flexibility for movement of net members but requires a high degree of colocation of the wireless segments (communications range on the order of 300 feet). WLANs are often used in offices and facilities where the wiring required for a standard network has not been installed. Other applications include provision of network interconnection where the nets must be configured and torn down rapidly. A tactical military command post or forward air base is an example of the latter. The target environment, shown in Figure 5.2-4, has been drawn to represent the case where a WLAN extends an existing network through a wireless modem link.

The WLAN environment is a notable exception to the definition of “wireless” provided earlier in Section 5.2, in that, in the WLAN case, the user owns the wireless infrastructure (however small that may be). The user buys the components and does not need to rely on a service provider for WLAN operation. This fact provides flexibility in location, mobility, and applications. However, the WLAN is tied to a wired LAN environment in most cases, thus reintroducing “borrowed” infrastructure requirements.

The wired infrastructure to which the WLAN is connected can be formulated in several ways. As shown in Figure 5.2-4, the “cloud” can be the Internet or a secured environment composed of an intranet or a VPN. The security implications of connecting WLAN components to an intranet or a VPN are of particular importance. It must be noted that the range from which an observer can observe (detect or read) the signals emanating from the wireless connection is always greater than the range over which the WLAN will operate. Very simply, the use of high-gain directional antennas from a remote location provides the same receive signal strength that can be achieved by a close-in user with a standard antenna and receiver.

The key elements of the environment are the physical space where the WLAN is implemented (size and type of physical environment and its perimeter), the level of classification or sensitivity of information handled in the system, and, as mentioned in the previous paragraph, the wired interconnect mechanism. Special cases of High-to-Low classification, firewalls, and other wired LAN security elements are assumed to be handled by the wired LAN segment of the target environment.

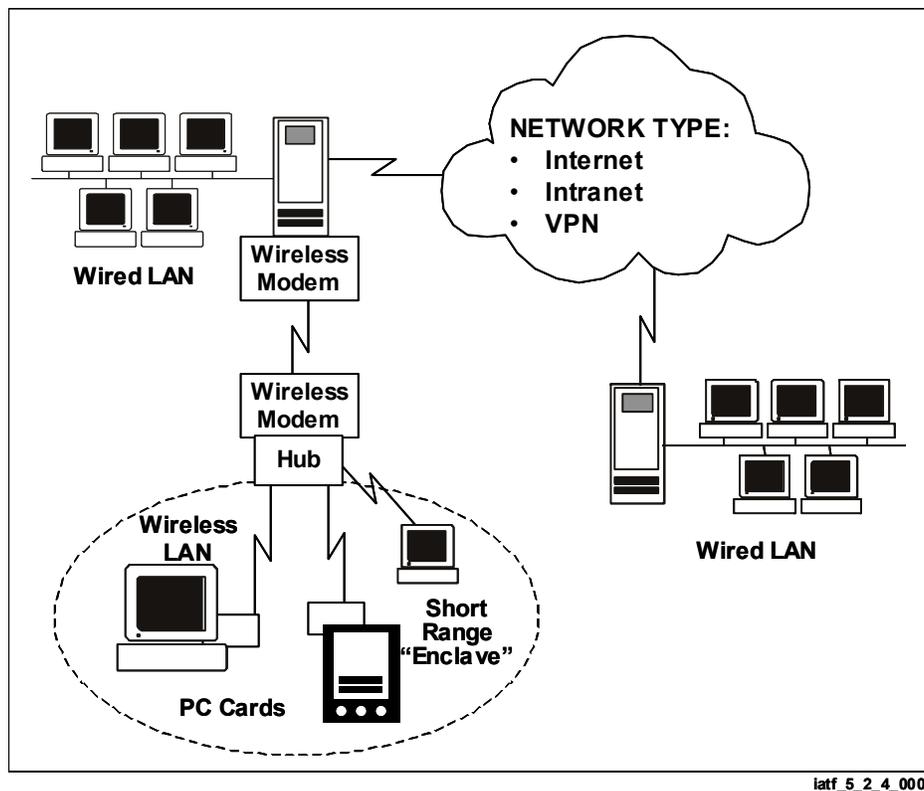


Figure 5.2-4. WLAN Environment

## 5.2.3.2 Consolidated Requirements

Users of WLANs typically connect through an access point to a larger wired network. Each access point can represent a separate user domain, or multiple access points can be assigned to the same domain to increase data throughput in high-usage areas. When connecting a WLAN to an existing network, system administrators must be careful not to weaken the existing network security of the wired LAN. The use of VPNs, as discussed in Section 5.3, System High Interconnections and Virtual Private Networks or secure wireless LAN products, will play large parts in ensuring adequate security for WLANs. Without access controls at the wireless nodes, an attacker can gain universal access to the entire network by simply penetrating a single node.

Additionally, a distinction must be made between use of a WLAN in a standard office environment and use in a highly mobile or tactical environment. An office environment will typically require a network to handle higher traffic loads and a large number of users. Tactical environments, on the other hand, will usually operate in a hostile environment. Traffic loads may vary, and networks will typically consist of fewer, more mobile users than wired cases. Requirements may differ dramatically between the two environments. The following is a list of proposed requirements.

### 5.2.3.2.1 Functional Requirements

#### User/Mobile Terminals

- Provide access control for restricted domains.
- Provide user I&A mechanism.
- Ensure VPN software compatibility to support data confidentiality.
- Support secure wireless LAN card.

#### Access Points/Network Equipment and Configuration

- Strong access control.
- Ensure network bandwidth availability. The network must be fast enough and able to handle a large number of nodes without becoming unusable.
- Ensure data integrity.
- Provide continuous authentication of all users connected to a WLAN.
- Establish secure wireless domains for each access point.

### 5.2.3.2.2 Networking Environments

- Ability to communicate with wired networks through a wireless access point within range of the LAN at data rates sufficiently high to prevent congestion.

- Ability to communicate at close range among mobile elements (ad hoc network) as in a field tactical situation.
- Provision of spreading codes that minimize interference with other wireless LANs.

### 5.2.3.2.3 Interoperability Requirements

- Networks using different modulation schemes cannot communicate directly with each other without any conversion. Both direct-sequence spread spectrum (DSSS) and frequency-hopped spread spectrum (FHSS) modulation are part of the IEEE 802.11 WLAN standard. In the standard network environment, gateways are used to translate between networks from one protocol to another.
- Collocating WLAN systems must not cause interference problems with other wireless systems in the vicinity. Spread-spectrum modulation attempts to minimize this interference. However, with the common 11-bit spreading code, WLAN systems will not attain a processing gain much higher than 10 dB (Federal Communications Commission minimum). Longer spreading codes would increase processing gain and could improve data security.
- Appropriate key management must be used to isolate/coordinate separate wireless LANs.

### 5.2.3.2.4 Anticipated Future Requirements

- Wireless networks must allow for the evolution and reconfiguration of the network and associated components without disruption of service.
- Higher data rates will likely lead to more frequent transmission of time-sensitive data, such as audio and video files. Current standard data rates of 1 or 2 Mbps are far too slow for practical video transmission given that a multiuser LAN begins to saturate at an aggregate throughput of approximately 10 percent of rated speed. Also, transmission of large text or image files can cause congestion in a WLAN. WLAN data rates are quickly approaching 56 Mbps.
- Current WLANs can optionally apply low-grade data scrambling or basic encryption to the transmitted data. All the header information is frequently sent over the air in the clear. This causes weak traffic flow security, a problem that will be discussed in the Potential Attacks section below.
- If WLANs are to be used in a classified environment, individual node identity and message header information may be classified and thus will need to be protected at a higher level of security than presently available. This will require capabilities akin to the Network Encryption System (NES) or other robust encryption discussed in Section 5.3.5 of the IATF, but with a portable form factor.

### 5.2.3.3 Potential Attacks

A WLAN without appropriate security mechanisms in place can add critical vulnerabilities to a network, making it easy for an attacker to penetrate. With WLANs, an adversary no longer requires physical access to the network, as in a wired situation, in order to exploit a wireless system. This physical access is particularly important to an adversary in the case of VPNs and intranets, where physical access is required if those systems are properly established and protected in accordance with the IATF recommendations. Addition of a WLAN to a VPN or an intranet removes the physical access requirement for an adversary to penetrate the system.

#### 5.2.3.3.1 Passive

- Signal detection and intercept are readily accomplished with WLANs due to the limited requirements for diversity in spread-spectrum systems. The standards are public in IEEE 802.11, facilitating signal detection.
- WLAN signals are designed to penetrate office walls and to maintain user connectivity at significant distances—up to several hundred feet. Therefore, an attacker has the advantage of operating without requiring access to a protected facility, and the attacker can use high-gain antennas and receiver equipment to recover a signal. (Note that this is a major difference from a wired architecture. While some devices on a wired network may inadvertently radiate, they are not designed to do so. Cable shielding and the use of fiber-optic cable for network connections make it difficult for an adversary to tap on to a wired network without gaining access to the actual cabling.)
- A passive attacker can determine critical information about network architecture just by monitoring message headers, even if all the transmitted data has been encrypted. While this may be acceptable for government and some DoD applications, many government sensitive networks and military tactical networks would prefer not to divulge critical information about network nodes. Therefore, there is a clear requirement for inclusion of strong message confidentiality and good traffic flow security (packet header cover) in future WLAN designs.

#### 5.2.3.3.2 Active

- Attacks on a WLAN can be accomplished easily with the proper network analysis equipment. Standard network sniffers can be adapted to analyze wireless network packets. Current sniffer technology allows the sniffer software to be run from a laptop computer.
- Denial-of-service attacks, though not specifically network based, can have drastic effects on critical DII and NII networks if not properly detected. WLANs operate like any other radio in that the receiver must maintain an adequate signal-to-noise ratio in order to maintain a link. When the noise overpowers the signal and any processing gain, proper

reception will not happen. If an adversary decides to jam an access point or a major portion of the wireless network, the WLAN will not continue to function. However, this type of attack, and the source of the interference, would be easy to detect and correct. On the other hand, if an attacker directs a jamming signal at only one node, the rest of the network has no way of knowing why that node has gone down. In fact, many of the access points (i.e., wireless hubs) on the market today will continue to show a valid connection to that node even if it is currently unreachable. If a WLAN is used in a critical part of the NII, preventing denial-of-service attacks will be a major issue to address.

- Network information available to an adversary can lead to spoofing attacks using directional transmission aimed at the system RF hub or at a single node. The attack against a single node is more difficult to defend against because the RF hub would be unaware of the interference.

### 5.2.3.3.3 Insider

- An insider on a WLAN can often have access to access point configuration files. Without proper administrator authentication procedures at the access point, a user can modify these configuration files to increase the vulnerability of the entire network. For example, access points will usually only forward a message to their wireless nodes if the intended recipient is in that accessed point's domain. Thus, the wireless link is more efficient, and an attacker cannot easily view messages between nodes on the wired network. A malicious insider could modify the access point configuration to pass all or none of the network messages on to its nodes, if proper administrative authentication procedures are not in place.
- As on a wired network, many insider attacks are available in a WLAN. While user privileges can be set on a network server by the system administrator, there is no mechanism in place to prevent a legitimate user on the system from entering more private areas on the network. File privileges can be set on sensitive files, but if a privileged user wants to take advantage of a WLAN, there is no mechanism to prevent this. Again, this problem is not specific to wireless networks and was addressed in earlier sections of the framework.

### 5.2.3.3.4 Distribution

Hardware or software modification in transit could be used as a first step in a complete attack by which an adversary eventually could cause the system to send data or allow access by way of electronic connections to information for which he or she is not authorized. These attacks are more readily prevented using physical and operational security techniques and are not a primary emphasis in this section.

### 5.2.3.4 Potential Countermeasures

Many of the countermeasures used in a wired network, and those described in Section 5.3.4, Potential Countermeasures (for VPNs), also apply to the wireless case. In general, maintaining privacy is accomplished by appropriate use of confidentiality mechanisms. If a WLAN is employed in a classified application, the strength of confidentiality mechanisms must be sufficient to withstand national laboratory strength attacks.

As discussed in Section 5.2.3.3.1, traffic flow security is a major issue. Unfortunately, a WLAN cannot simply implement a constant bit rate leased line or other traffic shaping mechanisms. Leased lines in the wireless case do not apply, and traffic shaping may severely limit the throughput of the wireless link and interfere with the collision avoidance mechanisms in place. One way to provide some traffic flow security would be to route all wireless traffic through secure tunnels.

Wireless network sniffers used in conjunction with bit generators can be used to insert messages into a wireless network that appear to have originated in the network. Continuously authenticated channels can prevent insertion of information into the channel that can lead to short plaintext attacks that allow cryptanalysis by guessing known responses to known short messages.

Prevention of denial-of-service attacks on WLANs is a difficult issue, although, in some respects, the wireless case is very much the same as a denial-of-service attack on a wired network. Network administrators must implement proper authentication software to prevent the manipulation of network hardware. In the wireless case, simple signal detection mechanisms can probably detect and locate an obvious RF jamming signal as easily as an administrator on a wired network could detect a broad denial-of-service attack.

### 5.2.3.5 Technology Assessment

The technologies for WLANs are targeted at minimized bandwidth licensing requirements. Since users own their system infrastructure for WLANs, the low power and spread spectrum techniques that support nonlicensing of the spectrum are valuable to the user community. However, users, particularly government and DoD users, are cautioned that unlicensed bandwidth in the United States, e.g., 2.4 GHz band, may require licensing for use in foreign countries. Federal licensing authorities must be consulted on foreign requirements for bandwidth and spectrum allocation before systems are implemented in foreign countries.

FHSS and DSSS are both defined in IEEE 802.11 for WLAN applications, and both have been implemented by product vendors, but DSSS is the more popular implementation. Limited LPD is provided by the waveforms, but the 802.11 standard is sufficiently restricted in spreading patterns that such protection cannot be deemed suitable for military environments. The anti-jam (AJ) protection that is afforded is similarly weak for the same reason.

Current encryption and data scrambling methods used in WLANs provide minimal data protection and are not suitable for protection of classified information. The data encryption

techniques for commercial WLANs are insufficient for other than privacy. Presently, key lengths are restricted to 128 bits. The casual probe will not achieve access, but the strength of the cryptography will not withstand a more determined attack. Cryptography that provides security for transfer of header information is not in place and is not easy to implement. DoD products such as TACLANE cryptography are available for high-grade protection of over-the-air signals. Development of PC card-based Type 1 security devices is also under study. The interfaces are complicated by use of such products because the commercial capabilities are meant to plug directly into processing elements. The DoD cryptography must be inserted between the processing and the transmission elements. The TACLANE is transportable, but not man portable.

Operating frequencies vary according to product vendor and system. Presently, the 2.4 GHz band is the most popular; however, higher data rates are achieved with larger bandwidth in the 5.6 GHz range. It has been found in certain application environments that interference problems can occur. Notably, microwave ovens have been found to “jam” some WLAN systems. The RF technologies used in the GHz range communications systems include antennas that vary from 2–3 dB isotropic to directional gains in excess of 20 dB. In fixed plant configurations (or portable configurations that remain in one location during operation), the directional antennas can be used for nodes of a WLAN to increase range to a distance of several miles. Such nodes cannot then be highly mobile, since directional antennas must be aimed for effective operation. Unfortunately, the same antennas can be used by an adversary to expand his or her probe range to a similar distance.

The wireless modem shown in Figure 5.2-4 provides the capabilities of a microwave transmission system at a small fraction of the cost. Such modems, as in the case of microwave links, can readily be equipped with over-the-air confidentiality applied to the modem point-to-point connection. Since the connection is point to point, and independent of protocol, there are straightforward solutions provided by commercial vendors and DoD to provide link encryption security at the requisite security levels.

### 5.2.3.6 Usage Cases

Other sections of this framework have addressed several cases involving connecting equipment at one classification level to equipment at the same or a different classification level across both trusted and untrusted networks. These cases are clearly an IATF issue and also apply in the WLAN domain. In general, some level of communications security is recommended for any equipment where there is a connection to a potentially hostile or unknown environment. In the case of wireless communications, all transmissions can be thought of as connecting to an unknown environment because of the nature of RF transmissions and the ease of signal intercept. Thus, the descriptions of each of the specific cases addressed in this framework remain unchanged for the wireless environment.

As mentioned previously, the type of network to which a WLAN is connected has substantial impact on vulnerabilities, attack approaches, and the damage that can be done. There are three interconnection possibilities in the scenario presented here for WLAN:

- Users connected to a stand-alone WLAN.
- Users connected to a WLAN that is interfaced to a wired VPN or intranet.
- Users connected to a WLAN that is connected to the Internet.

Figure 5.2-4 shows the three scenarios. The following security related elements apply:

- **Over-the-Air Exposure Exists.** Although spread-spectrum techniques are used, the spreading techniques are public and the signals are not difficult to intercept.
- **Detection Range of WLAN Signals Is Much Greater Than Communications Range.** Typical WLANs use small omnidirectional antennas. High-gain directional antennas can pick up signals at much greater ranges than those used for communications (the range can be several miles).
- **Information on Any WLAN Connected Network Is Exposed.** All communications on a WLAN are exposed to interception. Information on wired LANs to which the WLAN is connected is also exposed to interception. In the case of VPN or intranet connections, the protective mechanism of those networks may be defeated.
- **IP Headers Are Subject to Traffic Analysis.** The interception of IP traffic can compromise more than user data through the use of source/destination analysis.
- **WLAN Signals Can Be Spoofed.** Just as on the Internet, adversaries can use RF signal paths to masquerade as valid users or to deliver spurious messages.
- **WLANs Can Be Jammed.** Multiple jamming techniques exist for denying service to WLAN users.
- **Low Data Rates of WLAN Segment May Reduce Availability.** When a WLAN is connected to a high-speed wired LAN, WLAN users may experience reduced system availability and grade of service.
- **Service May Not Be Available in Mobile Systems.** If the WLAN network is developed using mobile components, nulls in signal may exist and users may periodically move out of range of other users or of network access points.

### 5.2.3.7 Framework Guidance

#### User Advisory

- As discussed in Section 6.2.6, Cases (Remote Access), top secret and compartmented information on wireless networks presents extreme risk and should be handled on a case-by-case basis.
- Do not assume that either the spread-spectrum techniques used or the short communications range of the WLAN components affords any protection against signal and data interception.

- Do not develop standard timing structures for transmissions. Asynchronous operations are preferred. Noise can alternate with real data.
- Use “ping” signals to test channel availability before commencing transmission.
- Do not process classified information on a WLAN without Type 1 encryption.

## Desired Security Solution

- Secure data and header information in sensitive transmissions.
- Provide intercept/low probability of detection (LPI/LPD) of WLAN transmissions for tactical situations.
- Protect wireless network against traffic flow analysis through RF transmission patterns.
- Continuously authenticate WLAN nodes to the “parent” system.

## Best Commercially Available Solution

- PC card/FORTEZZA<sup>®</sup> card software encryption of data prior to transmission.
- Most manufacturers use the 11-bit spreading codes called for in the IEEE 802.11 specifications. However, some manufacturers have modified the selection of spreading codes by implementing a way to select a different spreading code for each transmitted symbol. Thus, an additional level of transmission security is provided.
- The RF protocol, using direct spreading, is provided to increase bandwidth, make use of unlicensed spectrum, and increase the number of users that can be accommodated. The same technology also provides a degree of LPD protection.

## Technology Gaps

- Improved spreading and/or hopping characteristics of spread-spectrum transmissions could be implemented but are not accommodated in the standards.

## 5.2.4 Paging (One-Way and Two-Way)

Paging is defined as a broadcast or a duplex (that is, one-way or two-way) communication of short messages to highly mobile users in an area where system infrastructure is available for line-of-sight transmission of the messages. Paging was originally a one-way service provided over licensed channels for delivery of numeric messages. Today, paging can be one-way or two-way, so users may receive and send multiple types of short messages to and from their portable devices.

Paging can be accomplished over many networks, such as digital cellular, PCS, packet radio, and trunked radio. References to paging in this section apply to the transmission of many types of data over many types of system infrastructure depending on the facilities available to the service

## UNCLASSIFIED

Wireless Networks Security Framework  
IATF Release 3.1—September 2002

provider. Wireless communications providers have entered the paging market to enhance revenue for unused bandwidth in their cellular systems. Paging messages are broadcast when channels are tied up with circuit-switched cellular calls.

Pagers have gained widespread market penetration, and they are currently used by a large number of customers in the government, business, and personal environments. Although paging functions have been integrated into many types of mobile user systems (primarily cellular), paging is expected to exist as a stand-alone service well into the future because of the low cost of the service and the miniaturization of the user devices. Purely numeric paging will drop in usage, but bidirectional short-message service will take up the slack. One industry leader predicts a U.S. paging market of 70 million devices by the year 2005. However, there seems to be differing opinions on the future of pagers. Many now feel that devices, which only do paging, are declining and will continue to decline.

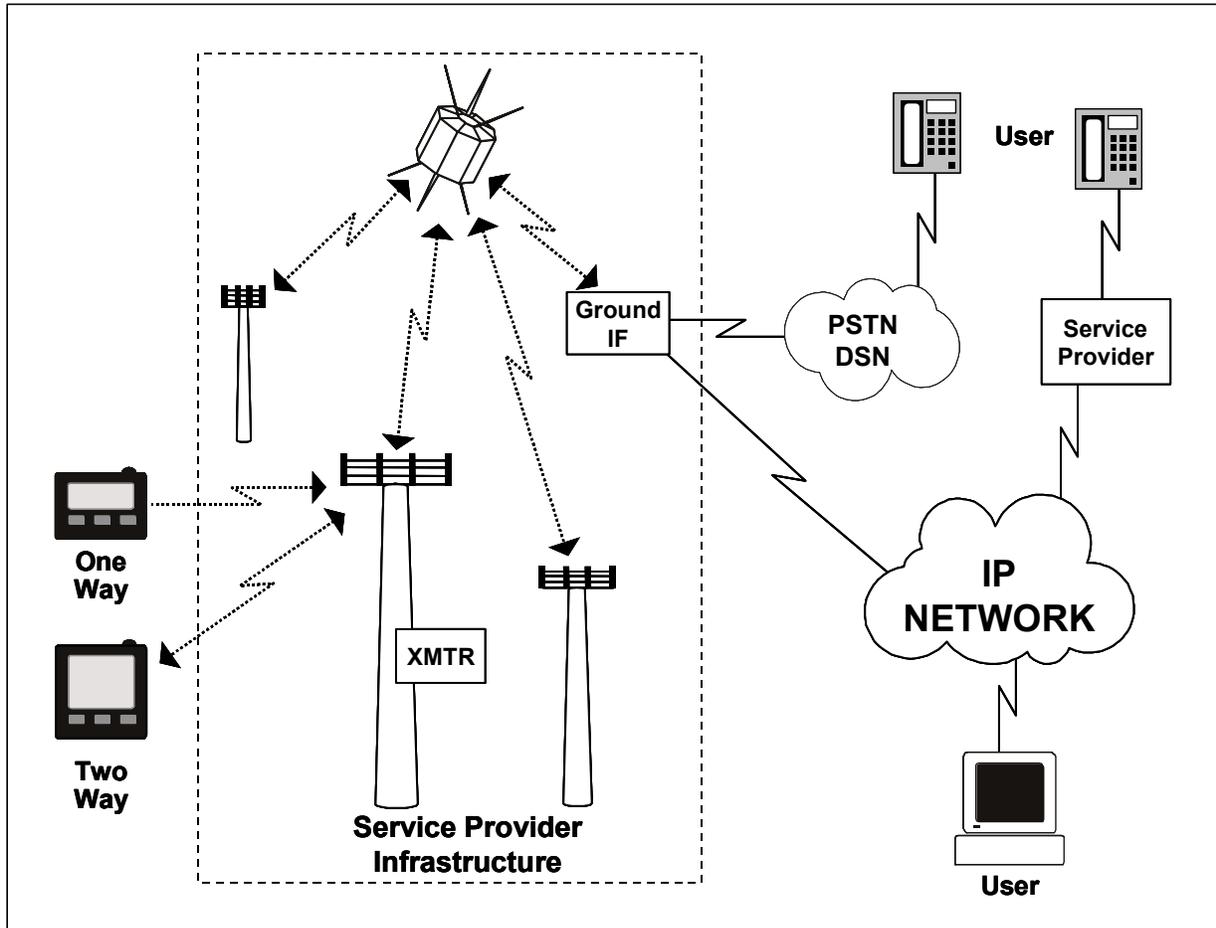
From a security and availability perspective, service provider advertising has not painted a totally accurate picture. Because each pager is identified by its own individual “cap code,” and the services are largely digital, there is a perception of message confidentiality. As presented in the news media, DoD and other federal government users have frequently become targets of pager attacks in the past. Paging is, in fact, a favorite “easy pickings” target of hackers. Primarily, the attacks have caused only embarrassment to the target organizations, but sensitive information has been involved in several cases (e.g., the location and plans of Secret Service personnel on a presidential protection mission in 1997).

In paging systems, message delivery is not guaranteed, but is largely reliable. Paging systems are designated as one way, 1.5-way, 1.75-way, and two-way. The intermediate numbers roughly describe the ability of the user device to respond to the messages and prompts. In general, the paging system does not know the location of a user, so the message is flood-routed to all areas in which the user has paid for service, thus increasing message exposure. Pagers above the one-way level are able to identify themselves to the system infrastructure so that the paging message is broadcast more selectively. The selective capability is increasing as more systems provide two-way paging. However, the basic low-cost service provided by most purely paging vendors is of the one-way variety. Battery lifetime is also a concern from an availability viewpoint; the more complex the device, the shorter the battery life.

### **5.2.4.1 Target Environment**

Pagers are used in a wide variety of environments, primarily personal and business, but also for urban police operations, emergency operation broadcasts, and even White House Secret Service communications. Two-way paging networks can be used by police in their vehicles for preliminary checks of criminal records or to perform quick driver’s license checks. Emergency operation broadcasts are used in both civilian and military environments to inform staff of the need to contact authorities. In these situations, guaranteed message delivery becomes critical, while security requirements will vary by users and particular situations. The following requirement list covers many different paging environments and will not apply to every situation.

A generalized environment for pager communications is shown in Figure 5.2-5. This environment is largely available in areas with high population density, since service providers wish to maximize the number of customers for a given (often sizable) system infrastructure investment. The figure represents cellular towers as the transmission mechanism, but this is not necessarily the case. Paging providers will often rent space for their transmitters on cellular towers (and cellular providers do use the cellular transmission media for paging), but pure paging systems use different transmitters and substantially higher power output due to the restriction of receiving sensitivity on miniaturized cellular receivers.



latf\_5\_2\_5\_0009

Figure 5.2-5. Pager Environment

## 5.2.4.2 Consolidated Requirements

The proposed requirements for paging operation are varied. The following list represents a consolidated set of functional capabilities that an advanced paging user would find useful.

### 5.2.4.2.1 Functional Requirements

- Receive telephone call-back (numeric) messages.
- Receive short text messages.
- Receive short voice messages similar to voice mail.
- Transmit short messages (numeric, text, and voice) (two-way paging).
- Provide message receipt verification to sender.
- Provide guaranteed delivery.
- Simulcast (reach multiple recipients with a single message).
- Provide confidentiality for message addresses.
- Provide confidentiality for message content over the air.
- Provide confidentiality for addresses and message content within service provider system.
- Provide indication of message receipt on mobile user device.

### 5.2.4.2.2 Networking Environments

- Both manual and automated interfaces (e.g., dial PIN and callback number) should be available at the service provider for numeric paging.
- Service providers require PSTN interfaces for message initiation.
- Various trunk (bulk transmission) media are required for distribution of messages to the over-the-air transmission sites. These can include leased satellite (as shown in Figure 5.2-5) or various land line or microwave systems (typically leased bulk data services where the provider is only concerned with delivery at the endpoints, and not the distribution path).
- The paging company/service provider requires an interface with the Internet for individuals to send messages to pager customers. Pagers interface with the Internet primarily to send and receive short messages and e-mail. Other Web services, such as traditional browsing and file transfer, are very costly because the user is charged by the number of characters downloaded every month. Pagers must maintain an emphasis on short messages to remain an affordable service.

### 5.2.4.2.3 Interoperability Requirements

- As paging technologies progress, older paging protocols are slowly decreasing in use. However, there is still a requirement for interoperability with older protocols like POCSAG.
- The Flex protocol has begun to dominate the market in the United States. Two-way paging protocols like the Motorola Reflex and Inflexion protocols are becoming de facto standards.

#### 5.2.4.2.4 Anticipated Future Requirements

- Provide confidentiality as a for-fee service element.
- Provide authentication of user to enable access to portable paging device.
- Provide authentication of message initiator.
- Increase message storage capacity of user paging devices.
- Provide interfaces with VPN.
- Provide over-the-air SMI capabilities to include user ID and key management to support confidentiality.
- Provide e-mail filtering and other message related applications.
- Provide interoperability with LEO satellite paging networks for global coverage.
- Provide interfaces to other user devices (e.g., palmtops, PCs) for message transfer and information synchronization.

#### 5.2.4.3 Potential Attacks

Pager users often do not consider the possibility that their communications might be intercepted by an eavesdropper. However, eavesdropping on pager traffic is relatively easy to do. Any individual with access to the Internet can download software and instructions on how to intercept pager traffic. Also, lists of pager cap codes, and often PINs, are published for all to see. There is a question of how sensitive the traffic sent over the paging network truly is. Traditional numeric paging simply alerts the paging customer to call a certain number. However, with the advent of text, message, and voice paging, more significant privacy and security concerns exist.

##### 5.2.4.3.1 Passive

- Intercepting pager traffic is readily accomplished, although illegal. Techniques, methods, and suggested equipment lists are posted on the Internet for any individual to read. Message traffic may be broadcast far beyond the area where the intended recipient is located due to the flood-routing algorithms used.
- Cap codes and PINs are often sent over the air to new users. An adversary can reprogram a second pager to receive all messages intended for a specific pager without being detected.

##### 5.2.4.3.2 Active

- E-mail and messages sent by Internet users are vulnerable to attack, as described in earlier sections of this IATF.

- Denial-of-service attacks through electronic jamming of the paging network in a localized area may go undetected by users.
- Spoofing techniques can be used by an adversary to send a message that appears to originate from a different location than it actually does. Without a way to validate message origin, recipients cannot be sure if they have received a valid message.

### **5.2.4.3.3 Insider**

- An insider is anyone having access to a paging service provider's database, customer personal account information, or paging equipment, whether or not this access is authorized by policy. These attacks could be motivated by deliberate malice or could be the result of unintentional mistakes on behalf of the user or service provider. Results of a deliberate attack can be especially damaging to the organization's information system due to the attacker's access to the information, his or her advantage in knowing the network's configuration, and thus the capability to exploit the network's vulnerabilities.
- A second type of insider attack involves theft of service or equipment by service provider representatives.

### **5.2.4.4 Potential Countermeasures**

- Users must be educated as to the capabilities and vulnerabilities of their pager service.
- Encryption methods can be provided for message confidentiality (net or public key).
- Authentication methods for both message initiators and recipients can be provided.
- Guarantee of delivery can be provided through use of 1.5-way, 1.75-way, and two-way paging techniques.
- AJ and LPI communications techniques can also be used.

### **5.2.4.5 Technology Assessment**

Since pagers are dependent on the RF media for message delivery, over-the-air confidentiality is a primary concern. Present packet structures for paging messages provide very little message bandwidth (on the order of dozens of bytes for older systems and hundreds of bytes for advanced paging systems). Additionally, most providers charge for their service by the byte delivered. The narrow available bandwidth creates difficulty with the overhead that is introduced for secure message delivery. Such overhead includes key distribution, synchronization, and reformatting of messages, e.g., Uencoding, for delivery over packetized networks. New technologies are continually increasing the bandwidth available to pager systems, so overhead concerns will be reduced.

One vendor has developed a pager security technique that employs over-the-air encryption and firewall wired network access. Although promising, the technique does not provide confidentiality in parts of the service provider system infrastructure.

Pagers presently have minimal storage and programming capacity to support security mechanisms. Hand held computers and cellular phones that can be programmed or provided with ancillary devices, e.g., PC cards, to provide paging service are candidates for insertion of security mechanisms, but these devices do not fit into the miniature device pager-only scenario.

Guaranteed message delivery remains an issue when a return path is not available. However, procedural methods like telephone callback can be implemented to give assurance of message receipt. In fact, telephones can be busy, and e-mails may not be delivered, so the pager scenario is not necessarily of lower assurance than other message delivery mechanisms. If message assurance is required, then two-way paging techniques can be employed at higher costs than those for one-way service.

The interfaces provided with pager devices are minimal at this point, primarily due to cost and size considerations. Offline security measures (authentication, encryption) can be considered if interfaces are provided for elements such as smart cards or CompactFlash cards. New standards for RF interfaces with miniature devices, e.g., Bluetooth, could more readily support security services.

## 5.2.4.6 Usage Cases

The usage cases for paging involve several different configurations, as shown in Figure 5.2-5. The potential use of the Internet, VPNs, or other IP-based network types in the scenario results in vulnerabilities discussed in other sections of this document in dealing with the wired network systems and system infrastructure. However, unlike the WLAN situation, the use of pagers with network connections does not necessarily increase vulnerabilities of the wired network. Pages are sent using a set of pager-unique protocols rather than IP protocols. Thus the exposure of the IP network is not as great as it would be with a WLAN connection.

As shown in Figure 5.2-5, there are three different access methods for initiation of the pager message:

- Sending party uses Internet to reach service provider.
- Sending party uses standard telephone call to reach service provider.
- Sending party uses cellular telephone to reach service provider.

The page message can be delivered under several scenarios that are service and service provider specific.

- One-way page with no response from the recipient.
- 1.5-way or 1.75-way page with limited response to the provider system from the message recipient.

- Two-way page where specific full message can be developed in response to the pager message.

When employing a pager system for sensitive and important messages, the mobile user must be aware of the characteristics of pager transmission.

- **Over-the-Air Interception of Pager Signals Has a Broad Range.** Since pager signals are broadcast to the entire coverage area of a pager system, an adversary can intercept messages from anywhere in the pager coverage area. The requirements for interception are trivial and available on many hacker Web pages. Also, in one-way paging systems, messages are broadcast multiple times to increase probability of delivery.
- **All Pager Messages Pass Through an Insecure Provider Network.** The provider may be telco connected, or connected through the Internet.
- **Message Delivery Is Often Not Guaranteed.** One-way pagers do not assure delivery, or at least do not inform the message sender that the page was not delivered.
- **Messages Can Be Stored in Low Security Environments.** Some providers will store messages for later repeated transmission if acknowledgments are not received.

## 5.2.4.7 Framework Guidance

### User Advisory

- Pagers have all of the vulnerabilities associated with over-the-air transmission, but the area of exposure is much greater due to transmission throughout the pager system.
- If reliability of pager message delivery is required, use at least a 1.5-way pager that gives a message acknowledging receipt of message. The one-way pager has no way to report message receipt.
- Digital pagers are somewhat less susceptible to attack than analog systems, but both are vulnerable to interception.
- Use the briefest message format possible. In terms of content, a numeric pager that requires a call-back is preferable to sending full messages on an alphanumeric system if the messages are not encrypted.
- Use of a standard wired telephone is preferable to the use of the Internet or a cellular phone for delivering messages to the service provider.
- At least one service provider (a team of SkyTel and V-One) provides an encryption service for over-the-air transmissions. The solution is better than no over-the-air security, but some exposure still exists within the service provider network and Internet connections.

## Desired Security Solution

- DII and certain NII customers require a higher degree of security in their pager network than is currently available. Sensitive information transmitted across a pager network should be encrypted on an end-to-end basis. This will require encryption capabilities at user terminals (i.e., the pagers). Reduced security involving over-the-air security only for message content and addressing will be suitable for privacy applications on a case-by-case basis.
- Authentication of sending party and acknowledgment of receipt are desirable characteristics.

## Best Commercially Available Solution

- Vendor solutions exist for provision of privacy-level encryption using more advanced programmable user paging devices, thus establishing a VPN environment for pager customers. However, the messages must be decrypted within the service provider network for routing purposes.
- If guaranteed delivery (or at least verification of delivery when it occurs) is a requirement, then a service provider must be selected that provides capabilities beyond the basic one-way paging systems.
- The recently announced provision of an elliptic curve public key cryptography key delivery system may assist in reducing the bandwidth overhead associated with Key Management Infrastructure functions.

## Technology Gaps

- End-to-end encryption capability with minimal overhead encoding schemes.
- Short form rekey and SMI technology for authentication and key distribution.

## 5.2.5 Wireless Local Loop/Wireless Public Branch Exchange/Cordless Telephones

Section 5.2.1 of this framework discussed a wireless telephone environment where a user with a hand-held telephone roams throughout a cell structure controlled by a cellular service provider. This section describes a similar environment, but on a much smaller scale, using what could be called a microcell or enclave structure. This section on wireless telephony defines a set of technologies and services that connect users to the wired circuit-switched telephone network using local low-power RF paths.

## UNCLASSIFIED

Wireless Networks Security Framework  
IATF Release 3.1—September 2002

The three technologies in this section have been grouped together because of the similarities in their target environments, use of technology, and protocols. WLLs can provide telephone service to remote areas where a wired infrastructure does not exist or can serve for reconstitution of communications when the wired infrastructure is damaged. Future deployment scenarios for DoD foresee the use of wireless PBXs and cordless telephone equipment in remote areas or in tactical situations. The environment and range for the wireless PBX case are very similar to those for the WLAN.

A WLL can be described as a wireless replacement for the connection between the Central Office (CO) and user switching equipment. WLLs are often used to provide telephone service to areas where laying cable is not practical because of terrain, or in remote areas where a microwave link or wireless modem is faster and easier to set up than a wired link to the CO. A typical configuration provides microcell concentrators within the local WLL service area with the RF links described above providing CO connection.

Wireless PBXs are often used in offices or manufacturing plants where individuals require mobility. A wireless PBX sets up a microcell structure where individuals carry a portable handset with them whenever they are away from their desk. Incoming calls are routed by the PBX first to users' desktop phones, then to their portable phones. In essence, the portable phone is just an extension of the desktop phone that can be used from anywhere in the site within microcell range. This setup is used frequently in applications like hospitals and large manufacturing plants. The ability to handle high user densities is what distinguishes a wireless PBX cell structure from the cellular phone system described in Section 5.2.1, Cellular Telephone.

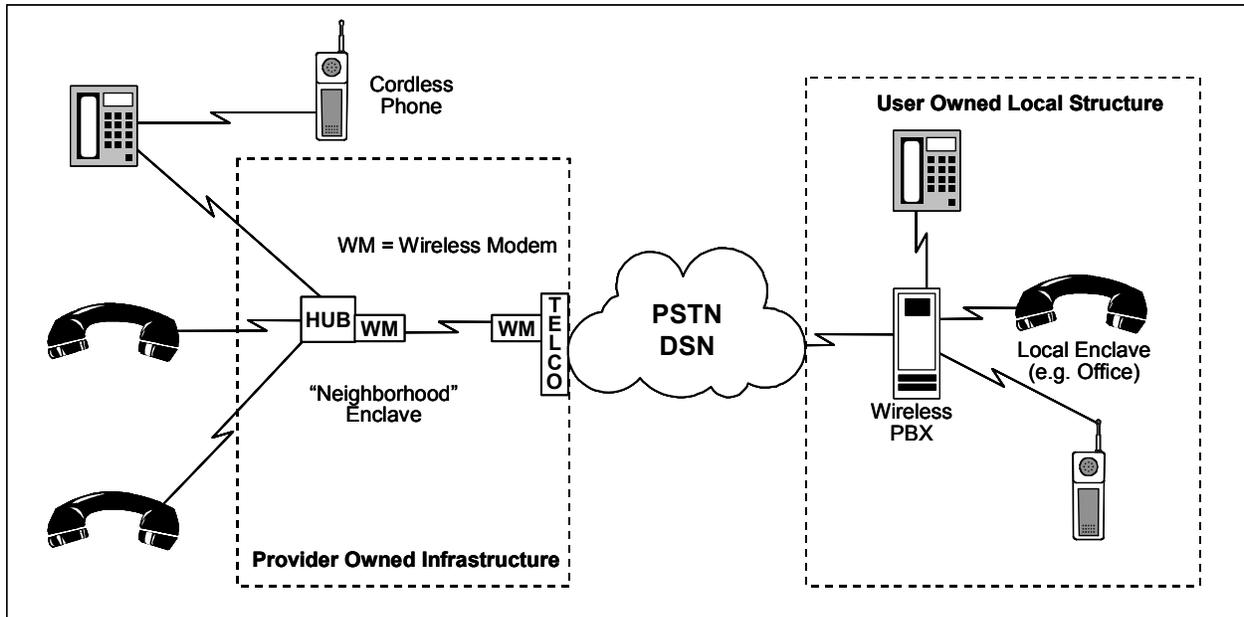
Cordless phones are the most common of these three devices, used primarily in a household or neighborhood environment. Unlike the handset used with a wireless PBX, a cordless phone is used simply as a replacement for the standard desktop telephone. Each base station interacts with a single handset. The phones also have very limited range, typically under 150 feet, but the range is expanding as new products are introduced.

### 5.2.5.1 Target Environment

Commercial application of the WLL is primarily envisioned for third-world areas or remote locations where a wired infrastructure does not exist. In government applications, a wireless PBX could be used by military personnel as a field tactical telephone system that does not require stringing of wires, or even as replacement for elements of the TRI-TAC system. Both WLL and wireless PBX systems can help forces restore sufficient telephone service to stay connected to a main operating base in the event of loss of wired communications capability as long as the forces and the main operating base are in relatively close proximity or within line of sight using wireless modem interconnection. Many other applications exist within the standard office environment for DII and NII customers, especially where other data networks interface with the wireless system in use. Security requirements in these systems vary based on the threat in the local area. Sensitivity of communications, the need for reliability, and the amount of controlled space around an area using a wireless PBX or a cordless phone will help determine the

specific threat to the user. A WLL provides for RF connections over a much larger physical area than the wireless PBX or cordless phone.

Figure 5.2-6 shows an example of how a wireless PBX and WLL could be deployed to provide telephone access in different situations. The WLL case uses a service provider system infrastructure, while the wireless PBX has a user-owned system infrastructure (again similar to the WLAN).



iatf\_5\_2\_6\_0010

Figure 5.2-6. Wireless Telephony Environments

## 5.2.5.2 Consolidated Requirements

### 5.2.5.2.1 Functional Requirements

Users/User Equipment (PBX and Cordless)

- Users must be able to make and receive dialed calls within the range of the system.
- Users must be provided with the standard features of wired telephony.
- Reliability and availability of service should be no worse than for wired system.
- Users and handsets must have assigned ID numbers.
- Handsets must be portable.

- Security of both control channel and user information channel information must be assured. The link between handset and base station must be at least as secure as the traditional wired telephone link.
- Confidentiality of user information on the “talk” channel is required.
- Confidentiality of keypad information should be provided. This function would secure credit card transactions, PINs, and other account numbers that are entered on telephone keypads.
- Confidentiality of signaling and call setup information is desired.

### **5.2.5.2.2 Networking Environments**

Converge mobile and fixed wireless capabilities into one flexible hybrid network.

### **5.2.5.2.3 Interoperability Requirements**

Wireless PBX and cordless telephone handsets should ideally be compatible with cellular telephone infrastructure.

### **5.2.5.2.4 Anticipated Future Requirements**

- In addition to telephone services, WLL will also be used to provide Internet and intranet access to distant locations at Integrated Services Digital Network (ISDN) data rates at a minimum.
- Militarized versions of commercial systems will provide end-to-end Type 1 confidentiality, call authentication, and jam resistance.

## **5.2.5.3 Potential Attacks**

### **5.2.5.3.1 Passive**

- WLL signals will typically traverse long distances on the reachback to the wired infrastructure using microwave or wireless modem systems. The signals pass across potentially hostile areas, providing easy access for an adversary.
- Wireless PBX and cordless communications have similar vulnerabilities to those discussed in the section on cellular communications. Both voice and control channel information is vulnerable to interception, although the intercept range is smaller with wireless PBX and cordless systems.

### 5.2.5.3.2 Active

- System administration for WLL and wireless PBX is typically done on a PC at the user location. System administrator functions can also be performed from remote locations through an Internet or dial-in connection. In this situation, all administrator functions are vulnerable to attack from any network around the globe. Therefore, sufficient protections must be in place to prevent unauthorized individuals from accessing the system.
- Denial-of-service attacks through electronic jamming, while easily detectable with the proper monitoring equipment, can have disastrous effects in emergency or battlefield situations.
- Spoofing attacks through changes in dialing or transmission of false messages are possible.

### 5.2.5.3.3 Insider

- Modify cordless handsets.
- Change user privileges in system administration database.
- Adjust output power control in microcells.

## 5.2.5.4 Potential Countermeasures

Several techniques are available to provide bulk encryption for WLL signals on the reachback (to the wired infrastructure) channels. Because of the high power and long distances covered with typical WLL installations, it is difficult to control where the signal radiates. Therefore, some method for encrypting this link is essential. Standard link encryption technologies (protocol independent) can serve the purpose.

For wireless PBX and cordless telephone channels, handsets and base stations can be equipped with a crypto token or smart card device to provide security between the handset and the base station. At a minimum, some sort of data scrambling or spread-spectrum modulation technique must be used to ensure that the wireless link is at least as secure as a traditional wired telephone link. Spread-spectrum techniques can also provide increased resistance to electronic jamming. Addition of a software or hardware token could be used to provide the data confidentiality and I&A required for more sensitive transmissions.

## 5.2.5.5 Technology Assessment

Several manufacturers provide WLL and wireless PBX solutions today that implement all the common telephony functions, including call waiting, call forwarding, three-way calling, and voice mail. Most of these systems are designed for the office environment and provide security features comparable to those found in cellular phone networks. Unlike cellular phone technology in the United States, wireless PBX systems primarily use one signaling protocol,

Digital Enhanced Cordless Telecommunications (DECT). DECT began as a cordless phone protocol and is now used in the United States and Europe for both cordless phones and wireless PBXs. In addition to DECT, some cordless telephones use other signaling protocols like CT-1 and CT-2. The Personal Handyphone System (PHS) is a protocol used primarily in Japan and other Asian markets.

WLL systems are still in the early stages of market deployment. As the number of products on the market increase, and users in the DII become aware of the benefits of WLL and wireless PBX systems in previously unwired urban environments, more frequent deployments of these systems will occur.

### **5.2.5.6 Usage Cases**

Other sections of this framework have addressed several cases involving connecting equipment at one classification level to equipment at the same or a different classification level across both trusted and untrusted networks. These cases are clearly an IATF issue and also apply in the wireless domain. However, use of wireless equipment interfacing with a wired network does not significantly change the cases that were previously discussed. In general, some level of communications security is recommended for any equipment where there is a connection to a potentially hostile or unknown environment. In the case of wireless communications, all transmissions can be thought of as connecting to an unknown environment because of the nature of RF transmissions and the ease of signal intercept. Thus, the descriptions of each of the specific cases addressed in this framework remain unchanged for the wireless environment. Wireless telephony calls are treated herein as system High connections to their environment.

### **5.2.5.7 Framework Guidance**

#### **Desired Security Solution**

- At a minimum for NII and DII applications, the wireless equipment must provide data security equivalent to the security provided on a wired link. Basic analog or digital modulation of a voice signal without any data scrambling or spread-spectrum modulation makes wireless transmissions easy targets for interception.
- For sensitive data, these wireless telephone systems must provide the capability to use appropriate encryption techniques for the level of information being transmitted. Implementation using hardware or software tokens for user handsets is a possible solution.

#### **Best Commercially Available Solution**

As discussed in the section on cellular telephony, the best current solutions involve using a user-carried installable token (e.g., akin to the SIM card) with a cellular GSM or PCS phone to provide user I&A. Some cellular telephones provide wireless PBX and cordless telephone handset connectivity.

## Technology Gaps

- Other than the minimal privacy provided by digital transmission of voice signals over the air, very few currently available systems provide any degree of data confidentiality or data integrity. User tokens or SIM cards could help provide user authentication and data confidentiality for cordless telephones and wireless PBXs between the handset and the base station.
- In such an obvious military application, the capability to provide ruggedized components and high-grade security is needed.

**UNCLASSIFIED**

Wireless Networks Security Framework  
IATF Release 3.1—September 2002

**This page intentionally left blank.**

## 5.3 System-High Interconnections and Virtual Private Networks

Many new options opened in recent years for providing alternative security mechanisms for protecting DoD information systems. Receiving justifiable attention are application layer mechanisms that offer end-system-to-end-system security services with stronger binding of the end user to applications than has been possible with simple password mechanisms. The problem has been that although the promise of application layer security has been very high, realization of all the benefits has been difficult. That difficulty arises from the fact that most computer platforms use operating systems that offer only minimal trust mechanisms if any at all. Since these untrusted operating systems control the computer platform resources, malicious elements of such operating systems could affect the invocation of the application layer trust mechanisms in ways that defeat the desired information assurance outcome. Moreover, the platform responds to network port operations in software processes outside the control of the higher layer security mechanisms, leaving the platform open to network attacks.

The response to this lack of strong invocation and lack of protection of the network port is that invocation of security mechanisms must be checked outside the end system. Furthermore, this checker must be the gatekeeper for whatever is allowed to pass to the end system. This gatekeeper has recently taken the form of an application layer guard that implements firewall mechanisms while performing an invocation check on all information allowed outside the protected enclave. This guard, while effective for non-real-time applications on networks with low sensitivity, has been difficult to scale to highly classified networks and real-time mechanisms. This difficulty, along with growth in the use of commercial networks by private industry, has created a renewed interest in efficiently using security mechanisms to create an effectively private network across a public backbone. This is not a new strategy for DoD. However, the renewed vigor in the pursuit of such solutions is recent. This section outlines the options available for implementing virtual private networks (VPN) and gives sufficient information to trade off the options.

Before the wide dissemination of Internet technology, networking between separate parts of an organization required a privately owned system of communications lines or leased fixed telecommunications services connecting the various entities. The number of techniques for providing communications between facilities has increased dramatically. While leasing telecommunications lines is still an option for those with specialized communications environments, there are many more cost-effective options. All major telecommunications vendors offer an on-demand virtual network service based on narrowband Integrated Services Digital Network (ISDN), frame relay, or Switched Multi-megabit Data Service (SMDS). Some vendors offer higher data rate services based on asynchronous transfer mode (ATM) technology. Some organizations are using connections over the Internet. With all of these communication methods comes some risk of exposing private information to outsiders. Each method offers varying degrees of risk and differing amounts of protection used to mitigate the risks. The purpose of this section is to explore the possibilities and to offer guidance on how information should be protected in transit across these networks.

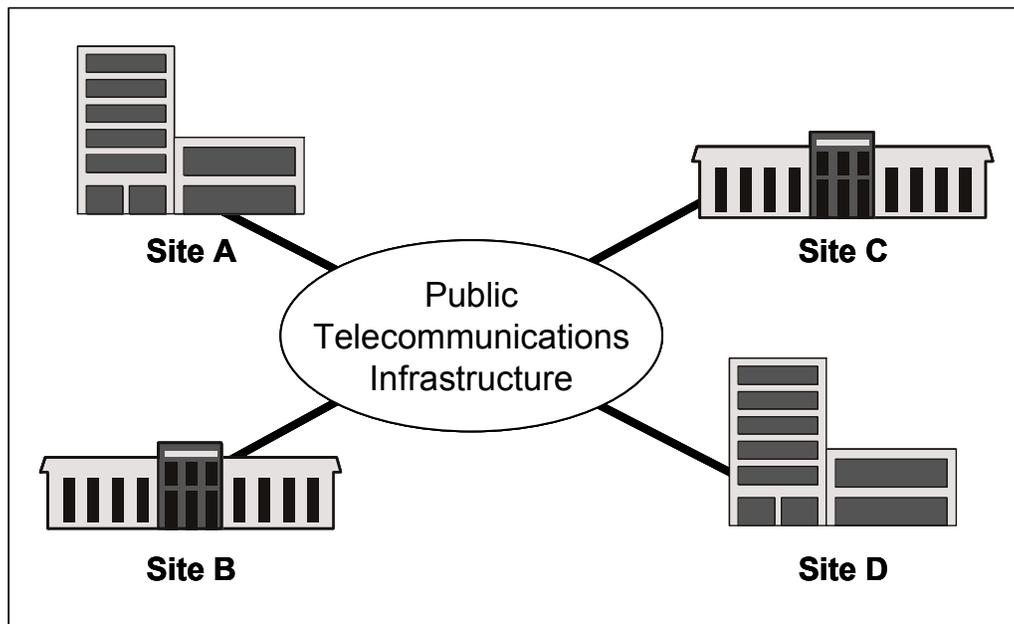
Some overlap is expected between the options presented here and in other portions of the IATF. This is particularly true for remote access of classified networks by lone users, and for high-to-low interconnect. This overlap occurs because the various forms of networking discussed here are not unique. The particular end achieved is the result of a particular implementation of the underlying techniques.

One note on terminology. Throughout this section, the term “Type 1” strength cryptography is used. Traditionally this has meant government-developed or -sponsored equipment containing security mechanisms that meet some minimum strength of implementation used where enough assurance mechanisms were in place to eliminate compromising failures. In the context that it is used here, it is generalized to include equipment from any source, provided that robust minimums of cryptographic strength and assurance mechanisms are included in the design. The exact definition of what these assurances and strengths must be is beyond the scope of this document.

### 5.3.1 Target Environment

A VPN allows the use of a public communications infrastructure in such a manner to exclude all entities outside a defined community. The communications may consist of leased lines, dial-up service, packet and cell switched connection-oriented networks, and or routed connectionless networks.

Figure 5.3-1 is deliberately vague about the type of communication infrastructure being used because a variety of infrastructures are possible.



iatf\_5\_3\_1\_0012

Figure 5.3-1. Target Environment Communications Infrastructure

**UNCLASSIFIED**

For example, the following infrastructures are among those available today:

- If the service is switched and connection-oriented, it can be frame relay or ATM.
- If it is dial-up service, it can be based on ISDN or digital subscriber line (DSL).
- If it is packet-switched and connectionless, it can be Internet or SMDS.
- If the service is leased line, it can be Digital Service, Level Zero (DS-0), DS-1, Fractional DS-1, Burstable T-1, DS-3, Synchronous Service Transport, Level Three (SST-3), or higher rates in North America. Table 5.3-1 provides additional information for each these.

**Table 5.3-1. Digital Service Standards**

Digital Standards	Definition
DS-0	In the digital hierarchy, this signaling standard defines a transmission speed of 64 Kbps. This is the worldwide standard speed for digitizing one voice conversation; (i.e., converting one analog voice channel into a digital signal. It is derived from using pulse code modulation (PCM) and sampling the voice channel 8,000 times a second. This signal is then encoded using an 8-bit code. Thus, 64,000 bps is derived from 8-bits times 8,000 times per second.
DS-1	In the digital hierarchy, this signaling standard defines a transmission speed of 1.544 Mbps. A DS-1 signal is composed of 24 DS-0 channels. DS-1 is often used interchangeably with T-1, which is the U.S. equivalent of E-1. T-1 is a Bell system term for a digital carrier facility used for transmission of data through the telephone hierarchy at a transmission of 1.544 Mbps. E-1 is the European equivalent of a T-1 circuit. E-1 is a term for digital facility used for transmitting data over a telephone network at 2.048 Mbps.
Fractional DS-1	A DS-1 circuit in which a fraction of the 24 DS-0 channels are used; (i.e., between 64 Kbps and 1.536 Kbps. If a full DS-1 circuit is 24 DS-0 channels at 1.544 Mbps, a $\frac{1}{8}$ fractional DS-1 is four DS-0 channels at 256 Kbps, a $\frac{1}{2}$ fractional DS-1 is 12 DS-0 channels at 768 Kbps and $\frac{2}{3}$ fractional DS-1 is 16 DS-0 channels at 1,024 Kbps.
Burstable T1	This service is a billing scheme. It is an unshared, non-fractional T-1 line running at 1.544 Mbps. While a DS-1/T-1 customer has the full capacity of the line (24 DS-0 channels at 1.544 Mbps) any time it is needed, the customer is billed only an average usage computed from periodic samplings of the input and output data rates on the link.
DS-3	In the digital hierarchy, this signaling standard defines a transmission speed of 44,736 Mbps. A DS-3 signal is composed of 673 DS-0 channels. DS-3 is often used interchangeably with T-3, which is the U.S. equivalent of E-3. T-3 is a Bell system term for a digital carrier facility used for transmission of data through the telephone hierarchy at a transmission rate of 45 Mbps. E-3 is the European equivalent of a T-3 circuit. E-3 is a term for a digital facility used for transmitting data over a telephone network at 34 Mbps. Also available is a fractional DS-3 service in which a fraction of the 28 DS-1 channels are used; i.e., between 1.544 Mbps and 43,232 Mbps. Other digital service levels are available; e.g., DS-2, 96 DS-0 channels at 6,312 Mbps; DS-4, 4,032 DS-0 channels at 274,760 Mbps.

UNCLASSIFIED

Digital Standards	Definition
SST	This is a SONET-based, private line transport product that offers high-capacity channels for synchronous transmission at transport line rate from 155.52 Mbps to 2,488 Gbps. It enables the interfacing of asynchronous networks with synchronous networks.
DSL	<p>DSLs are point-to-point public network access technologies that allow multiple forms of data, voice, and video to be carried over twisted-pair copper wire on the local loop between a network service provider's central office and the customer site. Included are asymmetric digital subscriber line (ADSL), rate-adaptive digital subscriber line (R-ADSL), high bit-rate digital subscriber line (HDSL), single-line digital subscriber line (SDLS), and very high bit-rate digital subscriber line (VDSL). Collectively, the DSL technologies often are referred to as xDSL. ADSL is an xDSL technology that allows more bandwidth downstream—from a network service provider's central office to the customer site—than upstream from the subscriber to the central office. ADSL is ideal for Internet/intranet surfing, video-on-demand, and remote LAN accesses. R-ADSL is an xDSL technology that adjusts dynamically to varying lengths and qualities of twisted-pair local access lines. R-ADSL makes it possible to connect over different lines at varying speeds. HDSL is an xDSL technology that is symmetric, providing the same amount of bandwidth both upstream and downstream. Due to its speed—1.544 Mbps over two copper pairs and 2.048 Mbps over three copper pairs—TELCOs commonly deploy HDSL as an alternative to repeated T-1/E-1 lines. SDLS is an xDSL technology that provides the subscriber only one DSL line. VDSL is the fastest xDSL technology, supporting a downstream rate of 13 to 52 Mbps and an upstream rate of 1.5 to 2.3 Mbps over a single copper-pair wire. Maximum operating distance for this asymmetric technology is 1,000 to 4,500 feet. The VDSL bandwidth could potentially enable network service providers to deliver high-definition television signals in the future.</p> <p>Note: TELCO is a generic term for local telephone company operations in a given area.</p>

No matter what the underlying communications scheme, the desired result is to connect separate pieces of a larger organization in a manner that provides unimpeded communications between the pieces of the organization, denies access to the information within the pieces by any outside organization, and provides for the privacy of information as it traverses the public infrastructure.

Many people make the assumption that a VPN is a distributed enterprise network connected across a public Internet but separated from that Internet by an encrypting firewall. This use of the term precedes the definition of Internet Protocol Security (IPSec) that is the basis of the present generation of encrypting firewalls. The three major telecommunications carriers offer a virtual private networking service that combines voice and data features, billing, access, screening, and rerouting capabilities but does not have any inherent encryption mechanism.[1] This chapter uses a broader definition of VPN that encompasses any means of using public communications infrastructure to manifest an apparently private network.

In the context of this IATF, there is little difference between a system-high interconnect and a VPN. Possibly the only real difference is that the end systems have implemented a private network with an wholly owned infrastructure or the end systems use a shared backbone based on some publicly offered service. Although some state that use of a provisioned service like DS-3 or Synchronous Optical NETWORK (SONET) is a system-high interconnect, these services are

multiplexed onto a public backbone, managed by a public entity, and the routes can slowly change in response to some network conditions. Therefore, even this type of networking represents the creation of a VPN across a public switched backbone.

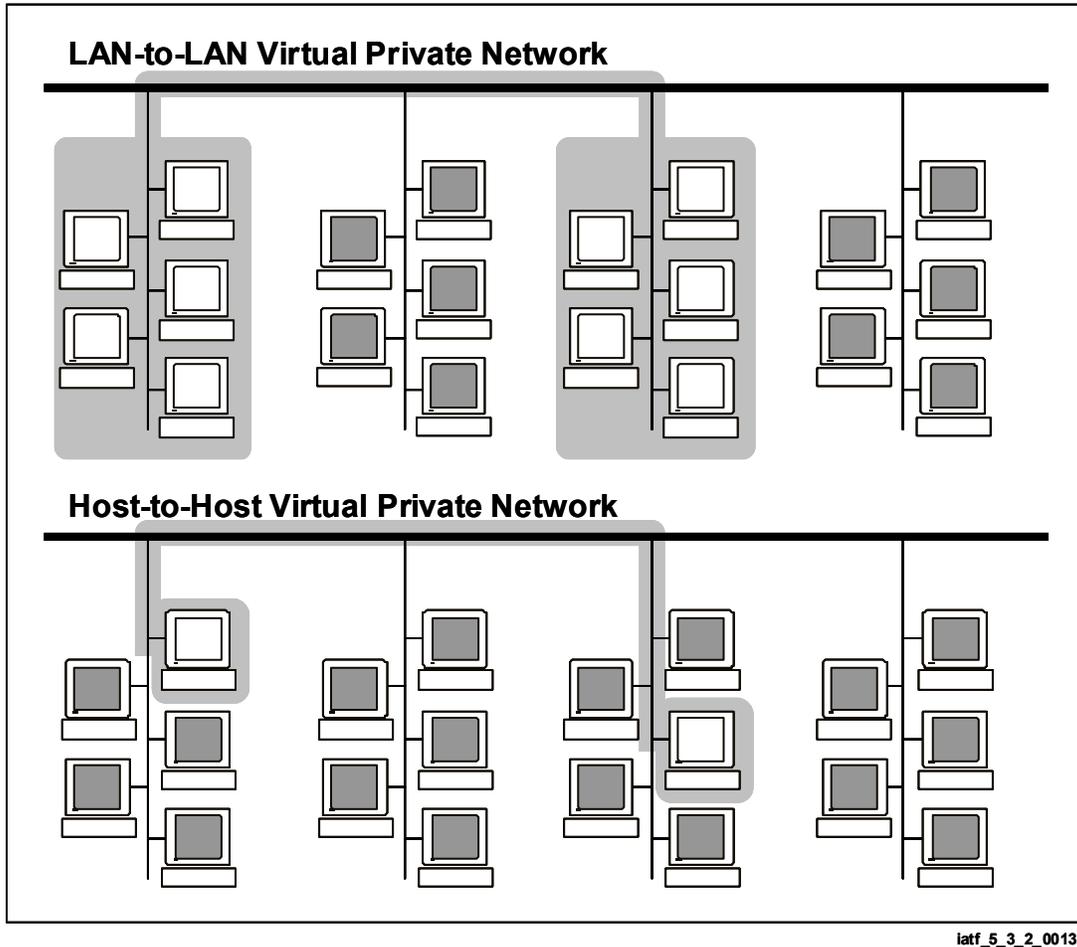


Figure 5.3-2. Local Virtual Private Network Architectures

## 5.3.2 Consolidated Requirements

The present requirements are derived from operating scenarios of present system-high networks based on use of leased line services and on an interconnect model that uses the Internet.

Anticipated requirements are derived from plans for the far-term Defense Information Systems Network (DISN), technology developments from Defense Advanced Research Projects Agency (DARPA) and the Global Grid community, plans stated by telecommunications vendors, and aggressive research and development (R&D) networks such as those pursued under the Nuclear Stewardship Program.

### 5.3.2.1 Functional Requirements

Near-term functional requirements are as follows:

- Must support connection of separated entities across public infrastructures (site-to-site model) or within private facilities (Local Area Network [LAN]-to-LAN or host-to-host model).
- Must support classified operations or unclassified operations.
- Must support standards-based network operations.
- Must keep network information confidential and integral while in transit.
- Must prevent entities outside the private facilities from gaining access to those facilities.
- Must use techniques that support scalable communications rates from kilobit per second rates to OC-192 (10 Gbps) and beyond.
- Must transport primarily data including voice, video, imagery, and data.
- Must optionally provide data integrity.

Mid- to far-term functional requirements are as follows:

- Must support quality of service in the telecommunications being supported.
- Must support data rates for specialized applications that exceed 13 Gbps by the middle of the next decade.
- Must support information that is mixed voice, video, and data.
- Must connect nonuniform security policies. As more risk management philosophies are developed for administering security within network domains, security policies can be expected to diversify even within similar classification levels of networks. These discrepancies will result in additional security requirements on VPN architectures.

### 5.3.2.2 Networking Environments

This section serves as a local reference regarding environments in the context of the virtual private networking arena.

Two networking environments are currently dominant. The first is link layer connection over leased lines and the second is Internet Protocol (IP) packet routing over the Internet or ATM wide area networks. Although frame relay and SMDS technologies have made significant inroads into the business community, they have been used rarely for classified communications. This has been attributed in part to the lack of native mode security systems for these means of

communication but also because there have been alternative means of achieving security services that could be used without affecting the functionality of the network.

Networking environments will undergo drastic changes over the next few years. With this revolution will come an explosion in the number of networking technologies. Although the IP and provision networks of today will not disappear, they will be joined by newer technologies and by variations of the old technologies. The present IP version 4 will evolve to incorporate bandwidth reservation schemes in an attempt to add quality of service attributes to deliver business-quality voice and video applications over the Internet. Other users will move to ATM networks because they are designed to deliver quality of service for these same applications. A war for market share will ensue between these networking technologies. The outcome of this battle is not clear. Currently, neither technology fully achieves all of its promises. The expected result will likely be a coexistence of these technologies.

As wireless network technologies evolve, there is likely to be a specialization of IP for the mobile environment that will require some level of gateway to the wired portion of the Internet.

Speeds of connectivity will increase. The maximum available today in a standardized format is an STS-48/STM-16 signal at 2.5 Gbps and some initial deployment of an STS-192/STM-48 signal at 10 Gbps. These signals will be wavelength division multiplexed up to 40 and 80 Gbps. The affordability of such large bandwidths is certainly a major issue. However, a few programs have identified communications requirements of greater than 10 Gb/s. The most easily referenced example is Department of Energy's (DOE) Nuclear Stewardship Program. To support simulations of aging effects in stockpiled nuclear weapons, it is estimated that computational capacities of 0.1 Petaflops are required, backed by 13 Gbps communications between the DOE weapons laboratories.

### **5.3.2.3 Interoperability**

A trend within the DoD is to break down barriers to connectivity rather than put more barriers in place. As a result, the natural segregation that would occur between entities in different communications environments, between entities communicating at different rates, and between those entities using different networking architectures is breaking down. Therefore, one must assume that a secure means of exchanging information between the various networking architectures is required.

Another interoperability issue is the DoD trend toward breaking down barriers between networks operating at different levels of classification and assurance. Although, this is a multilevel security problem and not a virtual private networking issue, the solutions must be mutually supportive.

### **5.3.3 Potential Attacks**

The attacks listed here are those primarily of concern to systems protected at network layers and below. One interesting paper, although written primarily about a particular implementation of

IP-based security, presents an open tutorial of many issues that must be considered when implementing network layer security solutions. [1] Although, the author often assumes that an adversary already has access to a private resource and therefore presents a pessimistic picture, the subject matter at least considers many security issues that are often ignored. This paper is used as a reference throughout this section.

Attacks against networks vary greatly regarding the techniques and results. While some try only to uncover private information, others try to disrupt operations, disseminate misinformation, and gain access to resources.

### 5.3.3.1 Passive Attacks

The primary concern with passive intercept attacks is the loss of information confidentiality while in transit across the network. Basic privacy rules to prevent inadvertent disclosure are insufficient for DoD. Recent reports show that cryptanalytic capability is available in the public domain as witnessed by the June 1997 collaborative breaking of the 56-bit strength Data Encryption Standard (DES). Although, the near-term threat to large volumes of traffic is questionable given the number of machines and hours involved, it does show the vulnerability of any single transaction. Therefore confidentiality mechanisms must pass some measure of minimum strength to be acceptable. However, that is not the only concern. Some military operations require the element of surprise. Therefore, one must assess the possibility of passive observation of network operations giving indications and warnings of impending actions. Such indications may be the identity of the end parties in an information exchange, a change in the volume of traffic or traffic patterns, or the timing of information exchanges in relationship to external events. The resulting potential security requirements are strong confidentiality and traffic flow security.

### 5.3.3.2 Active Attacks

This class of attacks may involve end systems or infrastructure. The most obvious network-based attack is the attempted login to a private computational resource. Bellovin shows how the ability to splice messages together can be used to change information in transit and cause desired results.[1] In the financial community, it could be disastrous if electronic transactions could be modified to change the amount of the transaction or redirect the transaction into another account. Reinsertion of previous messages could delay timely actions. Bellovin also brings up the issue of chosen plain text attacks<sup>1</sup> that can be used to bypass encryption mechanisms. [1]

Denial of service (DOS) attacks can be minimized by choice of network technologies. Any network that supports dial-up connections or routing of information can be used to deny service by flooding an end point with spurious calls or packets. More sophisticated attacks can involve manipulation of network elements.

---

<sup>1</sup> Many attacks are aided by making a machine encrypt plaintext chosen by the attacker. Many cryptanalytic attacks depend on the attacker being able to choose the plaintext to be encrypted. [1]

The following are resulting potential countermeasures.

- Strong access control.
- Continuous authentication.
- Integrity of information.
- Replay prevention.
- Network availability.

### 5.3.3.3 Insider Attacks

Many insider attacks are possible in a VPN. This is an architecture that concentrates on control of outside access. There is no additional mechanism to inhibit a person with legitimate access to a system from accessing more private areas of the VPN. A malicious insider could use covert channels to signal private information outside the VPN. However, there are many other avenues for a malicious insider to wreak havoc with an information system. Another threat that must be considered is the introduction of malicious code into a protected enclave. Such code can be easily imported through shrink-wrapped untrusted software, users swapping media with machines outside the enclave, or other paths that are implemented to import information from outside the VPN. Although many precautionary security requirements could be taken that are outside the scope of the virtual private networking scenario, the resulting potential security requirements for the VPN are establishment of security domains within the VPN and control of covert channels.

### 5.3.4 Potential Countermeasures

Privacy is maintained by appropriate use of confidentiality mechanisms. While application layer mechanisms can provide information confidentiality for classified and other critical applications, the problem with assured invocation of these mechanisms makes it difficult for these mechanisms to provide primary confidentiality mechanisms. The strength of confidentiality mechanisms for classified applications must be sufficient to withstand national laboratory strength attacks.

If traffic flow security is required, the best mechanism is one that prevents all insight into changes in traffic patterns. Therefore, the best mechanisms are link layer mechanisms on constant bit rate leased lines. Alternatively, lesser degrees of traffic flow security can be afforded by aggregating traffic through secure tunnels and by using traffic shaping mechanisms.

Many network attacks that involve manipulating cipher text or splicing information units can be countered by strong data integrity mechanisms and continuous authentication of the data channel. Replay can be prevented with cryptographic mechanisms that use timestamps or incrementing of counters to limit the acceptability of prior messages in the end systems. Continuously authenticated channels can prevent insertion of information into the channel. Such insertions could permit short plaintext attacks that would allow cryptanalysis by guessing known responses to known short messages.

Prevention of DOS attacks is often in the hands of the network provider. Use of provisioned networks will prevent many DOS attacks because the general population is unfamiliar with the management mechanisms in networks. However, there is little in present infrastructures to prevent manipulation of network hardware. The router authentication being implemented in the DISN is a start toward decreasing the vulnerability of networks to manipulation of network management information. Similar moves are being proposed within the Security Working Group of the ATM Forum for control of ATM switch configuration messages. Neither of these techniques is widespread so the network remains vulnerable to hacking.

Virtual private networking architectures provide little protection against the insider threat. Malicious insiders or malicious code introduced into the network all operate above network layers. These threats must be handled by higher layer services. If insider threats are a concern, the security implementation should also consider inclusion of firewalls, end-system-based privacy mechanisms, and protection mechanisms over the wide area network that limit exposure to covert channels.

## 5.3.5 Technology Assessment

There are many ways to implement a secure VPN. The easiest method for categorizing the options is to look at the possibilities as one moves up the protocol stack in a network. For purposes of this IATF, the discussion starts at link layer protocols where framing can take place. This is the lowest layer that can be transported through a standardized public infrastructure. The discussion stops at the transport layers. It should be noted that transport layer security services normally could only exist in end systems unless, at some future point, a transport layer proxy is created in a gateway device.

### 5.3.5.1 Layer 2 Protected Networks

The option of protecting a network at layer 2 is possible only if the owner has installed or leased a dedicated communications facility between sites. The security services that one achieves with a layer 2 protected network are strong site-to-site authentication, confidentiality, and a continuously authenticated channel. In most cases, one also achieves traffic flow security. An optional security service may be some data integrity functions or at least an antispoof capability.

A layer 2 protected network, given present protocol suites, cannot provide any true end-user authentication. It cannot provide any degree of privacy between users within the protected network at a reasonable expense. All switching and routing facilities will be Red facilities unless supplemented by other security mechanisms. This option contains no provisions for limiting information flow between facilities. If a firewall or equivalent function is required, it is inserted before the link encryption mechanisms.

Given the limitations outlined above, layer 2 protection for networks could easily be dismissed as not useful. However, some security mechanisms cannot easily be used in higher layers. The first mechanism is traffic flow security. If a user is concerned about receiving indications and warnings about impending actions, traffic flow security is imperative. Although, some traffic

flow security is possible using rate shaping of information, this technique requires nonstandard applications and protocol stacks, which could entail significant life-cycle costs.

The second mechanism not available in higher layer is the limitation in the number of covert channels. Covert channels are often viewed as either the gravest of threats to our information systems or a hobgoblin to be dismissed with a wave of the hand. The reality is that accreditors must have to evaluate the threat of covert channels to their particular information system and determine the desired level of protection against the threat. Although, a detailed discussion of any of these vulnerabilities is outside the scope of this paper, it does not take too active an imagination to postulate the existence of covert channels given that any field in a packet that can be modified or any parameter of transmission that can be varied is a potential covert channel. A layer 2 protected network removes all covert channel classes encompassing length of information transfer, timing of information transfers, and addressing of information transfers. Remaining covert channels can arise from the ability to exploit incompletely defined transport overhead and will be stemmed by the ability to control access to the overhead.

Another desirable property is that the simplicity of the design of link layer systems means that it is easier to achieve a target throughput at the link layer than at any other layer. As users reach for the limits of available communications technologies, it is more likely that a link layer solution will be the most acceptable solution. Table 5.3-2 summarizes the positive and negative characteristics of layer 2 protected networks.

**Table 5.3-2. Characteristics of Layer 2 Protected Networks**

Positive Characteristics	Negative Characteristics
Highest speeds possible	Highest communications costs
Highest protection against traffic analysis	No protection against cascading of networks
Highest protection against covert channels	No protection against insiders
Fewest avenues for network-based attacks	Can only authenticate from site to site
Continuous site-to-site authentication	Requires carrier to reconfigure network to add new nodes

- 1) **SONET.** SONET is the standard in the United States for trunking of data at rates greater than 45 Mbps. It is delivered in multiples of 51.84 Mbps with the minimum multiple being three. This service is referred as a synchronous transport signal 3 (STS-3.) If the entire capacity is treated as a single data container, the service is referred to as STS-3c, where the c denotes a concatenated service. The international version of this service is Synchronous Digital Hierarchy. The basic unit of service is a Synchronous Transport Multiplex, which is the equivalent of the SONET STS-3c transport. Present widespread deployment supports 155, 622, and 2488 Mbps transmission rates. Initial deployments of SONET at 9952 Mbps have occurred. Approximately 3.33 percent of the data flow is devoted to transport overhead. Another 1.11 percent is devoted to path overhead in nonconcatenated channels.

Presently, only government-developed equipment is available to secure SONET

## UNCLASSIFIED

System-High Interconnections and Virtual Private Networks (VPN)  
IATF Release 3.1—September 2002

networks. SONET key generators encrypt the data payload providing for strong confidentiality and complete traffic flow confidentiality. Data integrity must be handled at higher layers. SONET overhead passes through the system unaltered or, alternatively, only minimum fields are passed through the system undefined and network control channels are cleared. The operators of local SONET networks decide the level of transport overhead flow between local and wide area environments. A commercial device has been developed to meter these interactions between local and wide area SONET networks but the future of the device is not certain. No known commercial SONET encryptors exist at this time. However, a commercial entity has expressed interest in providing services based on such a device.

- 2) **Sub-SONET Rate Services.** The widespread data trunks in the United States are fractional DS-1, DS-1 at 1.544 Mbps, and DS-3 at ~ 45 Mbps. These services represent a multiplexed hierarchy for combining 64 Kbps voice channels into higher order trunks and eventually into SONETs adapted to direct transport of nonvoice data. The transport overhead varies from 1.4 percent for DS-1 service to 3.9 percent for DS-3. Trunk services are protected by a series of standard government-developed encryption equipment. These encryptors have been the basis of numerous VPNs based on provisioned services. In addition, numerous commercial offerings have seen a limited success in the marketplace. Commercial link encryptors are ripe for evaluation for possible use in layer 2-protected VPNs. Similar to the SONET devices described above, such link encryptors provide strong confidentiality, continuously authenticated channels, and traffic flow protection. They may also provide data integrity based on error extension properties of the encryption mechanism.

An interesting alternative to securing constant provisioned services is to apply an ATM-based solution. Because ATM can transport constant bit rate services, it is possible to use a cell-encryption-based technology to provide encryption services for link layer protocols. Many technical issues must be considered in the actual implementation of this technique. Among others, how the physical link is manifested at the service access point and relative costs are important considerations. Such a solution may not have all the security properties of traditional link encryptors. A discussion of the security properties of ATM will be included in a later release of this document.

- 3) **N-ISDN.** Narrowband Integrated Services Digital Network (N-ISDN) is a digital data transport system. It can be supplied in several forms including basic rate and primary rate services. Basic rate service consists of two data channels and one signaling channel with a combined capacity of 144 Kbps. In the United States, primary rate service consists of 23 data channels and 1 signaling channel for a total capacity of 1.544 Mbps. Europe and Japan use a different standard for primary rate service. Government equipment is being designed for N-ISDN. This device was initially prototyped as a single data channel and a single signaling channel and has since been followed with a version with two data channels and one signaling channel. No known commercial devices exist for native N-ISDN security. Security services available for N-ISDN depend on how security is invoked. Security can be implemented by encrypting complete data channels. Such an implementation would have security properties similar to the link

## UNCLASSIFIED

System-High Interconnections and Virtual Private Networks (VPN)  
IATF Release 3.1—September 2002

encryption devices discussed above. N-ISDN can also be used for multiplexed data transport. In fact, this transport is the basis of the commercially successful frame relay service offered by many carriers. If security is invoked at this layer, security properties will be the same as those discussed in the layer 3 section to follow.

N-ISDN is used as a low bandwidth connection between end systems and as a medium speed dial-up temporary connection between fixed and mobile systems. Direct dial-up secure N-ISDN represents a reasonable protection for dial-up access into a secure enclave, provided that policy allows such connections, strong user authentication is invoked, and procedures are put in place to protect classified information on a remote system while outside a protected enclave.

- 4) **Analog Phone Service for Data Transport.** Analog phone service requires a digital modem for transport of information across the analog link and is available as a dial-up medium for low bandwidth temporary connections. Newer modem technologies represent nearly the same capacity as an N-ISDN data channel without the set up charges and communications cost associated with N-ISDN. Commercial prototype encrypting modems have been developed for such secure data connection use and represent a reasonable method of providing a temporary link to a VPN, provided that strong user authentication is part of the connection process.

An alternative to the encrypting modem is the use of the data port of the government-developed secure telephones. Part of the authentication scheme for government secure voice equipment is the voice recognition between speakers. A totally automated system could bypass this important function. Many dial-up functions in low-cost computers accept manual dialing. A possible security policy would be to require audio identification of the sender before going secure or to require an augmenting strong authentication during log-in.

- 5) **Voice Transport.** Voice networks are often disregarded by the data network community, but in the DoD they still carry a large volume of secure traffic. Modern secure phones are based on digital representations of voice that are encrypted and sent across the network by digital modem. This is true whether the end system is connected to an analog service like Plain Old Telephone Service (POTS) and analog cellular service or a digital service like N-ISDN or newer digital cellular technologies. The distinction between voice networks and data networks is expected to diminish in the next few years. N-ISDN, ATM, digital cellular, and Internet phone are already blurring the lines. Government secure voice architectures have unified secure interoperability across most voice transport mechanisms. The exceptions to this rule are Internet Phone and native ATM voice transports. An area ripe for work is the extension of secure voice architectures into these newer network technologies.

### 5.3.5.2 Layer 3 Protection Across Public Networks

Layer 3 networks support dynamic routing and switching of information. For the purposes of the IATF, this discussion primarily covers IP and ATM transport. For this reason, the discussion is not complete. Network protocols like Network Basic Input/Output System (NETBIOS) and Internet Packet eXchange (IPX) are not covered. In addition, ATM spans a range of network layers. If implemented as a permanent virtual circuit, it becomes a strict layer 2 entity. In many implementations, ATM is used below layer 3 but above the Media Access Controller becoming the equivalent of about a layer 2.5 entity. Prototype applications are capable of completely replacing layer 3 solutions. Because of the cell switched nature of ATM, it is closer in properties to the pure layer 3 solutions and is therefore handled in this section. A protection philosophy based on layer-3-type networks offers the end users more affordable communications costs than layer-2-protected systems. A layer-2-protected system requires the provisioning of a new communications line and the acquisition of a pair of protection devices enables the new connectivity. With a layer-3-protected system, one only has to enable the access control mechanisms to allow the new connectivity. This comes at a cost of a higher risk of vulnerability to traffic analysis and the exposure to covert channel problems and directed network-based attacks. Table 5.3-3 summarizes the characteristics of layer-3-protected networks.

**Table 5.3-3. Characteristics of Layer-3-Protected Networks**

Positive Characteristics	Negative Characteristics
Some billing models charge by volume of traffic allowing greatest control of cost	Traffic analysis easy under some configurations
Most flexibility in adding new nodes to network	No protection against cascading of networks
Continuous site-to-site authentication possible	No protection against insiders
	Many covert channels for exploitation
	Many DOS attacks possible under some implementations

### IP Network

Only one widespread Type 1 system provides layer 3 protection for networks—the Network Encryption System (NES). This system uses a security protocol called SP-3 to encapsulate and transmit information securely across the Internet. NES has its own unique IP address and a broadcast address. When information is encapsulated, the outer IP envelope contains only gateway-to-gateway addresses. Therefore, end system identity is not available on the public Internet.

For this method to work, the device contains a configuration table that maps end system addresses to gateway addresses. The security services provided are site-to-site confidentiality, site-to-site authentication, and site-to-site integrity. Traffic flow protection of the aggregate data flow is not provided, although it is possible to write specialized applications whose purpose is to smooth the traffic flow across a site-to-site flow.

## UNCLASSIFIED

System-High Interconnections and Virtual Private Networks (VPN)  
IATF Release 3.1—September 2002

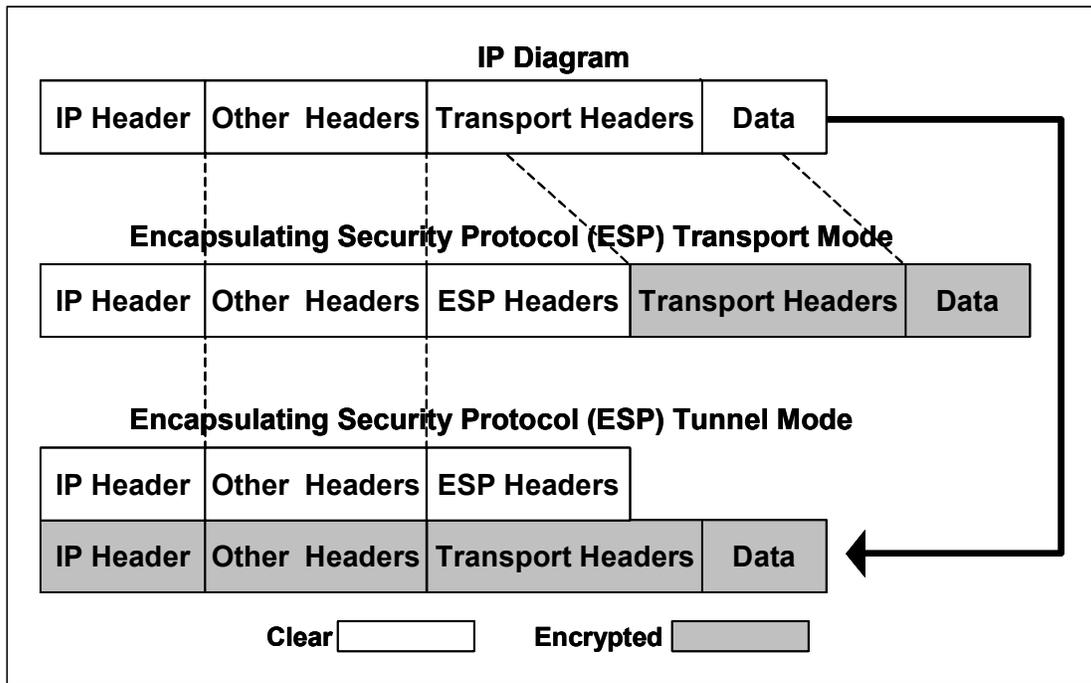
Numerous commercial IP encryptors also exist. These older commercial systems tend to have many proprietary features that preclude interoperability of equipment. Because of this lack of interoperability, it is not recommended that older commercial IP-based encryption systems be studied for securing DoD systems. For immediate applications requiring a layer 3-protection mechanism in support of the flow of classified information, NES is the only available solution.

There is potential for a widespread IP layer encryption solution based on what has been called IPSec. IPSec is the security framework that has been standardized by the Internet Engineering Task Force as the primary network-layer protection mechanism. IPSec consists of two parts, an Authentication Header (AH), whose purpose is to bind the data content of IP frames to the identity of the originator, and an Encapsulating Security Protocol (ESP) for privacy. The AH is intended to be used when integrity of information is required but privacy is not. ESP is intended to be used where data confidentiality is required. The draft Request for Comments (RFC) that defines IPSec architecture states that if data integrity and authentication are required with confidentiality, then an appropriate security transform should be used that provides all services. The minimum set of protection mechanisms consists of the DES for confidentiality and the hash algorithm MD-5 for authentication. The standard does provide room for negotiating alternative protection mechanisms through use of the Internet Key Exchange Protocol (IKE). IKE provides both a framework for creating security associations between endpoints on a network and a methodology to complete the key exchange. At least one published paper points out potential security concerns about using IPSec default security mechanisms. [1] The author points to occasions where the integrity functions of DES in Cipher Block Chaining mode can be circumvented with the right applications by splicing of packets. [1] The referenced paper recommends that AH and ESP be used together instead of individually.

ESP defines two methods of encapsulating information: tunnel mode and transport mode. Tunnel mode, when used at an enclave boundary, aggregates traffic flow from site to site and thereby hides end system identity. Transport mode leaves end system identity in the clear and is most advantageous when implemented at the end system. Figure 5.3-3 shows where the ESP header is placed within an IP datagram for IP version 6. In the more ubiquitous IP version 4, the section marked Other Headers does not exist. The AH precedes all nonchanging end-to-end headers. If one wanted to follow Bellovin's suggestion and use AH with ESP, the authentication header must immediately precede the ESP header. [1]

Although, no government-sponsored equipment currently implements IPSec, one such device is under development. TACLANE is an IPSec and ATM encryptor that is certified to handle classified information. It uses the ESP tunnel mode without the AH. It also does not implement the default IPSec algorithms of DES and keyed MD-5, because hard-wired security policy states that DES and MD-5 are not strong enough for Type 1 grade security. TACLANE always negotiates to higher-grade security mechanisms or does not commence data transmission. A follow-on development for the TACLANE program will provide fast Ethernet cards for TACLANE and increase its encrypted IP throughput to 100 Mbps.

It is recommended that all future IP security equipment be IPSec compliant. The primary confidentiality mechanisms should be implemented in security gateways that support no user-level processes.



iatf\_5\_3\_3\_0014

**Figure 5.3-3. IP Layering Encryption Methods**

No Type 1 grade IPsec-compliant commercial encryptors exist. Even in current government developments, there are technology gaps for devices that can handle full Ethernet bandwidths, 100 Mbps Ethernet bandwidths, and Gigabit Ethernet bandwidths. In the commercial arena, there are many IPsec implementations for individual end systems and for firewalls. Both of these implementations will require Type 1 grade equipment.

## ATM

ATM security was developed in anticipation of requirements for high quality multimedia communications. The flexibility of the transmission mechanism makes it possible to tailor the security features of the system depending on how ATM is used. The standardization process for security in ATM is not as well established as that for the IP community, although some basic features and cryptographic modes have been defined through the Security Working Group of the ATM Forum.

Some of the main differences between ATM and IP include the following. ATM relies on a call set-up mechanism or explicit provisioning while IP routes are discovered en route. ATM relies on the state of a connection, while IP (especially version 4 IP) is stateless. ATM fixes cell size while IP uses variable size packets. IP frames carry end-to-end address information whereas ATM cells carry only local identifiers between each pair of switches. Quality of service in ATM is determined by availability along the entire route whereas IP quality of service is based solely on admission control to the network.

## UNCLASSIFIED

System-High Interconnections and Virtual Private Networks (VPN)  
IATF Release 3.1—September 2002

The primary motivations for considering an ATM security solution are the need to integrate high quality voice, video, and data applications and the need for quick implementation. Although the abilities of ATM are more apparent at the high end of communications, the mechanism scales across a wide range of operating rates.

Because IP packets can be reordered in transmission, each packet must contain sufficient information to enable synchronization of security mechanisms. ATM security can rely on the state of the connection to maintain synchronization. If the implementation is aware of ATM adaptation layers, information is available to deal with a limited amount of cell loss while maintaining synchronization. IPsec defines per packet authentication schemes through the AH. ATM security, as defined to date, does not have the equivalent function. Antispoof functionality is available that relies on higher layers to complete authentication, but the degree of protection is not the same as IP using the AH.

Because ATM can be implemented in so many ways and because the security services differ for each implementation, the options are discussed individually.

ATM can be used in a Constant Bit Rate (CBR) mode to connect enclaves emulating layer 2 trunk traffic. When ATM is used in this way while configured as a Permanent Virtual Circuit (PVC), all of the security services of secure provisioned link communications are available but provide more flexibility for upgrading service as required. If Switched Virtual Circuit (SVC) service is available at the enclaves, potential DOS attacks must be handled. Enclave-to-enclave IP over secure ATM (RFC 1483) has the same security attributes as IPsec in tunnel mode. Site-to-site identification is possible but the identity of end systems is hidden within the tunnel. Traffic rate is visible to the outside world but aggregation of large amounts of traffic and traffic smoothing can help obscure traffic flow information. Because of this similarity, this section refers to such a mode as a tunneling mode of ATM despite the lack of a formal definition. End-system-to-end-system secure ATM has security properties similar to IPsec transport mode. Complete end system identification is possible and individual traffic flows are discernible. Secure virtual paths allow end system identity to be hidden within a secure signaling channel within the virtual path. Though individual traffic flows will be discernible on the wide area network, there will be no information to tie the flow to an originator within the enclave except for perhaps stimulated events. Similar to the tunneling case, when end to end-user information is available, this section refers to that ATM transport mode as a tunneling mode.

The splicing attacks that Bellovin attributes to IPsec encapsulating security payloads may also be possible with ATM Forum-recommended encryption mechanisms.[1] This is an area for further study. If such an attack is possible, there is no equivalent to the AH to counter the threat. It is important to note that even if such attacks are possible with the ATM Forum-recommended modes, such attacks need not exist with all algorithm suites.

Government-sponsored equipment for securing ATM SVCs and PVCs are available for data rates up to 622 Mbps. A Type 1 interim system was developed for a single permanent virtual circuit that has limited availability. That Type 1 interim system also has a commercial equivalent. The previously mentioned government-sponsored IP encryptor will in fact produce a

## UNCLASSIFIED

System-High Interconnections and Virtual Private Networks (VPN)  
IATF Release 3.1—September 2002

combined IP and ATM encryptor. Further government developments are being considered for tactical platforms and for end-system use.

In the commercial arena, two companies have produced ATM encryptors. One unit operates over DS-3 circuits to secure a single PVC. Another unit operates at 155 Mbps and third unit operates at 622 Mbps. While none of these commercial units Type 1 grade, this is an area for commercial investment consideration.

The incorporation of native mode firewalls in ATM is in early stages of demonstration. No Type 1 products incorporate that functionality at this time. Some commercial systems have been demonstrated that incorporate simple IP packet filters. It is expected that there would be a similar need for encrypting firewall technology in ATM networks just as there is in IP networks. Although some doubt the extensibility of good firewalls to the level of performance that would be required in an encrypting firewall application, practical network administration makes the near-term utility of such a device very attractive.

### **Transport Layer Security**

Over the last few years, more attention has been given to providing a set of common security services in end systems. One version that gained acceptance actually existed just above the transport layer and was called Secure Session Layer Security. This effort has migrated to the Internet Engineering Task Force who placed the service at the top of the transport layer. This service is being called Transport Layer Security (TLS). One advantage of TLS is that this is the first place in the network stack where security services can be broken out per application rather than applying generic services to a secure pipe. However, this set of security services must be implemented in end systems and is therefore subject to all the invocation concerns of application layer services. The traffic flow problem is even more acute in TLS because of the visibility of individual services. At this point only early commercial implementations of TLS exist and none of these are the equivalent of Type-1-grade standards.

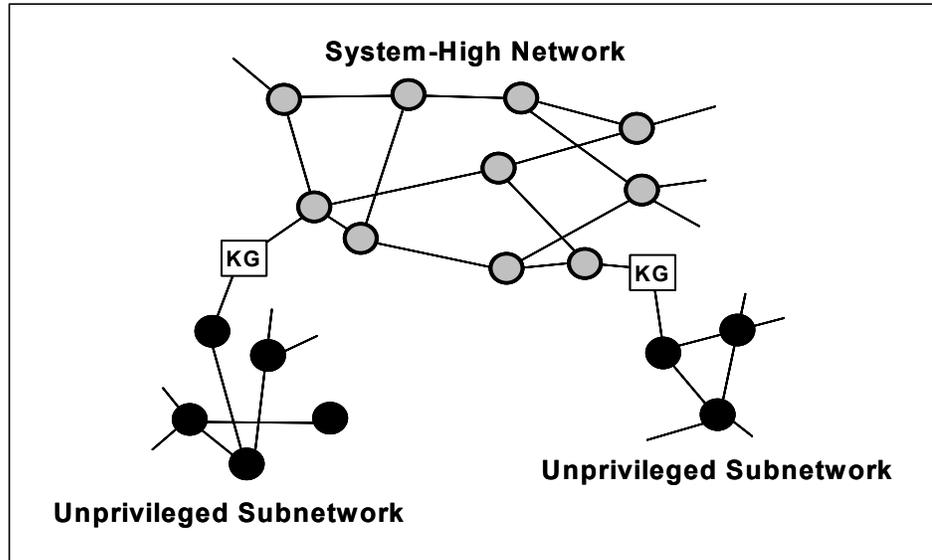
### **Super-Encryption in VPNs**

Super-encryption should be considered when there is a requirement to enforce privacy within the VPN. Such privacy may be implemented in end systems using lower assurance implementations of IPSec or ATM encryption under the control of an end system, TLS, or application-level mechanism implemented either in hardware or software. Alternatively, an entire subnetwork may be provided privacy by using a network encryption element. Note that this generalized description gives much flexibility to scale the level of protection mechanisms employed to fit the threat against an information system. Applicable architectures include link-protected switching and routing centers with end-system-based privacy mechanisms, link-protected switching and routing centers with enclave-based privacy mechanisms, and enclave-based protection backed by end-system-based privacy mechanisms. For instance, one should consider link-protected switching and routing centers with network layer security mechanisms if there is a traffic flow security requirement and the switching centers are maintained by unclassified personnel.

## Reverse Tunneling

In some scenarios, one needs to tunnel lower classification information through a higher classification system-high network. This is often accomplished by using the same high-grade cryptographic mechanism that would be required to tunnel high-grade traffic through a public network. Figure 5.3-4 illustrates the placement of cryptographic mechanisms for reverse tunneling.

The primary threat in this case is leakage of classified information into the lower classification tunnel. To help solve this problem, the cryptographic equipment should be under the control of the higher classification network and not under the control of the end users. If the lower level system is itself classified, it may have its own security



iatf\_5\_3\_0002

**Figure 5.3-4. Reverse Tunneling Placement of Cryptographic Mechanisms**

mechanisms. It is recommended that the network layer confidentiality system use a tunnel mode rather than a transport mode mechanism if one is available. Tunneling maximizes the isolation between the levels of information and prevents the low side from using short cipher to elicit recognizable responses from nodes on the high side of the tunnel. Although it is traditional to use cryptography strong enough for protection of classified information in the reverse tunnel, the information within the tunnel may only be unclassified. An area for investigation is whether well-implemented commercial systems can be used for such applications. Good implementation must address the need for strong integrity mechanisms on the secure tunnel. This will help prevent malicious code within the VPN from infiltrating information through the lower level tunnel. Finally, the implementation should consider what, in analog radio frequency devices, would be called reverse isolation. In particular, careful attention must be paid to unintentional leakage of higher level plaintext information through the encryptor and out the lower level information port.

## Relationship of Virtual Private Networking and Remote Access

The notion of virtual private networking implies an enclave of users who are protected from the network as a whole by some boundary device. Remote access implies a sole user gaining access

## UNCLASSIFIED

System-High Interconnections and Virtual Private Networks (VPN)  
IATF Release 3.1—September 2002

to the enclave by some protected means. Although the mechanisms to implement this access may be similar to that used for VPN, the details of the connection are vastly different.

Although dial-up access through a phone line resembles a VPN implemented at layer 2, it can implement security mechanisms at layer 2 or layer 3. The preferable solution would be a layer 2 protection mechanism with strong user authentication. An acceptable solution would be a layer 3 IPSec solution, given that the AH is implemented in the solution and strong user authentication is required. What makes these solutions more acceptable is that data exchange occurs directly between end systems without the need for protocol negotiation with an untrusted entity.

Remote access through an Internet Service Provider (ISP) using IPSec resembles an IP-based VPN. The primary difference is that remote access through an ISP consists of simultaneous connections to a private entity and a public entity without any intervening firewall or other protection mechanism. No monitoring of the information flow occurs between the remote host and the ISP to determine that no malicious transfers are taking place. This uncontrolled simultaneous connection between private and public entities takes this configuration outside the virtual private networking arena. Two areas of concern would have to be addressed before an ISP could be considered as a viable means of remote access to a secure enclave. The first concern is the window of unprotected access to the remote station during the period when the connection is made to the ISP but before IPSec or other mechanism can be invoked on communications with the secure enclave. The second is the concern that the remote terminal can become a convenient method for an insider to pass information outside the secure enclave because the remote terminal has simultaneous connection to the secure enclave and the unsecured ISP. The only solution would be a guaranteed invocation of the IPSec security mechanism across all IP source-destination pairs once a connection is made.

### **Role of Firewall Technologies in VPNs**

The resurgence of VPNs based on encryption mechanisms is largely the result of concern about penetrability of firewalls. However, encryption alone will only create secure data pipes between enclaves. There are no restrictions on the type and content of information that can be carried by that pipe. Joining enclaves with a secure data pipe also creates a default security policy that is the sum of the most promiscuous aspects of the individual policies. There are many situations in which this default policy applies. When connecting peer entities where the primary threat to the information is from external sources and where either all personnel accessing the system possess the same level of clearance or they may be deemed so trustworthy that they would not access restricted information given the opportunity, secure data pipes alone may be sufficient security. If these assumptions are not valid, the secure pipes must be supplemented by additional separation mechanisms. Firewalls are one way of providing that additional separation. Appropriate firewalls can allow an administrator to control the types of information flow across the VPN. For further discussion of firewall capabilities, see Section 6.1, Firewalls.

It is important to reiterate that, in this case, the use of a firewall is recommended for the situation in which two subnetworks are at the same security level but accreditors have assumed differing levels of risk in providing network security. Those interested in the case in which high-to-low connections are required should refer to Section 6.3.1, Guards, of this document.

## UNCLASSIFIED

System-High Interconnections and Virtual Private Networks (VPN)  
IATF Release 3.1—September 2002

There is a great diversity in the quality of implementation of firewall technology, and the purpose of this section is not to rate implementation quality. However, some general guidance on when to use firewalls and how restrictive they should be is appropriate.

- Primary protection between classified systems should be through some lower layer encryption system. Although these devices provide no protection against malicious users inside the network, they do limit accessibility of the VPN by outsiders.
- When true peers are connected, no firewall should be required.
- When applications demand high bandwidth, firewalls are likely to fail to meet the requirements. One area for suggested research is techniques to increase the throughput of a firewall while maintaining its effectiveness.
- When two connected systems are not exact peers, use of at least one firewall is recommended, and it should be placed at the enclave with the most demanding security requirements.
- When a firewall is required, the restrictions on connectivity should be commensurate with the minimum communications requirements and the difference between security levels and compartmentation within the respective enclaves.

### **Interoperability of VPN Protection Technologies**

Up to this point this section on VPNs is written as though the population were segmented into defined communities that have no communication with each other. Under these conditions, it is easy to define a unique security solution for each community. Within the DoD, such islands of communication cannot exist. During times of contingency, lines of communication are likely to be opened where none had been planned. This creates a conflict between the need for interoperability between organizations and the need to design a secure communications infrastructure that meets mission needs. The following are possible solutions to the interoperability problem.

- Require a uniform communications and security infrastructure.
- Require end systems to implement all security features and require peer-to-peer negotiations.
- Implement gateways that convert information to plaintext and reencrypt in the appropriate format.
- Develop methods of maintaining confidentiality through interworking functions.
- Implement redundant security mechanisms and modify protocol stacks to give visibility to the invocation of security mechanisms at all layers.

Of these options, 1 and 2 are unworkable for the following reasons.

## UNCLASSIFIED

System-High Interconnections and Virtual Private Networks (VPN)  
IATF Release 3.1—September 2002

- A uniform solution will not meet all requirements, and requiring that all systems carry all security mechanisms is too expensive.
- These options will likely result in failure to communicate if any of the peers fail to complete a secure setup, or in compromise if the default is to pass the requirement for securing the communications to the next higher layer when peers fail to negotiate secure setup.

Options 4 and 5 are research areas at this time. The TAFLANE equipment, in some sense, is an early implementation of option 5. If a secure ATM call setup fails, the device assumes that communications must be secured via IPSec. This, however, is a point solution and does not address the breadth of interoperability problems.

Therefore, in the near term, the only viable solution is option 3, red gateways between dissimilarly protected networks. Research is needed to determine whether options 4 or 5 can be viable at some point in the future to reduce plaintext exposure created by the use of the option 3 red gateways.

### 5.3.6 Cases

To apply these security technologies to user networks, it is most convenient to describe typical situations that must be encountered. In each of these situations, it is assumed that the end networks are of a single level of classification, employ the same structure of components, and that consistent security policies are in place. The following cases are considered.

- Classified networks connected over public infrastructures where indications and warnings are not a consideration.
- Classified networks connected over public infrastructures where indications and warnings to adversaries must be considered.
- Unclassified but controlled networks connected over public infrastructures.
- Tunneling of lower classification information over a classified system-high network.
- Tunneling of higher classification information over a classified network.
- Maintaining compartmentation and privacy over a secured classified network.
- Single backbone architectures for voice, video, and data.
- Connection of networks where subnetworks have incompatible security policies.

## 5.3.7 Framework Guidance

### **Case 1: Classified Networks Connected over Public Infrastructures Where Indications and Warnings Are NOT a Consideration**

This case covers the connection of classified enclaves when traffic flow security is not a priority, and it represents the majority of deployed classified VPNs. This case applies when the communications on the network are not involved in the planning and deployment of strategic or tactical forces, when the network is not involved in sensitive time-dependent operations, and/or when there is no tie to strategic intelligence sensors where reactions of the network can be used to probe the capabilities of sensors.

Three viable alternatives exist for creating secure VPNs over public infrastructures for this case. The most secure is to use Type 1 link-layer protection. This gives the greatest protection against outsider attacks on the network and the fewest means for malicious insiders to send information outside the network. This level of protection comes at the cost of increased communications cost and inflexibility in expanding or changing the network layout. Almost as good a choice would be using circuit emulation on an ATM permanent virtual circuit using Type 1 ATM encryption. This solution may give some cost flexibility.

If communication costs or the need for flexible communications precludes the use of leased circuits or circuit emulation, network-layer-based solutions should be considered. Type 1 enclave-based solutions are recommended. NES is an example of a Type 1 enclave-based solution for IP-based network topologies. Other, more standardized Type 1 IPSec-compliant solutions also are available. FASTLANE and TACLANE provide Type 1 solutions for ATM-based topologies.

There are no host-based Type 1 systems for network layer protection at this time. While this class of solutions can potentially be very cost-effective, the strength of invocation has not been sufficiently addressed to make a recommendation that such solutions be used. There are no commercial security systems of sufficient strength for protection of classified information at this time.

### **Case 2: Classified Networks Connected Over Public Infrastructures Where Indications and Warnings to Adversaries MUST Be Considered**

What distinguishes this case from the previous one is that observation of external traffic patterns even without decryption of the underlying information could give critical information to adversaries. For example, if a network extends into a tactical theater of operations, changes in traffic patterns may indicate the imminence of offensive operations thereby prohibiting the element of surprise. Another example would be where a network can be identified as processing information from critical sensor platforms. Here probing the sensor and observing resulting traffic patterns can give away sensor response times and sensor sensitivity.

## UNCLASSIFIED

System-High Interconnections and Virtual Private Networks (VPN)  
IATF Release 3.1—September 2002

The basic solution set is the same as the previous case. The best solution is still the Type 1 link-based security system. The reasons provided in Case 1 still hold, with the addition of the complete traffic flow protection. Although, the existence of links can be easily identified, the change in traffic patterns is indiscernible.

If link-based solutions are not feasible, prime consideration should go to enclave-based network layer solutions that tunnel multiple logical connections through a single path. This solution is represented by the NES because it tunnels enclave information via IP packets that are addressed from NES to NES. As Type 1 IPSec-compliant systems that use the IPSec tunnel mode become available, these systems also will meet security requirements. ATM wide area connections can provide some of the same capabilities for IP LANs because multiple IP source destination pairs can tunnel through the same ATM virtual circuit.

As end-to-end ATM applications become viable, tunneling will become more difficult because individual virtual circuits will be set up between end systems for each source-destination pair. The best solution for this case will be a secure virtual path service between enclaves, which will at least enable identification of the end points of each virtual circuit to be encrypted within the virtual path. However, the characteristics of each data flow will be observable. When traffic analysis is a threat, any of the network-based solutions, especially the end-to-end ATM solution, can be made better with rate shaping of the traffic by the end systems.

No host-based Type 1 systems for network layer protection exist at this time. Although, this class of solutions can potentially be very cost-effective, the strength of invocation has not been sufficiently addressed to allow a recommendation that such solutions be used. No commercial security systems of sufficient strength for protection of classified information exist at this time.

### **Case 3: Unclassified But Controlled Networks Connected Over Public Infrastructures**

This case is the unclassified but controlled version of Case 1. The difference in the solution is that commercial-strength mechanisms may be adequate for protection without going to the expense of a Type 1 equipment. The security benefit is probably insufficient to consider a link-layer protected solution for the unclassified but controlled case. It is recommended that a commercial enclave-based network layer solution be used whether that solution is ATM or IP-based. A mode that supports IPSec tunneling or the ATM equivalent is preferable to a transport mode solution.

Host-based solutions are not recommended for primary protection of a direct connection to public networks until further testing has been accomplished to check strength of invocation and their ability to be bypassed.

## **Case 4: Tunneling of Lower Classification Information Over a Classified System-High Network**

This case exists when a classified network that already exists is protected at a link layer and used to transport unclassified or unclassified but controlled information as a matter of convenience. In this situation, protection has traditionally been implemented with Type-1-encryption systems as in the case of the tunneling of unclassified information through Secret Internet Protocol Router Network (SIPRNET) using the NES.

The properties desired from such a solution are that the mechanism be sufficient to protect information that is presented to the network, that invocation cannot be bypassed, and that reverse isolation of the mechanism be sufficient to prevent leakage of the higher classification information onto the lower classified network. Strong data integrity mechanisms must be part of the security services offered by the security device used. These mechanisms are used to protect the information on the low side of the connection but to eliminate the possibility of malicious insiders using the channel as a means to send information out of the secure network.

Although Type 1 solutions can still be used for such applications, commercial network layer systems should be considered. In addition, a tunneling mechanism should be mandatory. Note that this requirement eliminates IPSec transport mode solutions. The equipment implementing the security should be under the ownership, control, and configuration of the higher classification network. The system must not be able to be configured from the port that is connected to the lower classification network.

## **Case 5: Tunneling of Higher Classification Information Over a Classified Network**

An example of this type of application would be the tunneling of a Top Secret network like the Joint Worldwide Intelligence Communications System (JWICS) through the SIPRNET.

The central issue in this case is whether the solution must be as strong as that required for tunneling over an unclassified network or, because protection is provided in Case 4 to deal with the use of a lower classification network, whether a weaker mechanism can be considered.

It is recommended is that a Type 1 enclave-based tunneling mechanism be required. The mechanism should be under the control of the higher classification network.

## **Case 6: Maintaining Compartmentation and Privacy Over a Secured Classified Network**

The difference between this case and Case 5 is that compartmentation is an enforcement of need-to-know among people who are equally cleared. It is assumed that the protection on the network is already sufficient to deter penetration by outsiders. Therefore the real need is for privacy within the network rather than protection from malicious outsiders. Although application layer

## UNCLASSIFIED

System-High Interconnections and Virtual Private Networks (VPN)  
IATF Release 3.1—September 2002

solutions are sufficient for lower bandwidth applications, more demanding applications will probably require some network-based privacy solution.

Given the threat environment, this is an ideal case for using commercial host-based solutions, whether IP transport mode or ATM end-to-end.

### **Case 7: Single Backbone Architectures for Voice, Video, and Data**

This architecture was one of the primary motivations for the development of secure ATM (in addition to the scalability and the speed of implementation). By placing the security at the ATM layer, a single set of mechanisms successfully protects all information that crosses an enclave boundary. That vision is too optimistic. Problems occur with voice connectivity. A secure voice architecture currently covers all transport means except broadband voice. Although ATM security is perfectly capable of protecting voice communications, the problem is the lack of secure interworking between broadband voice and secure N-ISDN and POTS voice. Until these interworking issues are resolved, it is not recommended that broadband voice services be secured with native mode ATM security services.

### **Case 8: Connection of Networks Where Subnetworks Have Incompatible Security Policies**

The previously recommended solutions for VPNs all assume that the enclaves have compatible security policies. Under present security guidelines and as a risk management philosophy becomes more widespread, security policies are likely to diverge. Therefore it is expected that enclaves to be connected will have security policies that are incompatible in some way. In the standard virtual private networking scenario, the unimpeded flow of information within the virtual network create a resultant security policy that is a fusion of the most liberal aspects of the security policies of the individual enclaves. The system security administrators of the individual enclaves either need to recognize the resultant security policy and assess the impact on their systems or an additional separation mechanism must be added to help enforce the desired policy. This case is an ideal place for the marriage of firewalls with VPNs. In this respect, the commercial community is far ahead of the Type 1 community with the widespread availability of encrypting IPSec-compliant firewalls. When additional separation is required, an appropriate IP or ATM-based firewall that implements features needed by the enclave, cascaded with the Type 1 enclave protection mechanism, is recommended.

## UNCLASSIFIED

System-High Interconnections and Virtual Private Networks (VPN)  
IATF Release 3.1—September 2002

### References

1. Bellovin, Steven M., “Problem Areas for the IP Security Protocols,” July 22–25, 1996, San Jose, CA: *Proceedings of the Sixth Usenix UNIX Security Symposium*, 1996.  
<http://www.usenix.org/publications/library/proceedings/sec96/bellovin.html>

This site provides an abstract of the document. You must become a member of USENIX to see the full text of the document. To become a USENIX member, see the Membership Information link on the Web site.

### Additional References

Virtual Private Networks, Faulkner Information Service, Pennsauken, NJ, May 1996.

**UNCLASSIFIED**

System-High Interconnections and Virtual Private Networks (VPN)  
IATF Release 3.1—September 2002

**This page intentionally left blank.**

## 5.4 Security for Voice Over Internet Protocol (VoIP)

Although Voice Over Internet Protocol (VoIP) has been around for many years, it has only recently gained widespread interest and implementation. Because it is a fairly new technology, it has not undergone the same level of scrutiny and use as more established technologies.

Although many of the risks associated with VoIP are known, there is still much to be learned. In some ways, we are still at the point in the learning curve where we don't know how much we do not know. Some of the risks and vulnerabilities related to VoIP will be remedied as the technology evolves, but there inevitably will be some residual risk that cannot be ameliorated. It is still difficult to determine what portion of the current security issues fall into the "fixable" category, and which must be classified as "managed residual risk."

Because VoIP is still, to a large extent, an unknown quantity, this section will discuss the related security issues at a conceptual level. Thus, we will not indicate a particular setting of a particular field in a given protocol as a problem but will discuss the issues in generic terms. For example, we may discuss crypto as a source of delay, which may affect voice quality, but we will not suggest a particular crypto algorithm or piece of crypto equipment. In addition, because the technology is still in the "early adopter" phase, this section takes a somewhat cautionary tone: Prudence dictates that security practitioners take care when faced with technologies that have not yet established a strong foundation of security analysis and experience.

Although this section focuses on Voice Over Internet Protocol, many of the same general concepts may be equally valid for similar technologies that move digitized voice over digital networks using protocols that may have been originally designed for data networking rather than voice. Such technologies include, but are not limited to, Voice over Frame Relay (VoFR), Voice over Asynchronous Transfer Mode, and Voice over Digital Subscriber Link. These related technologies are discussed briefly in Section 5.4.5, but a full discussion of the technologies and their place in a total Internet telephony solution will have to wait for a future update of this section.

The key feature of all of these related technologies is the migration of voice from its historic technological underpinnings of analog signals on a synchronous, connection-based architecture to a digital signal moving over a packet-switched architecture. The latter means of transit is asynchronous, although it is perceived by the end user as being "real time." This migration has created several complications and necessitated the revisiting of some of the underlying design assumptions of traditional phone networks.

A critical feature of this technology shift is the culture shock that occurs when technical personnel who have worked with telephone networks and those with a network background must work together. The tendency is for each group to view the problem of a converged network encompassing data and voice in the context of its own experience and history. Telephony engineers tend to think of the system as a phone network that is using new technology and expanding to include data, while data network engineers view voice on their digital networks as

## UNCLASSIFIED

Security for Voice Over Internet Protocol  
IATF Release 3.1—September 2002

just another type of bits. In reality, both groups must undergo a significant learning process as they become familiar with problems and concerns that those from the other camp view as common knowledge. Each group must familiarize itself with the basic concepts and knowledge of the other group and fill in the gaps in its own knowledge. Only when this initial acclimatization has occurred can the two groups effectively consider the complications that arise from the interactions of these formerly separate realms.

To assume that installing VoIP is “...just like hooking up <familiar product or piece of equipment>” seriously understates the system-level implications. Like any new technology, there are nuances that may not be initially recognized, especially when the transition involves new architectural assumptions not just a direct replacement of an old technology with a newer one.

An additional area in which the transition from one set of assumptions to another will prove critical is the realm of law, regulation, and policy. With VoIP, any new technology, it will take some time for the rules to catch up with the technology.

A tangential issue that may have an indirect impact on security is the perception that significant cost savings will be generated by switching to VoIP. The argument is that moving from two separate infrastructures to a single infrastructure, will naturally produce a great reduction in cost. Although there has now been some cost analysis of the short-term expenses incurred for equipment, wiring, personnel (retraining, hiring, or replacement), and the transition of telephony bandwidth to network bandwidth, these cost figures are for nonsecure environments. It remains to be seen whether security considerations will increase costs, or even mitigate against converging into a single network. There may be both security and reliability arguments for moving voice to a separate packet-switched network.

Poor cost planning can have hidden implications for security. If cost estimates for switching to VoIP are not carefully performed, resources originally allocated for security might instead be tapped to achieve basic functionality. Estimates of the costs of security for the new technology may also be inaccurate, due to VoIP's brief history and the new assumptions and interrelationships it brings with it. Conservative budgeting is called for to avoid shortfalls caused by imprecise understanding of the costs of implementing the core technology and applying security functionality on top of it.

In some senses, attackers are in the same situation as defenders with respect to VoIP. They too are facing a new technology and will probably need time to develop the theories, tools, and techniques to maximally exploit it. Although some VoIP attack tools are available and other tools and exploits from the data network realm can be adapted for use against VoIP, the threat is still in a ramp-up mode. It is hard to predict how long this stage will last. At least one factor will be the market penetration of VoIP in the coming months and years. As potential targets increase in number and attractiveness, the likelihood that the technology will draw adversary attention increases. This may result in a race between attackers and defenders as to who will turn their attention to any particular vulnerability first. This second stage will introduce a now familiar cycle, with advantage swinging back and forth between attackers and defenders as new

vulnerabilities are found and techniques to minimize or exploit the vulnerabilities are deployed by the respective sides.

## 5.4.1 Target Environment

VoIP is potentially a functional replacement for both regular and secure phones and can, at least hypothetically, be used in any location where more traditional phones have been used in the past. That said, the transition to VoIP is not simply a matter of unplugging the old handset and plugging in the new one. In VoIP, the majority of the changes are hidden from the end user, involving replacement of telephone cabling, private branch exchanges (PBX), and other equipment with network cable, routers, and other such elements.

The target environment is in some ways very familiar, since there is broad user experience with data networks and basic phone usage. At the same time, use of a phone over a data network and its implications from an administrative perspective are very new. The technology and issues are understandable, though complex. What is unclear is how best to adapt the historically connection-based synchronous phone system model to a packet switching–based asynchronous infrastructure, and the implications of that transition.

Another set of issues concerning the new environment is the policy, legal, and regulatory framework that covers the phone system and the data network. Numerous laws, policies, and regulations, on issues ranging from wiretaps to Emergency 911 functionality, have been developed over the years with the traditional telephone system in mind and with the assumption that the telephone network is a fairly homogeneous and isolated environment. Similarly, some existing laws, regulations, and policies governing the operation of data networks may not cover the concept of content other than traditional data. Although there have already been attempts to adapt regulation and law to the new technological landscape, it may be many years before the legal and regulatory picture stabilizes.

There are numerous questions about how the combined environment will be treated. For example, there are now specific rules on the treatment of information that flows over government networks, such as e-mail and file transfers. Some of this information is designated as “official government records” based on its presence on a government network, how it was generated, how it is stored, and so on. Once telephone conversations are converted to data packets on a government network, do those same rules apply? On the other hand, does a network sniffer become an illegal wiretap if it sniffs VoIP packets (as it would if the same content were intercepted on the public switched telephone network [PSTN])? For legal purposes, what makes a phone call a phone call as opposed to data?

Because this technology is so new, we will not attempt to define specific target environments in detail. (There are just too many possible architectures and implementations for us to pick the ones that will become commonplace.) Instead, we will present the issues that may apply in various contexts, with the assumption that the reader will select, and perhaps extrapolate, to derive useful information regarding a specific usage scenario. Nevertheless, it is clear that there

will be nuances in the development and implementation of this technology that are either underappreciated, or have not yet been recognized.

## 5.4.2 Requirements

The general intuitive requirements for VoIP can be stated simply: VoIP is to provide a functional replacement for a traditional telephone infrastructure in a given context. However, in meeting user expectations, more detailed requirements emerge, some of which may be optional in some circumstances. These more specific requirements include, but are not limited to, the following items:

- Acceptable voice quality in real time (<150 ms delay).
- An acceptable addressing scheme, which may or may not map directly to existing phone number schemes, but which must be translatable to existing phone networks and legacy systems.
- Access control to allow one to limit calls into or out of the organization's telephone infrastructure from either a public system or another enclave on the basis of such factors as calling number, called number, time of day, and others. This type of access control is what one would expect from a conventional private branch exchange (PBX), and this functionality should not be lost in a VoIP implementation. Indeed, this capability may prove to be more crucial in the VoIP realm than it was in traditional telephony.
- Sufficient auditing and billing functionality to meet mission, regulatory, and statutory requirements.
- Cost which is equivalent to, or an improvement over, existing phone technology, when all factors are added in.
- Ability to interface and interoperate with existing secure telephone technology, such as secure telephone unit (STU) III and secure telephone equipment (STE).
- Quality of service, including reliability and availability, that is comparable to that of existing telephone technology.
- Call prioritization and preemption capabilities, including both prioritization of telephone calls (e.g., "the General's call always goes through") and prioritization of telephone traffic versus data traffic on the network to maintain acceptable service levels.
- Emergency 911 geolocation information, as required by law and/or regulation (and perhaps the ability to disable it for some applications).
- Robustness. A converged network is a single point of failure; therefore, it must be designed for redundancy, fault tolerance, and graceful degradation.
- Confidentiality. Sniffing a network is easier than tapping a traditional phone network, in large part because it requires less precise physical access. Therefore, some sort of

confidentiality mechanism may be needed to achieve functionality (even basic functionality) equivalent to that of the traditional phone network.

- **Legality.** All pertinent legal and regulatory requirements applicable to the traditional phone network must be met in a VoIP environment. However, as noted in the previous section, it should not be assumed that the same rules automatically apply in the same ways in the new environment. Therefore, there should be a conscious effort to determine the ground rules when using the new technology.
- Connection to the PSTN must not introduce errors or vulnerabilities to the PSTN, lest the PSTN decline to allow the connection.
- Feature set (conferencing, call waiting, call forwarding, voice mail, Caller ID, automatic dial-back, etc.) similar to the standard feature suite one expects from PSTN service.
- Traffic management and load monitoring capabilities similar to what one would expect from a typical PBX installation.

### 5.4.3 Potential Attacks

Research regarding potential attacks on VoIP systems is still in its early stages. The technology has not been around long enough for truly creative or detailed exploits to be developed or hypothesized. Nevertheless, many aspects of these systems are likely to provide fertile ground for those interested in exploiting VoIP. Some of these attacks will involve simple exploitation of “beginner’s mistakes” that will be rapidly corrected as the technology matures. Other forms of attacks will focus on flaws that are much more deeply rooted, and will be more difficult to prevent or mitigate.

The following list of attack types should not be viewed as complete. This technology is still too new for practitioners to fully understand the threat situation and its nuances.

- **Direct Access Over the Network.** If the phone is on the network, it is likely that some of its functions (speaker phone, room monitor, etc.) will be remotely accessible over the network. Limiting such access to authorized usage may be tricky.
- **Network Sniffing.** The original telephone infrastructure was designed to create a point-to-point link between caller and recipient, with the assumption that there would be no other parties on the line. Switched-packet networks are designed to send data over commonly accessible paths. Any signal that is not protected by encryption or other means must be assumed to be accessible to an adversary, possibly without the direct physical access that was generally necessary to tap the PSTN.
- **Manipulation of Traffic Flow.** Data networks are inherently asynchronous, in that the data packets do not flow over a dedicated connection for the duration of a session. By manipulating the routing of packets, an adversary could cause dropouts, insert latency (time delay between transmission and reception), or insert jitter (variation in the latency). Although such attacks make little sense in a data network, except in very specialized

## UNCLASSIFIED

cases, they would have significant effect on the perceived quality of a connection to a voice user. It remains to be seen how difficult such attacks would be to implement, or how prevalent they will become.

- **Data Exfiltration.** VoIP traffic will require what is essentially a high-bandwidth breach of guards and firewalls, so as not to incur too much delay. It is also a given that VoIP packets, unlike data packets in known formats, will be very difficult (perhaps impossible) to scan for legitimate content or hidden data without introducing unacceptable delay. Unless effective means are found to isolate VoIP traffic from data traffic, VoIP will prove to be an attractive vehicle for data exfiltration, either by malicious Trojan horse code, or by an insider with bad intentions.
- **Denial of Service (DoS).** While a DoS attack could take many forms, the most obvious would be taking down or flooding the network, or some portion thereof. In the traditional system, if the network were rendered inoperable, an organization could still maintain some communications functionality over the phone. In a commingled “converged network,” one would have both (i.e., network and phone service), or neither. This situation creates an attractive target. Obviously, if the VoIP portion of the network were isolated from the data portion, or if there were a fall back to traditional telephone infrastructure, this type of attack could be less effective.
- **Routing Delay Attacks.** An adversary might attempt to artificially induce delay to ensure that particular phone conversations were routed through particular network paths. In this way, an adversary could potentially choose a location for a packet sniffer or other monitoring equipment, then maneuver the desired traffic past that point.
- **Control/Signaling Attacks.** As noted, modern data networks often run control and data signals over common links. Hypothetically, this is also possible on conventional phone networks, but given the limited access to the switching systems, the phone network is less vulnerable.
- **Bandwidth Attacks.** If an attacker could tie up sufficient bandwidth on a given link, there might not be sufficient throughput to support VoIP voice encoding schemes, which assume a certain minimum bandwidth to function properly.
- **Protocol-Based Attacks.** Because VoIP is still new, it remains to be seen what might occur if an adversary manipulated the various protocols in unanticipated ways. More analysis of the protocols and the implementations in various equipment is needed to determine what protocol-based vulnerabilities to buffer overflows, man-in-the-middle attacks, traffic analysis, content-based attacks, or other mischief may exist in VoIP systems.
- **IP Spoofing.** IP spoofing is a well-known class of data networking attacks, in which an adversary hijacks a session, assuming the identity of the intended recipient. It is not hard to imagine the use of these same techniques to reroute or intercept VoIP phone traffic, allowing either masquerade or man-in-the-middle attacks.

- **Domain Name Server (DNS).** DNS system is a sort of distributed repository of network address information. It is roughly analogous to a phone book, allowing one to query based on an identifier such as a name, and get a corresponding address, usually expressed as a series of numbers in a particular format. At present, there is little security or authentication in the DNS system. As phone traffic moves to Internet Protocol (IP), the DNS system will become an even more critical piece of the infrastructure.
- **Brute Force Password/Personal Identification Number (PIN) Attacks.** Because a telephone handset (the entry mechanism in the VoIP environment) has only a numeric keypad, the possible symbol search space for passwords and PIN is greatly reduced. The limitations of human memory limit the useful length of a PIN or password even further. The result is that passwords and PINs are likely to be less secure. Alternative forms of identification and authentication (I&A) may be needed in some applications.

## 5.4.4 Potential Countermeasures

This section, like that on potential attacks can provide only general information, because the technology is still too new to have an established repertoire of proven tools and techniques.

However, it is anticipated that the most critical areas for countermeasure development will be in the realm of encryption, covert channel/steganography detection and prevention, and protection against protocol-based attacks.

- **Encryption.** Various efforts to use high-speed links or end-to-end encryption have been made in early VoIP installations. The critical concerns are latency, jitter, bit error rate, error propagation, and bandwidth. As is often the case with encryption, the implementation details are crucial to success. One should also be aware of the various levels at which encryption can be applied. Application layer encryption can provide end-to-end coverage but increase covert channel problems at firewalls and guards because of the traffics being encrypted. Virtual Private Networks (VPNs) and link encryptors may be used at the network layer but may require decryption and re-encryption at various points, leaving the message exposed briefly at some nodes. Encryption can also introduce delay, either during call setup or as latency during the session. If the encryption is not sufficiently fast, some form of voice compression may be required for effective use.
- **Firewalls/Guards.** The use of VoIP requires the adaptation of the firewalls in the network to allow access to ports used by VoIP and to allow out the various protocols VoIP use. Because an adversary could use these paths as well, configurations must be chosen carefully. Note that in this instance the concern is not so much about the impact on VoIP, as about the effect of the introduction of VoIP equipment and traffic on the security of the preexisting data network. In a similar vein, it is unclear how VoIP can be incorporated across a network boundary protected by a guard. The very concept of a guard, or other secure downgrading mechanism, implies a degree of delay that would be unacceptable for VoIP. In such cases, another solution for the voice traffic must be found, whether this entails putting VoIP only on networks (whether unclassified or

“system high”) that do not require the downgrade function or reverting to traditional telephony solutions.

- **Covert Channel and Steganography Detection.** Whereas the preceding item addressed the need for adaptation of existing firewalls and guards and the effects on the preexisting data network, this item assumes that additional filtering or monitoring will be necessary to detect modulation or other misuse of legitimate VoIP traffic flows to carry covert data either in or out. Historically, identification and prevention of covert channels have constituted one of the knottiest problems in computer security, even when confined to the data realm. The additional need to detect covert channels in the underlying analog signal increases this protection challenge significantly. This problem may require isolation of the VoIP system to prevent introduction of modulating signals. This is another area in which combining digital signal processing and the sharing of a single network between voice and data create a class of risk that was not present (or was far less likely) in separate voice or data systems.
- **Traffic Flow Tools.** Given the relative accessibility of network traffic information, protection against traffic analysis may be more crucial in a VoIP realm than in the more closed environment of a traditional telephone network. As a result, there may be a need to create a means of disguising traffic flow patterns, either by covering or masking routing information or by generating bogus traffic to disguise the flow of the real calls.
- **TEMPEST.** Given the high bandwidth of a VoIP channel, we may need to be conscious of potential modulation of the signal by other equipment in the operational environment. TEMPEST analysis of relevant equipment may be necessary in some environments.
- **Anti-Tamper.** The VoIP channel’s high bandwidth and the ability to remotely access the VoIP equipment over the network make the VoIP handset an attractive target for such basic tampering as modifying the switch that disconnects the handset microphone when the phone is on the hook. There are many other tampering possibilities, but most can be addressed by a standardized program of inspection and analysis of the equipment, combined with simple tamper-detection mechanisms.

## 5.4.5 Technology Assessment

### 5.4.5.1 Technology Assessment and Selection Overview

Because VoIP is an emerging technology, there are as yet no well-established, objective selection criteria, and the various possible architectures and configurations have not yet narrowed down to a few canonical variants. Adding to this problem is the fact that the traditional telephone system is such an established technology that its functionality has come to be assumed. We take for granted functionality such as call prioritization or preemption, echo canceling on

long-distance calls, “toll quality” voice reproduction, universal access, and relative privacy of individual calls, among other functions.

In the absence of accepted selection criteria or an established body of worked examples of successful and secure implementations, adopters of VoIP technology should first consult with the technologists supporting their existing traditional phone system and determine which functions are being actively used. This process must be approached as a blank slate, with the intent of fully documenting what the current phone system does behind the veil of comfortable, familiar reliability. Once this baseline functionality has been documented, the new VoIP system can be examined with an eye toward ensuring that all existing functions will be carried over, with appropriate trade-offs and adjustments where necessary.

Examination of the existing or traditionally assumed phone functionality may identify several classes of functionality. Some are “must have” items from the user’s perspective (e.g., voice quality), others may be required by policy (e.g., Emergency 911 geolocation), and still others are characteristics of VoIP (latency and jitter specifications) that don’t map neatly back to the old telephone system.

In all cases, the object of the examination is to fully characterize the old system and to consciously establish expectations for the new system. The goal is to work out all details beforehand, so that there are no moments of disappointed realization that the new system is not “just like the old phones,” once the VoIP is installed.

From a security standpoint this evaluation is doubly important in that many of the security assumptions regarding the old telephone system will no longer apply, while new security requirements will emerge. First, many of the security assumptions regarding the old telephone system relate specifically to the architecture of that system. Because the telephone system is connection-based, conversations were generally not physically available to other users. Control, billing, and switching attacks were somewhat difficult because of the largely “out of band” nature of the control substructure.

In a packet-switched system operating over common channels, the technique for tapping a conversation is significantly altered, because anybody can sniff the traffic over common lines. On the control side, the control signaling is often carried over the same infrastructure as the message links. In general, VoIP security requires much more extensive intervention to achieve the same basic level of security that was assumed with the traditional system, mainly because risk has shifted from physical access to virtual access.

Achieving higher levels of security is a mixed bag. In some instances, (e.g., encryption and intrusion detection), additional security may be provided by security measures that are already present in the data network. In other cases, VoIP implementation will be in conflict with existing data network security mechanisms (for example, many firewalls, and downgrader/guards).

In general, however, the introduction of VoIP into existing data networks will require development of selection criteria that take into account the effect on existing data network

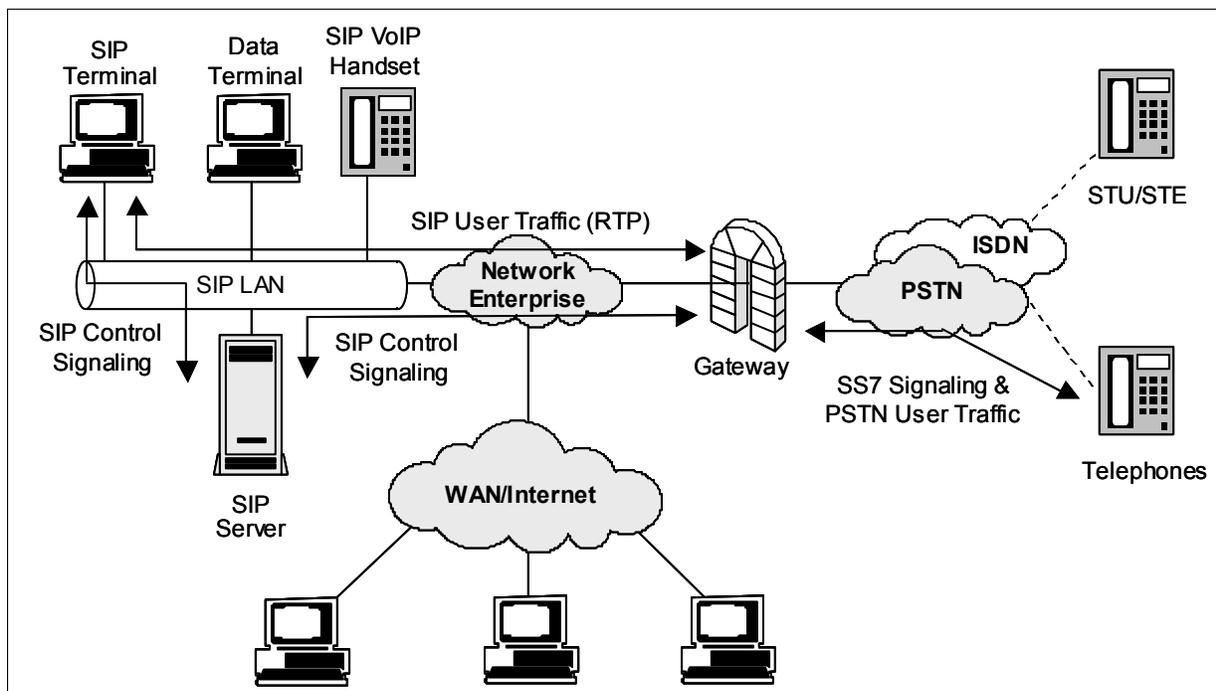
security, the interaction between data network security and VoIP, and new classes of attacks and security issues that will arise from the co-location of both functions on the same infrastructure.

The following paragraphs address some technology specifics, and the implications those specifics have for the security practitioner.

## 5.4.5.2 SIP

Session Initiation Protocol (SIP) is a text-based protocol, like Simple Mail Transfer Protocol (SMTP) and Hypertext Transfer Protocol (HTTP), for initiating interactive communication sessions between users [1]. Such sessions include voice, video, chat, interactive games, and virtual reality. SIP is the protocol used to set up conferencing, telephony, multimedia, and other types of communication sessions on the Internet [2].

SIP is described as a control protocol for creating, modifying, and terminating sessions with one or more participants in an IP-based network. These sessions include Internet multimedia conferences, Internet (or other IP network) telephone calls, and multimedia distribution. Members in a session can communicate via multicast, through a mesh of unicast relations, or by a combination of these. SIP supports session descriptions that allow participants to agree on a set of compatible media types. It also supports user mobility by proxying and redirecting requests to the user's current location. SIP is not tied to any particular conference control protocol [4]. Figure 5.4-1 illustrates a typical SIP network and the different information flows involved in a SIP call.



iatf\_5\_4\_1\_5401

Figure 5.4-1. SIP Network

To provide telephony services, a number of standards and protocols must come together. Real-Time Transport Protocol (RTP) is used. RTP is an Internet protocol for transmitting real-time data such as audio and video. RTP consists of a data and a control part. The latter is called Real-Time Transport Control Protocol (RTCP). In addition, a mechanism is needed for guaranteeing voice quality (for instance, Resource Reservation Setup Protocol [RSVP] or Yet another Sender Session Internet Reservations [YESSIR]). An authentication method is also needed with SIP (see Section 5.4.5.7.4).

Currently, SIP is a draft, proposed as standard RFC 2543, from the Internet Engineering Task Force (IETF), the body responsible for administering and developing the mechanisms that make up the Internet. The main work of the IETF's SIP working group involves bringing SIP from proposed to draft standard, in addition to specifying and developing proposed extensions that arise from strong requirements. The SIP working group will not explore the use of SIP for specific environments or applications. It will, however, respond to general-purpose requirements for changes to SIP provided by other working groups, including the Session Initiation Protocol Project INvestiGation (SIPPING) working group, when those requirements fall within the scope and charter of SIP [1]. The SIPPING working group has the more focused goal of documenting the use of SIP for several applications related to telephony and multimedia, and developing requirements for any extensions to SIP needed for those applications.

### **5.4.5.3 H.323**

The H.323 standard is a cornerstone technology for the transmission of real-time audio, video, and data communications over packet-based networks. It is an umbrella standard that specifies the components, protocols, and procedures that provide multimedia communication over packet-based networks that do not provide a guaranteed quality of service (QoS). H.323 can be applied in a variety of mechanisms: audio only (IP telephony); audio and video (video telephony); audio and data; and audio, video, and data. H.323 can also be applied to multipoint multimedia communications.

The H.323 standard is specified by International Telecommunication Union (ITU)-T Study Group 16 and is currently in version 4. Version 1 of the H.323 recommendation titled, "visual telephone systems and equipment for local area networks (LANs) that provide a nonguaranteed QoS," was accepted in October 1996. It was, as the name suggests, heavily weighted toward multimedia communications in a LAN environment. The emergence of VoIP applications and IP telephony paved the way for a revision of the H.323 specification. With the development of VoIP, new requirements emerged, such as providing communication between a PC-based phone and a phone on the PSTN. Such requirements expanded the need for a standard for IP telephony.

Version 2 of H.323, packet-based multimedia communications systems, was defined to accommodate the additional requirements; this version was accepted in January 1998. New features in version 2 included call hold, call park and pickup, call waiting, message waiting, and some fax and multimedia broadcasting capability. These features basically map voice calls over IP and standardize call connections, allowing calls from different systems to interoperate.

## UNCLASSIFIED

Security for Voice Over Internet Protocol  
IATF Release 3.1—September 2002

Version 3 of the standard added fax-over-packet networks, gatekeeper-gatekeeper communications, and fast-connection mechanisms. Among other features, these mechanisms provided for better performance and preserved system resources by enabling an endpoint to specify whether it has the ability to “reuse” a call signaling connection and whether it can support using the same call signaling channel for multiple calls. This capability is particularly important for gateways that may have thousands of calls running simultaneously. By using these two features, a gateway can maintain a single Transmission Control Protocol (TCP) connection between itself and the gatekeeper to perform all call signaling [5].

Version 4 contains enhancements in several important areas, including reliability, scalability, and flexibility. H.323 has a strong market in voice, video, and data conferencing on packet networks; version 4 makes strides toward keeping H.323 ahead of the competition [6], although version 4 is not widely implemented [7].

The IETF standards are interoperable with the ITU-T standards on the voice transport level because ITU-T incorporated IETFs RTP protocol in its H.323 umbrella standard. However, the two institutions propose different signaling protocols: ITU-T uses the H.323 standard (“visual telephone systems and equipment for local area networks which provide a nonguaranteed quality of service”), whereas IETF pushes the SIP signaling. Currently, there are many discussions and predictions about which approach will gain greater popularity [7].

A primary goal of the H.323 standard is interoperability with other multimedia-service networks. This interoperability is achieved through the use of a gateway, which performs any network or signaling translation required for interoperability.

The H.323 standard specifies four distinct components, which when networked together, provide point-to-point and point-to-multipoint multimedia communication services. These components are—

- Terminals.
- Gateways.
- Gatekeepers.
- Multipoint control units (MCU).

The gatekeepers, gateways, and MCUs are logically separate components of the H.323 standard but can be implemented as a single physical device.

### **5.4.5.3.1 Terminals**

Terminals are used for real-time bidirectional multimedia communications. An H.323 terminal can be either a personal computer (PC) or a stand-alone device, running H.323 and the multimedia applications. It supports audio communications and can support video or data communications. A primary goal of H.323 is working with other multimedia terminals. In pursuit of this goal, H.323 terminals must support the following standards and protocols:

- **H.245.** An ITU standard used by the terminal to negotiate its use of the channel. The H.245 control channel provides in-band reliable transport for capabilities exchange, mode preference from the receiving end, logical channel signaling, and control and indication.
- **H.225.0.** An ITU standard that uses a variant of Q.931 to set up the connection between two H.323 endpoints.
- **Registration Admission Status (RAS).** A protocol used to communicate with the H.323 gatekeeper.
- **RTP and Real-Time Control Protocol (RTCP).** Protocols used to sequence the audio and video packets. The RTP header contains a time stamp and sequence number, allowing the receiving device to buffer as much as necessary to remove jitter and latency by synchronizing the packets to play back a continuous stream of sound. RTCP controls RTP, gathers reliability information, and periodically passes this information on to session participants [8].

### 5.4.5.3.2 Gateways

A gateway connects two dissimilar networks (e.g., an H.323 network and a non-H.323 network). For example, a gateway can connect and provide communication between an H.323 terminal and a terminal on the PSTN. This connectivity is achieved by translating protocols for call setup and release, converting media formats between different networks, and transferring information between the networks connected by the gateway. A gateway is not required, however, for communication between two terminals on an H.323 network.

### 5.4.5.3.3 Gatekeepers

A gatekeeper can be considered the brain of the H.323 network. It is the focal point for all calls within the network. Although they are not required, gatekeepers provide important services, such as addressing, authorization, and authentication of terminals and gateways; bandwidth management; accounting; billing; and charging. Gatekeepers can also provide call-routing services.

### 5.4.5.3.4 Multipoint Control Units

MCUs provide support for conferences of three or more H.323 terminals. All terminals participating in the conference establish a connection with the MCU. The MCU manages conference resources and negotiates between terminals to determine the audio or video coder/decoder (CODEC) to use, and it may also handle the media stream.

## 5.4.5.4 Media Gateway Control

The Media Gateway Control Protocol (MGCP) specifies communication between call control elements and telephony gateways. It was conceived partly to address some of the perceived inadequacies of H.323 at the level of centralized network infrastructure. MGCP, in its current form, is a combination of two earlier protocols, Simple Gateway Control Protocol (SGCP) and IP Device Control (IPDC) [11]. The IETF, through its Media Gateway Control (Megaco) Working Group, is working on a standard to replace MGCP; this new standard will use the same architecture and baseline as MGCP but will support asynchronous transfer mode (ATM) [11].

Megaco RFC 3015 (also published as ITU-T Recommendation H.248) was developed by the IETF Megaco Working Group in close cooperation with ITU-T Study Group 16. Megaco addresses the relationship between the Media Gateway (MG) and the Media Gateway Controller (MGC) by standardizing the interface between the Call Control entity (MGC) and the Media Processing entity (MG) in the decomposed Gateway architecture [10]. The MG converts media provided in one type of network to the format required in another type of network, while the MGC controls the parts of the call state that pertain to connection control for media channels in a MG. Megaco may be integrated into such products as central office switches, gateways (trunking, residential, and access), network access servers, cable modems, PBXs, IP phones, and soft phones to develop a convergent voice and data solution [10].

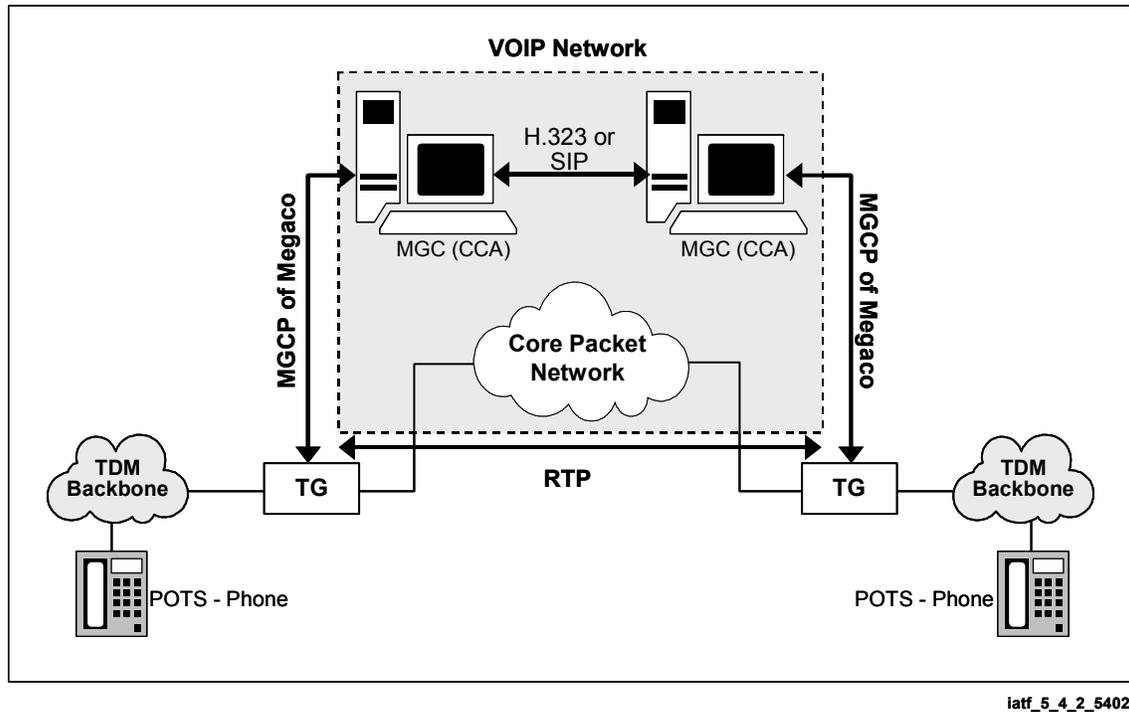
### 5.4.5.4.1 Relationship between Media Gateway Control and H.323 or SIP

MGCP is a complementary protocol to both SIP and H.323 [16]. MGCP and the newer Megaco are designed specifically as internal protocols for traffic between MGCs and MGs for decomposed gateway architectures. H.323 and SIP protocols handle call signaling between MGCs or other H.323 entities (gatekeepers and endpoints). An MGC handles call processing by interfacing with the IP network via communications with an IP signaling device, such as an H.323 gatekeeper or an SIP server and with the circuit-switched network via an optional signaling gateway [16]. The MGC implements the signaling layers of H.323 and presents itself as an H.323 gatekeeper or as one or more H.323 endpoints. MGs focus on the audio signal translation function, converting the audio signals carried on telephone circuits and data packets carried over the Internet or other packet networks [16]. Thus, the Megaco and MGCP protocols complement both H.323 and SIP protocols by providing support for multipoint, multimedia calls at the media level. Figure 5.4-2 illustrates the relationship between the MGCs, MGs, and the signaling protocol.

## 5.4.5.5 Voice over ATM

Asynchronous Transfer Mode, or ATM is a multiservice, high-speed, scalable technology. It is a dominant switching fabric in carrier backbones, supporting services with different transfer characteristics. ATM simultaneously transports voice, data, graphics, and video at very high speeds.

Large enterprises increasingly desire broadband connectivity to the wide area network (WAN) for headquarters and main offices. ATM is one way to provide a broadband connection to accommodate these enterprises' vast amounts of voice and data transmissions, such as heavy graphics, payroll information, and voice and video conferencing.



**Figure 5.4-2. Relationship Between Media Gateway Control Protocol and H.323 or SIP**

ATM networks have the ability to negotiate a traffic contract at connection establishment. For a voice connection, a traffic contract can be negotiated to meet the specific requirements of the connection. In addition, ATM protocols include an ATM adaptation layer (AAL 2) specific to voice. These characteristics make ATM an ideal network for carrying voice traffic. On the down side, ATM services are expensive and are not universally available. Most networks today do not have ATM protocols running from end terminal to end terminal. Instead, ATM is usually used as a backbone or technology to transport IP packets or other network traffic. For voice communications, QoS must be provided end to end. This means that the protocol running over ATM, as well as the ATM network, must establish a traffic contract that can support the voice connection. A voice over ATM architecture is illustrated in figure 5.4-3.

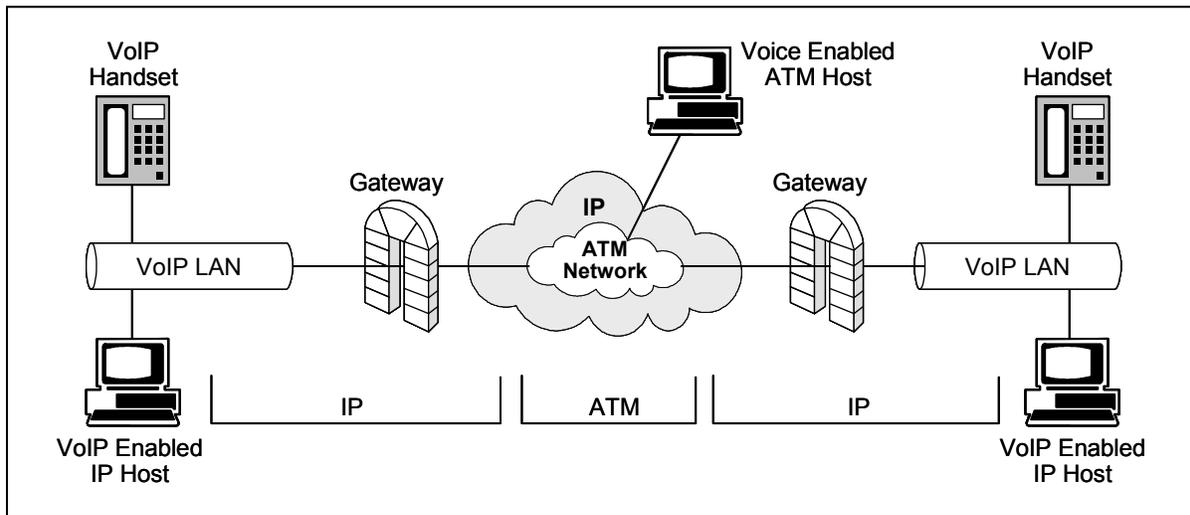
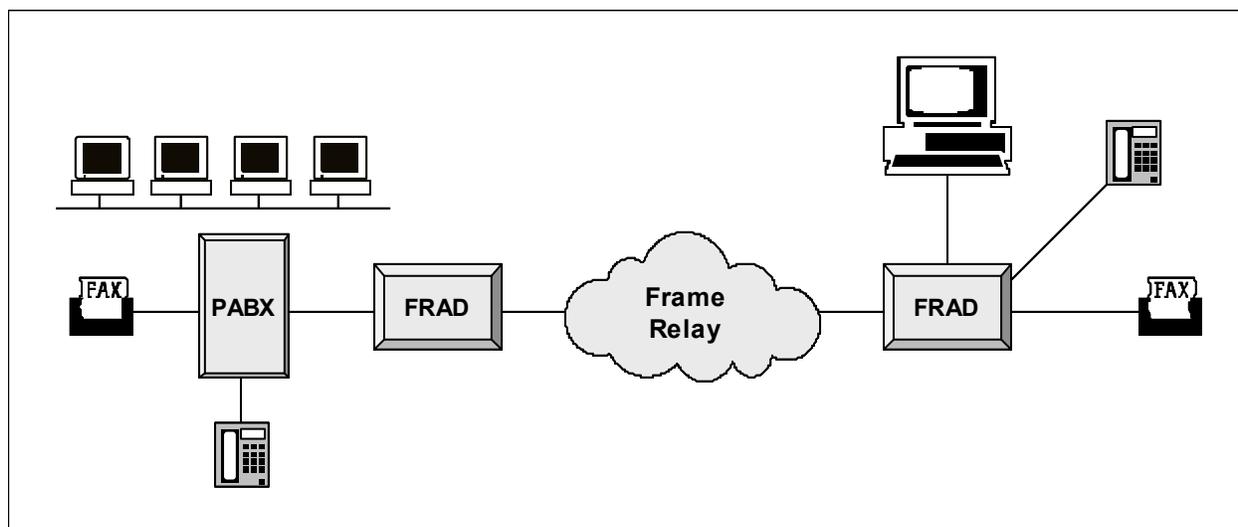


Figure 5.4-3. Voice over ATM

### 5.4.5.6 Voice over Frame Relay

Of the three packet/cell technologies (frame relay, IP and ATM), frame relay is the most widely deployed. Frame relay is commonly used in corporate data networks because of its flexible bandwidth, widespread accessibility, support of a diverse traffic mix, and technological maturity [12]. Initially, frame relay gained acceptance as a means of providing end users with a solution for LAN-to-LAN connections and other data connectivity requirements. In addition to providing a flexible and efficient data transport mechanism, frame relay lowered the cost of bandwidth for tying together multiprotocol networks and devices [14]. Often, it is used as a transport protocol linking two or more IP networks. Although frame relay does specify a minimum throughput for each connection, it does not support a rich QoS scheme. However, it has better QoS characteristics than IP networks and is used to carry both voice and data connections today. A voice over Frame Relay architecture is illustrated in figure 5.4-4.



iatf\_5\_4\_4\_5404

**Figure 5.4-4. Voice over Frame Relay**

Frame relay service is based on permanent virtual connections (PVC). The technology is appropriate for closed user groups and is also recommended for star topologies and situations in which performance must be predictable. VoFR is a logical progression for organization's already running data over frame relay [12].

Sometimes, congestion can occur in frame relay networks; this typically results in being dropped. Because voice connections are less tolerant of dropped frames than are data connections, too many dropped frames can have disastrous effects with voice traffic. There are mechanisms for traffic management in frame relay networks to mitigate congestion conditions. With the ratification of the frame relay forum's (FRF) FRF.11, a standard was established for frame relay voice transport. The Frame Relay Forum Technical Committee developed the Implementation Agreement FRF.11 to define standards for how vendor equipment interoperates to transport of voice across a carrier's public frame relay network.

## 5.4.5.7 Security Issues with Protocols and Equipment

### 5.4.5.7.1 H.235

H.235 is the security portion of the H.323 standard prepared by ITU-T Study Group 16. Its purpose is to provide for authentication, confidentiality, and integrity within the current H-Series protocol framework [13]. In addition to protecting voice traffic itself, H.235 provides protection for Q.931 (call setup), H.245 (call management), and Gatekeeper Registration/Admission/Status (RAS). Version 2 of H.235 supersedes H.235 version 1, featuring several improvements, such as elliptic curve cryptography, security profiles (simple password-based and sophisticated digital signature), new security countermeasures (media anti-spamming), support for the Advanced Encryption Algorithm (AES), support for backend service, definition of object identifiers, and incorporated changes from the H.323 implementers guide [13].

### **5.4.5.7.1.1 H.235 Authentication**

Authentication may be provided in conjunction with the exchange of public-key based certificates. It may also be provided by an exchange that uses a shared secret between the entities involved. This may be a static password or some other a priori piece of information, such as shared secret key methods based on Diffie-Hellman key exchange [13]. H.235 also describes the protocol for exchanging certificates but does not specify the criteria by which the certificates are mutually verified and accepted. The intent behind the certificate exchange is to authenticate the user of the endpoint, not simply the physical endpoint [13]. The authentication framework in H.235 does not prescribe the contents of certificates (i.e., does not specify a certificate policy) beyond that required by the authentication protocol. However, an application using this framework may impose high-level policy requirements, such as presenting the certificate to the user for approval [13].

For authentication that does not use digital certificates, H.235 provides the signaling to complete various challenge-response scenarios. This method of authentication requires prior coordination by the communicating entities so that a shared secret can be obtained [13]. As a third option, the authentication can be completed within the context of a separate security protocol, such as TLS or IPsec [13].

### **5.4.5.7.1.2 Confidentiality**

H.235 articulates a media encryption mechanism for voice streams carried on packet-based transports, to provide confidentiality. Its first step toward this goal was providing an encrypted channel on which to establish cryptographic keying material and/or set up the logical channels, which will carry the encrypted voice streams [13]. For this purpose, when operating in a secure conference, any participating endpoints can use an encrypted H.245 channel. This channel allows cryptographic algorithm selection and encryption key commands to pass protected. If the H.245 channel must be operated in a nonencrypted manner, the specific media encryption keys can be encrypted separately in the manner signaled and agreed to by the participating parties [13]. The confidentiality of the data is based on end-to-end encryption. Confidentiality can be ensured between endpoints only if connections between the trusted elements are proven using authentication.

### **5.4.5.7.2 IPsec**

IPsec was designed to provide interoperable, cryptographically based security for IPv4 and IPv6. The set of security services includes access control, connectionless integrity, data origin authentication, protection against replays, confidentiality, and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection for IP and/or upper layer protocols. Thus, IPsec can be used to protect both VoIP signaling (i.e., SIP and H.323) and VoIP user traffic (i.e., RTP).

IPsec uses two traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), which use cryptographic key management procedures and protocols.

ESP has been widely embraced by industry and there are multiple implementations available. However, AH has not been so widely accepted. ESP can provide an authentication service. While AH has the added benefit of authenticating some of the fields in the IP header, this is not seen as a significant advantage. The key management and security negotiation for IPsec is handled through IKE. IKE is used to establish key material and a security association to be used by ESP.

To use IPsec to protect VoIP traffic, security associations must be established between VoIP components that will communicate. This implies a mesh of security associations. Depending on the number of communicating entities, there can be a large number of IPsec SAs. IPsec can be applied to protect most protocols used with VoIP. It is applied at the network layer, whereas most protocols used with VoIP exist above the network layer (i.e., VoIP signaling at the application layer).

### **5.4.5.7.3 Megaco**

The Megaco standard does not have any security features built into the protocol. It depends on the underlying protocols to provide authentication of the source of communications and security of the content. For VoIP communications, the standard recommends using IPsec's AH to validate the source of packets and the integrity of packets between the MG and the MGC. AH can also be used to protect against replay attacks. IPsec's ESP can be used to protect the confidentiality of the communications between the MGC and the MG, particularly if session keys are to be transmitted in the session descriptions from the MGC to the MG to encrypt audio messages.

In practice, AH is rarely used. Instead, ESP is used to provide authentication and well as integrity and confidentiality. ESP can be employed to build a secure tunnel between the MG and the MGC. This tunnel can then be used to protect all Megaco traffic. Typical networks have only a few MGs and MGCs, which will not create a scaling problem when provisioning the IPsec tunnels.

### **5.4.5.7.4 SIP Security**

The current SIP Internet Draft specifies the same authentication scheme as HTTP. SIP authentication is between a user agent client and a user agent server. Although one application may act as both client and server, the authentication is usually not end-to-end (i.e., user-to-user). Instead, authentication is usually between a user and a server or between two servers. For conference calls, there must be a conference control application to which all participants in the conference must authenticate.

There are two SIP authentication schemes: Basic Authentication and Digest Access Authentication. Basic Authentication transmits passwords in clear text and should not be considered. Digest Access Authentication is a basic challenge-and-response mechanism. The server issues a challenge to the client containing a nonce. A valid response from the client must contain an MD5 hash of the user name, the password, the given nonce, and the request SIP-URL

## UNCLASSIFIED

Security for Voice Over Internet Protocol  
IATF Release 3.1—September 2002

(i.e., user address). This authentication scheme is designed for the client to authenticate to the server, not for the server to authenticate to the client. No provision is made for the initial secure arrangement to user and server of the user's password. Digest Access Authentication is not as secure as a public key authentication or Kerberos authentication.

This authentication scheme specified by SIP should not be confused with the HTTP authentication scheme implemented in commercial browsers. Browsers use the authentication scheme specified by TLS or Secure Socket to Layer (SSL), which is different from the authentication scheme described here.

SIP specifies PGP to provide integrity and confidentiality. The default integrity algorithm for SIP is SHA-1, but MD-5 is also specified. Integrity is provided on a SIP flow across the entire SIP message, but excluding the IP header. SIP flows are usually server to server (proxy server or user agent server) or user to server.

The SIP working group in the IETF has recognized the inadequacy of these provisions. As a result, the SIP working group is defining a security architecture. At present, no time frame has been established for the availability of this new security architecture.

SIP security requires mutual authentication to ensure that both parties are who they claim to be. A mechanism such as JTLS or SSL should not be used alone because these only perform a one-way authentication, typically server to client. In the case of VoIP, both client-to-server and server-to-client authentication are important. SIP security also requires integrity, to ensure that messages are not modified, and confidentiality, to protect against traffic analysis attacks.

An interim solution for SIP security—until the new security architecture is developed by the IETF—is to build protected tunnels between SIP clients and servers. These tunnels could be built using IPsec. SIP servers would require an IPsec SA between each pair of servers. SIP clients would initiate an SA between themselves and their SIP server when they want to make a VoIP call. Each server would communicate to other servers within the network using preestablished SAs. Finally, the servers serving the destination user would initiate an IPsec SA to the destination user for the last leg of the signaling. These IPsec SAs are not user to user. Therefore, they could not be used to protect the RTP stream carrying voice traffic between users. A new IPsec SA is required to be established between users to protect the RTP stream.

### **5.4.5.7.5 Firewall Considerations**

The Real-Time Transport Protocol (RTP) that is used by both SIP and H.323 for carrying VoIP user traffic through the network uses a wide range of ports—10,025 to 65,000—to transport user packets. This makes it difficult to restrict firewall ports to specific types of traffic. VoIP uses four TCP ports per VoIP connection, two for signaling (forward and reverse channel) and two for transport of user information (forward and reverse channel). RTP also typically has been implemented using User Datagram Protocol (UDP), which is commonly blocked at firewalls because it is not connection oriented and is used by streaming applications that consume large quantities of bandwidth. Clearly, opening ports 10,025 to 65,000 and allowing all UDP traffic would severely compromise the security of the network.

There are currently two configurations for overcoming VoIP's firewall issue. The first is dynamic port mapping. This feature may not be offered by all router vendors and operates in a slightly different way with each vendor implementation. The filtering router fronting the firewall receives a VoIP connection that may be on any port between 1,025 to 65,000. The router changes the port to a small range of ports through which the firewall is configured to allow VoIP traffic to pass. This limits the number of ports that must be open on the firewall. However, because four ports are required per VoIP call, the number of open ports can grow quickly if even a moderate number of VoIP users must be supported.

The second configuration is static mapping. In this case, each VoIP user is assigned to a group of four ports on the firewall, which will be used only for a VoIP call that a designated VoIP user initiates. This option requires considerable manual configuration. Each time a VoIP user is added or removed, the configuration must change.

With VoIP, as with many other protocols, the firewall cannot by itself stop an attack that takes the form of an allowed protocol on an approved port. In addition, the need to limit delay will affect the use of intrusion detection systems (IDS) or other filtering and detection mechanisms. This may be an area for future research, to find a means of achieving the same level of protection against malicious code and covert channels in the conveyed network environment that is expected in a data environment.

Another issue involved in using VoIP through a firewall concerns Network Address Translations (NAT). Frequently firewalls use NAT to provide additional security and to allow the use of private addresses within an organization's intranet. The problem with using SIP and NAT together is that the SIP User Resource Locator (URL) addresses can be located in multiple locations in the SIP header (e.g., Request line, the TO field, the FROM field, the VIA field, the Contact field, the Record-route field, the Route field, and the last part of the Call-ID field). The firewall or application server on the public side of the firewall must be intelligent enough to translate all of these address fields into public addresses or to translate public addresses to private addresses if the packet is going into the intranet.

### **5.4.5.7.6 Secure Voice Interoperability (STE/STU/ Wireless)**

STE and STU are approved for carrying secure voice traffic over PSTN and ISDN networks. However, even if a site no longer maintains PSTN or ISDN service, its secure voice requirements will still mandate the use of STEs and STUs to work over the VoIP infrastructure. Therefore, sites will need to carry STE and STU traffic over the packet-based VoIP network.

STE performs its security signaling within the ISDN B channel and does not perform any customized signaling in the ISDN D channel. Therefore, if an ISDN card is installed in a VoIP-capable router, the STE call can proceed transparently to the transport technology. STE users can be connected to an ISDN-capable router and complete secure calls to other STE or STU users. They can also complete nonsecure calls to VoIP users. However, STE users will not be able to complete a secure call to a VoIP user.

STU interoperability is identical to that for STE. If a PSTN interface is provided by a VoIP router, STU signaling can be carried transparently by the VoIP network. STU users can complete secure calls to other STU users across a VoIP infrastructure and nonsecure calls to VoIP users.

A secure wireless terminal uses a customized security signaling protocol for security, called Future Narrow Band Digital Terminal (FNBDT). FNBDT signaling runs at the application layer and can be carried transparently over a VoIP network. Secure wireless users can complete non-secure calls over a VoIP network. They can also complete secure calls to other secure wireless users or to users of a terminal (e.g., STE) that is FNBDT enabled.

The scenarios described for STE, STU, and secure wireless interoperability assume that there is a connection between the enterprise VoIP network and the PSTN.

#### **5.4.5.7.7 Signaling System 7 Security Issues**

Enterprise VoIP networks will require connectivity to a wide area PSTN to allow VoIP users to communicate with PSTN users. This connectivity requires that the VoIP control plane interoperate with the PSTN control plane. The PSTN control plane is based on Signaling System 7 (SS7). One of the basic design considerations for SS7 was that it would be a closed network, and PSTN users would not have access to the SS7 network. However, connecting a packet-based VoIP network to the PSTN opens up connectivity between nodes on the enterprise IP network and the SS7 network.

#### **5.4.5.7.8 Performance Considerations**

VoIP technologies are very sensitive to jitter, latency, and other network parameters. Therefore, the network must be properly provisioned. There must be sufficient bandwidth and network resources available in the enterprise to accommodate the increased demands of VoIP traffic. An improperly provisioned network may provide degraded service for both VoIP and existing data applications. In addition, the network must have a QoS policy in place. Part of the QoS policy may mandate the use of Diff Serv, MPLS, RSVP, or another QoS mechanism. These QoS mechanisms also require security. It is possible for an unauthorized user to use QoS mechanisms to reserve a large portion of the network bandwidth or resources, leaving little or no resources available for other applications.

QoS protocols do not have adequate security functionality built into them. Although, some protocols (e.g., RSVP) have an integrity checksum, which also provides some limited authentication, confidentiality, key management, and a strong authentication mechanism are also required.

Because of QoS protocols' lack of security, the current best security recommendations for these protocols in the enterprise are to restrict access to the network to authorized individuals and to implement good personnel security. Good access control and authentication mechanisms should be used to in place to limit access to the routers. It is possible to limit access to QoS protocols in

an enterprise network that is owned, operated, and used by the same organization. However, this recommendation is not feasible in a network in which services may be leased and shared by other organizations (i.e., a WAN).

Bandwidth and performance that may have been acceptable for data applications may not be acceptable for voice. Today, most networks do not have QoS mechanisms. Therefore to accommodate the increased timeliness demands of voice, overprovisioning may be necessary. Overprovisioning, in concert with good traffic management, can provide an acceptable interim solution until QoS mechanisms can be deployed.

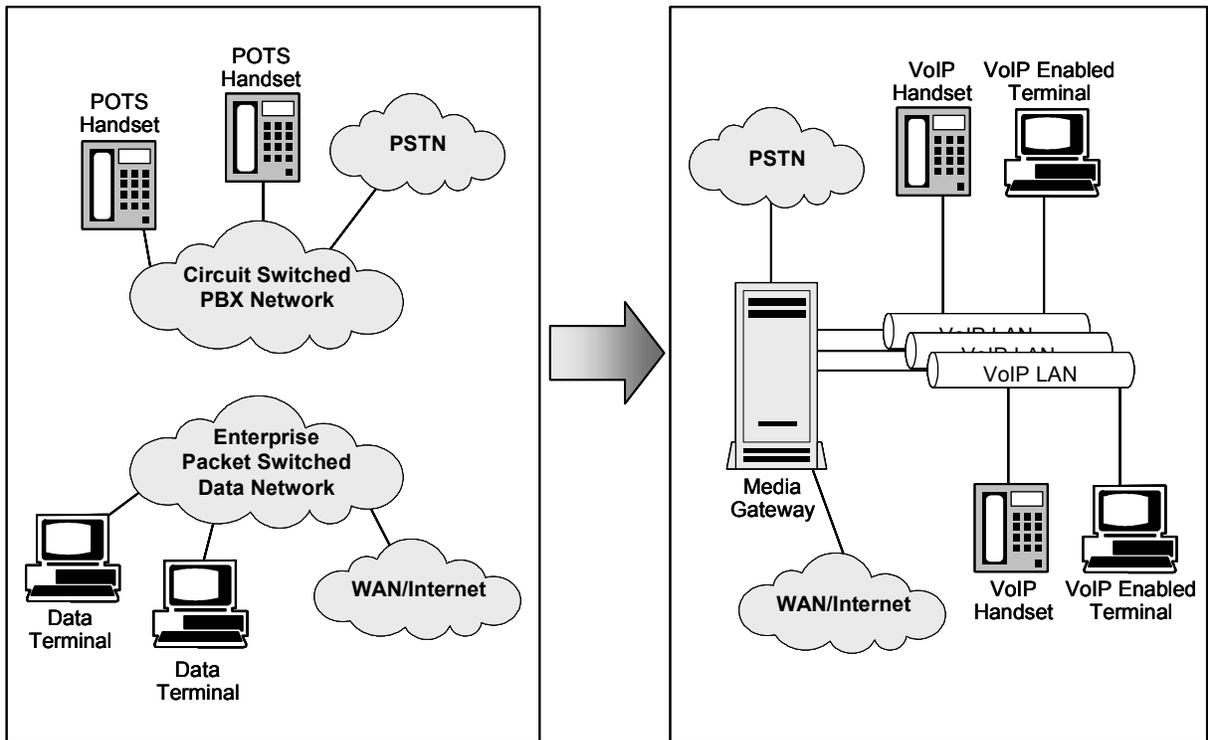
## 5.4.6 Cases

### 5.4.6.1 Integrating a VoIP Capability with an Existing Infrastructure

This scenario considers a case in which an enterprise network that has been used to carry data applications is augmented to carry voice traffic. It is assumed that the network is owned and operated by a single organization and that the organization manages the network and has authority to perform upgrades. The circuit-switched network used by the organization may be phased out entirely, or a small circuit switched capability may remain. The organization expects the same voice quality and reliability for voice traffic over the packet-switched network that it has expected from the circuit-switched voice network. Connectivity to the PSTN will be maintained. The organization also assumes that performance for existing data applications will not suffer. An additional assumption is that there is no QoS on the network. All traffic is best effort. This scenario is illustrated in figure 5.4-5.

The first step in this scenario is to determine what additional bandwidth requirements the voice applications will place on the network. The existing network may be capable of meeting the demands of data applications; however, additional bandwidth for the enterprise network and for external connectivity will be required to support voice service. It is unwise to simply add voice service to an existing network without understanding the additional stresses. Voice applications are less tolerant to delay, jitter, and other QoS parameters. Levels of performance that had been acceptable for a data network may fall short for use of a voice application. Typically, access links are the points at which most network congestion occurs. Additional voice traffic will put additional stress on these links, and they must be augmented accordingly.

Some organizations may want to maintain a limited circuit-switched phone system for emergency use. The packet network will be subject to increased stress during emergencies. In addition, attacks and viruses that may degrade the performance of the network will also now degrade the performance of the voice service. A limited circuit-switched capability can aid in the recovery efforts of the packet network, if degraded performance occurs.



latf\_5\_4\_5\_5405

**Figure 5.4-5. Integrating a VoIP Capability onto an Existing Network**

Many of the protocols that are required to support VoIP are not hardened. Therefore, VoIP security for an enterprise environment must rely heavily on physical security, controlling access to network devices, and personnel security. All network management traffic to VoIP network components should be protected with confidentiality, integrity, and authentication.

To protect VoIP signaling information, tunnels using IPsec can be created between VoIP enclaves, between VoIP users and VoIP servers, and between VoIP servers. Protection is not possible for communications between all external entities. However, calling patterns can be analyzed to determine which organizations frequently communicate. An IPsec tunnel can then be established between these organizations to pass VoIP signaling information.

When a call is placed between a VoIP user and a PSTN user, the security provided by an IPsec tunnel will stop at the PSTN gateway. For protection of calls between VoIP users and PSTN users, the PSTN gateway must be hardened. Management access to the gateway must be limited and protected. The router fronting the gateway should be configured to filter addresses that are not authorized to use or access the gateway. Management traffic between the gateway and the management station should be protected with confidentiality, integrity, and authentication. Protection of the gateway from the SS7 side will require further study.

## 5.4.6.2 Building a VoIP Capability

This scenario addresses a case in which a new network is being created to handle voice, video, data, and other multimedia traffic. It is assumed that the network is owned and operated by a single organization and that the organization manages the network and has authority to perform upgrades. There will be either no circuit-switched voice network installed or a very limited service to accommodate mission-critical applications. The organization expects the same voice quality and reliability for voice traffic that is expected from a circuit-switched voice network. This scenario assumes that there is no QoS on the network. All traffic is best effort.

In building a new network that will carry both VoIP traffic and traditional data traffic, a network designer must consider the bandwidth demands voice will place on the network. Faster network protocols, such as Fast Ethernet and Gigabit Ethernet, should be considered for the enterprise network. Although protocols such as these may not have integrated QoS, they may be more effective for voice just because of their speeds. These protocols can also help provide over provisioning, which can be used to offset or compensate for the lack of QoS mechanisms.

Other than some flexibility with design considerations and bandwidth allocation, the security issues that apply in creating a new VoIP network are the same basically as those involved in adding VoIP service to an existing network. Thus, the same security recommendations apply to this scenario that applied to the previous scenario.

## 5.4.7 Framework Guidance

Perhaps the most important guidance that can be provided to those attempting to implement VoIP securely is that it is inherently a systems engineering task, rather than a matter of plugging in the various boxes. Although the realms of telephone systems and data networks are each well understood to a notable degree in regard to functionality and security, the intersection of these distinct systems in a converged VoIP environment creates three new sets of complications.

First, the convergence creates new risks for the phone aspect of the system. For example, wiretaps by agents other than by law enforcement are now relatively rare, because they require both physical access to the circuit in question and knowledge that is not widely available outside the telecommunications industry. It is not that implementing a wiretap is difficult, just that it is not a commonly known technique. However, once the shift to VoIP is accomplished the knowledge, tools, and access needed to monitor a phone conversation (e.g., packet sniffing tools, protocol information, and access to the packets themselves) will be far more available in the network environment. Placing a “wiretap” on a VoIP network is not necessarily easier than doing so in the traditional phone system. In fact, in many ways it is more complicated technically. In addition, “sniffing packets” is commonly accepted, having many legitimate uses. Thus, both the technical and the social barriers to wiretapping will much lower in a data network environment.

Similarly, the introduction of VoIP creates new risks for the existing data networks. An example of this might be the need to open ports in existing firewalls to allow VoIP traffic to go through

without adding delay. Clearly, this will leave new holes in the perimeter that may be exploited by intruders, or by malicious insiders. This problem is not insurmountable, but requires an awareness of the new dynamics created by the addition of VoIP.

Lastly, there will likely be some new class of vulnerability that is based on synergetic interaction between either the base technologies, or the security mechanisms that support them. Again, the proper attitude is not acceptance of lessened security, but rather an awareness that the convergence of these two previously independent technologies and infrastructures creates unanticipated complications and permutations that must be analyzed carefully and addressed. As yet, this is not a plug-and-play security situation, and this will probably be the case for some time, as is typical for any new technology. The early adopters will need to proceed with skill and caution to create viable solutions to their specific challenges.

## 5.4.8 Technology Gaps

The major technology gaps in the VoIP security realm are as follows:

- **Intrusion Detection.** Currently, there is little available capability to combine IDS monitoring of data and voice traffic. This situation is not so much the result of theoretical limitations as a consequence of the technology's still being in the early-adopter. Although, there are some IDS products designed for use on PBXs, we are still at the base of the learning curve in our understanding of the sorts of attacks that might piggyback on top of voice protocols, punch through the openings in firewalls that must be present for voice traffic to pass, or otherwise exploit vulnerabilities created by the convergence of voice and data on the same network. There will probably be a need to detect attacks and probes on both message traffic and control signaling portions of voice protocols and equipment. Both host-based and network based IDSs with this capability may be needed.
- **Identification and Authentication.** Given the reduced isolation of control signaling in VoIP compared with the traditional phone system, there is a need for a strong I&A capability to protect access to the control functions. This capability might be built into the equipment or might be a separate functionality positioned between the equipment and the network. I&A may also be needed to link a particular phone address to a user or location.
- **Encryption.** Although, existing crypto products can be used to provide trunk encryption, link encryption, or even end-to-end encryption, there will be a need for encryption functionality to be better integrated with and tuned to the specifics of VoIP usage, with special focus on reducing delay.
- **Firewalls, Guards, and Downgraders.** Each of these devices serves to separate an enclave from the outside world or the rest of the network. The need to limit latency, jitter, and delay necessitates a review of the design of these devices in the context of the converged network. The same openings that allow voice traffic to pass unimpeded may also either create high-bandwidth covert channels for data infiltration or exfiltration or

provide a point of entry for other probes and attacks. Although it may be impossible to examine voice traffic in real time without incurring unacceptable delay, it may be possible to isolate the voice traffic in some way from the rest of the network to minimize the vulnerabilities introduced by opening these entry points.

- **Integration.** It remains to be seen whether fully integrating voice with data is the best way to take advantage of packet-switched digital voice. It might be preferable to isolate the packet-switched digital voice on a separate network. In either case, well-thought-out systems engineering focused on the interactions and interdependencies of the whole system is the preferred approach rather than an ad hoc box-based mix-and-match solution focused on individual functions.
- **Graceful Degradation.** Although, a well-designed implementation of packet-switched voice will have factored uninterruptible power and fault tolerance into the plans, a converged network will still be a single point of failure in a way that totally separate data and telephone infrastructures were not. The security implications of this fact should be considered in whatever steps are taken to increase robustness and reliability.

## 5.4.9 Summary of Important Concepts

At this point in the evolution of VoIP, the key considerations are as follows:

- This is a new technology and, like any other new technology, involves a learning curve. This situation requires caution, and careful consideration of how one implements the technology. Be aware that unexpected vulnerabilities may be uncovered and that the technology may change course, rendering early implementations “nonstandard.” The same cautions apply to any efforts to secure the technology.
- Converging voice and data infrastructures is a systems engineering problem. The combination and interaction of previously isolated infrastructures, each with a distinct conceptual basis, will likely have at least some unintended results: some good, some harmless, some bad. Careful analysis of the system as a whole is crucial if the security risks are to be adequately identified, evaluated, and addressed.
- Voice connectivity is such a basic and widespread service that the pressure to attain a high level of functionality, even at the expense of security, will be greater than it might be in a less pervasive application. It is therefore critical that security be designed into the system to as great an extent as possible, so that it is not sacrificed later in a trade-off decision during system upgrades.
- Legal, regulatory, and policy issues may affect the design requirements of the system in unanticipated ways. It is therefore important to be aware both of current legal/regulatory/policy requirements and of those that are being proposed or discussed as you design your VoIP system.

## UNCLASSIFIED

Security for Voice Over Internet Protocol  
IATF Release 3.1—September 2002

### References

1. <http://www.ietf.org/html.charters/sip-charter.html>
2. <http://www.sipforum.org/>
3. <http://www.sipcenter.com/aboutsip/sip.htm>
4. <http://www.sipcenter.com/files/whatisip.pdf>
5. [http://www.packetizer.com/iptel/h323/whatsnew\\_v3.html](http://www.packetizer.com/iptel/h323/whatsnew_v3.html)
6. [http://www.packetizer.com/iptel/h323/whatsnew\\_v4.html](http://www.packetizer.com/iptel/h323/whatsnew_v4.html)
7. <http://iptel.org/info/trends/sip.html>
8. Overview of H.323, Cisco Gatekeeper External Interface Reference, version 3. Cisco IOS Release 12.2(2)XA
9. “Megaco and MGCP.” *Network Magazine*. October 5, 2000 (Doug Allen, senior editor, can be reached at [dougallen@cmp.com](mailto:dougallen@cmp.com)).
10. <http://www.hssworld.com/voip/stacks/megaco/megaco.htm>
11. Elachi, Joanna. Standards Snapshot: The State of the Big 3 in VoIP Signaling Protocols. November 27, 2000.
12. Gil Biran. Voice over Frame Relay, IP and ATM: The Case for Cooperative Networking. <http://www.protocols.com/papers/voe.htm>
13. International Telecommunication Union ITU-T H.235 Version 2 (11/2000)  
Telecommunication Standardization Sector of ITU
14. Frame Relay Forum: Market Development & Education Committee and Technical Committee, White Paper: A Discussion of Voice over Frame Relay, August 2000.
15. <http://www.frforum.com/>, The Basic Guide to Frame Relay Networking
16. <http://www.esoft.com.tw/product/mgcpo.htm>

## 5.5 Multiple Security Layers

Users are struggling to implement networks in which information of different classification levels are being transported over the same backbone. Users are using need-to-know to create communities of interest. The network is being relied on to provide data separation for each compartment. Guards that allow information to migrate from one compartment to another is a technology gap. Labels at the network layer, Closed User Groups (CUG), and encryption are all technologies being investigated to provide reliable data separation. A new section to be supplied in a later release of the framework.

This section will be provided in a later release of the framework.

**UNCLASSIFIED**

Multiple Security Layers  
IATF Release 3.1—September 2002

**This page intentionally left blank.**