AN INTRODUCTION TO SECURE TELEPHONE TERMINALS

Computer Systems Laboratory Bulletin
March, 1992

This bulletin addresses several frequently asked questions about secure telephone terminals, discusses practical security issues from a federal user's viewpoint, and provides sources for additional information. A secure telephone terminal is a device that connects to a telephone line or a cellular telephone system and provides a variety of security services to the conversation or information being transmitted.

Secure telephone terminals are becoming more widely available for the protection of both classified and unclassified voice, data, and facsimile (fax) communications (most modern secure telephones have a data port for connecting to computers or fax machines). The secure terminals range in capability from protecting conversations between the handset and the base terminal in cordless telephones to protecting national security classified information in fixed and mobile telecommunications.

BACKGROUND

Federal Roles and Responsibilities

Each federal agency is responsible for the security of its own information processing and telecommunications. In accordance with the Computer Security Act of 1987, each agency is responsible for identifying the unclassified, but sensitive, information to be protected and for selecting the equipment or procedures to be used in providing the protection. In accordance with applicable National Security Directives (NSDs) such as NSD 42, agencies are also responsible for protecting classified information using National Security Agency (NSA)-approved information security systems.

The National Institute of Standards and Technology (NIST) is responsible for developing standards for, and providing assistance to, agencies in protecting their unclassified information. NSA is responsible for providing the security necessary to protect classified information and "Warner Amendment" sensitive information.

Additional information on the roles of NIST and NSA in the computer security area is contained in the CSL Bulletin of February 1991. Other agencies, such as the General Services Administration, the National Telecommunications and Information Administration, and the National Communications Agency, also provide specific services and guidance in utilizing secure telecommunications.

Technology Overview

Most current telephone terminals and transmission facilities are based on and use analog electromechanical and electronic technology. This technology models the human speech communication system which produces (in the voice box), receives (through the ears), and processes (in the brain) continuous waveforms of speech. Early forms of secure voice communication simply scrambled the voice signals to produce unintelligible noise which was then transmitted. The descrambling equipment would convert the noise back to recognizable speech.

Modern telephone terminals and transmission facilities use digital technology which utilizes a sequence of the binary digits 0 and 1 to represent computer data, human speech, or fax pictures. Existing analog telecommunications systems can transmit digitized voice, data, and pictures using a special device called a modem.

Modems provide transmission rates generally up to 9600 bits per second. Thousands of bits per second can be communicated with moderate technology digital communications systems and millions of bits per second can be communicated with high technology systems. Voice, data, and pictures can be mixed on the same transmission medium (e.g., optical fiber) and separated for presentation to the intended recipient. This is the basis of the modern Integrated Services Digital Network (ISDN). Improved security can be provided to these communications by simply permuting or encoding the bits that represent the speech, data, and pictorial images.

Current Status of Secure Telephone Terminals

Commercial "cordless" telephones are presently available which protect conversations between a handset and its base station. Unprotected cordless telephones have a usual range of approximately 100 feet and conversations can sometimes be picked up by an identical base station located in a neighbor's house. These "protected" telephones typically use a simple coding system, with a number of user-selected codes, to prevent someone from passively listening to a conversation. These telephones also protect against someone making a long-distance telephone call from a handset outside a residence to avoid the long-distance charges. These telephones provide protection against what is considered a low level of threat.

Commercial cellular telephones are vulnerable to scanning devices that are designed to monitor telephone conversations within a local "cell." Some cellular services are beginning to offer protection to local subscribers for their communications between a cellular terminal and the nearest cellular switching office. However, they do not protect the communications to a remote telephone or cellular terminal. These secure cellular telephones provide protection against local threats.

During the early 1980s, NSA sponsored a development program which resulted in the Secure Telephone Unit (STU) III terminal. The STU-III looks like a typical telephone but provides end-to-end security between any two STU-III devices, even those manufactured by different vendors. Three U.S. vendors are authorized to make the devices: AT&T, General Electric, and Motorola. The STU-III utilizes current analog telephone communications but secures the speech signals by digital security techniques. There are also cellular STU-III terminals which provide "end-to-end" security between any two cellular STU-III terminals or between a cellular mobile terminal and a fixed terminal. The STU-III terminals provide protection against what is considered a high level of threat.

GOVERNMENT POLICY AND REGULATIONS

Government policy exists on the protection of classified communications; classified information (voice/data/fax) must be encrypted for transmission using cryptographic algorithms implemented in devices endorsed by NSA. Cryptographic key used for these applications is provided via NSA-approved Communication Security (COMSEC) methods.

There is no specific government policy that directs agencies to encrypt all unclassified sensitive communications. Circular A-130, issued by the Office of Management and Budget, directs agencies to assure that an appropriate level of security is maintained in all information technology installations and to conduct periodic risk analyses to assure that appropriate cost-effective safeguards are used. NIST develops the technical standards that can be used for this protection. An agency determines when such protection is needed.

Types of Cryptographic Algorithms and Security Devices Four types of cryptographic algorithms and security devices are defined in the National Information Security (INFOSEC) glossary [NSTISSI No. 3019]. Type 1 cryptographic devices are endorsed by NSA and contain classified algorithms approved by NSA for securing classified information. Type 2 cryptographic devices are endorsed by NSA and contain classified algorithms approved by NSA for protecting Department of Defense unclassified information covered by the Warner Amendment (10 USC 2315). Type 3 cryptographic algorithms are NIST standards to be used for protecting all unclassified, sensitive, non-Warner Amendment government information or commercial information. Type 4 cryptographic algorithms are commercial algorithms that are not NIST standards. NIST plans to establish a Computer Security Objects Register (CSOR) to include information about these algorithms.

In order to facilitate interoperability among diverse user communities, security devices may contain more than one type of algorithm. For instance, a Type 1 STU-III terminal also contains a Type 2 algorithm. A Type 2 STU-III terminal contains the same Type 2 algorithm but also implements the Data Encryption Standard (DES). A Motorola Type 3 (i.e., DES) secure telephone terminal is not a STU-III but does interoperate with the Motorola Type 2 STU-III when using the DES algorithm. The other STU-III vendors (i.e., AT&T and General Electric) are also developing Type 2 STU-III devices that contain the DES for protecting sensitive or valuable non-Warner Amendment information.

Security for Voice/Data/Fax

Modern telecommunications applications integrate voice, data, and pictures in a single digital communication system. Modern cryptographic algorithms and security devices can protect all of these integrated applications. Users can often utilize one device for all applications.

Security may include different protection services, depending on the application and device. All secure telephone terminals protect information from unauthorized disclosure to varying degrees. Most provide some type of authentication of the terminals and access control for the person or computer using the terminal. Most provide communications integrity (i.e., protection of the transmitted information from unauthorized modification or replacement). Users should specify the type and level of protection desired when procuring a secure telephone terminal.

EXPORT OF SECURE TELEPHONE TERMINALS

All security devices that encrypt information are subject to U.S. export control. Devices that encrypt voice/data/fax must have an export license issued by the U.S. Department of State before they can be legally shipped or taken out of the country. Software systems that encrypt voice/data/fax are subject to the same restrictions. Thus users of secure telephone terminals within the U.S. must be aware of export restrictions if they wish to communicate securely with someone overseas.

STU-III devices may be used outside the U.S. and Canada only with NSA permission. Type 4 security devices may be exportable if they contain only cryptographic algorithms approved for export; these are designated as Type 4(E) devices. Some Type 3 secure telephones also contain a Type 4(E) algorithm for international communication with a compatible Type 4(E) device. At present, there are no Type 3(E) (i.e., exportable DES protected) secure telephones in existence.

SECURE TELEPHONE TERMINAL STANDARDS

The NSA STU-III development program demonstrated the need for tightly controlled standards in order to assure interoperability among STU-III devices of different vendors. The STU-III program not only specified the algorithms and protocols to implement but also provided conformance and interoperability tests for the STU-III terminals.

NIST has issued two standards related to data encryption. Federal Information Processing Standard (FIPS) 46-1 defines the Data Encryption Standard (DES) algorithm. FIPS 81 specifies four modes of operation for the DES. In addition, FIPS 140-1, expected to be issued in 1992, will specify physical and logical security requirements for a cryptographic module. These standards are applicable to Type 3 secure telephone terminals. NIST does not issue standards for Type 4 devices.

Security

Security is provided in STU-III devices via NSA-specified algorithms and key management systems. Type 3 devices use the DES for encrypting information but presently use proprietary techniques for generating or distributing the needed DES keys. Type 4(E) secure telephone terminals use proprietary techniques for both.

Interoperability

NSA specifies how interoperability is achieved in STU-III terminals when using the Type 1 and Type 2 modes. Motorola specifies how interoperability is achieved between their Type 3 secure telephone and their Type 2 STU-III telephone when both are using the DES mode. Motorola also achieves interoperability between the same Type 3 secure telephone and their Type 4(E) secure telephone. They provide a proprietary key management system for their commercial secure terminals using public-key technology. The other STU-III vendors use proprietary techniques for key management for the Type 3 mode of operation.

At the present time, Type 3 terminals from one vendor do not interoperate with Type 3 terminals from other vendors. Commercial users should be aware of this when procuring such terminals. Government users of Type 2 STU-III terminals cannot interoperate with Type 3 terminals procured from a different vendor. Type 4 or 4(E) terminals of different manufacturers also typically do not interoperate. Procurement documents should specify the interoperability required.

ADDITIONAL SECURITY REQUIREMENTS

Users should be aware of additional security requirements when using secure telephone terminals. Type 1 STU-III requirements are specified in the Operational Security Doctrine (NSTISSI No. 3013). Type 2 STU-III requirements are specified in an Interim Operational Security Doctrine (Draft NSTISSI). Users of Type 3 and Type 4 secure terminals should be aware of and follow similar security requirements and practices.

A secure terminal must be provided adequate physical security to protect it and its physical environment from unauthorized use, acquisition, access, modification, or installation of monitoring devices. A physical and logical access control system must be supported. Terminal and user identification systems are required and must be administratively supported for authorized users. Terminals capable of operating in unattended data communication modes must have adequate internal access control mechanisms to prevent unauthorized outgoing or incoming transmissions. Adequate cryptographic key control is required. Since the entire security of the terminal is based on protecting the cryptographic key from unauthorized disclosure, replacement, or use, such protection must be continuously provided. Keys should be destroyed when no longer useful.

SUPPORT INFRASTRUCTURE

Similar to the communications services infrastructure that is available nationally and internationally to support telephone communications, a security services infrastructure must be available to support communications among secure telephones. NSA provides these services for authorized users of STU-III terminals. Users of Type 3 or Type 4 security devices should be aware that key management and trusted maintenance must be provided to maintain secure operation.

Sales

With the exception of Canada, sales of STU-III terminals (Type 1 and Type 2) are limited to the U.S. government and their contractors. Type 1 STU-III terminals may be purchased for the protection of U.S. government classified information. Type 2 STU-III terminals may be purchased to protect all U.S. government sensitive unclassified information: Type 2 mode for Warner Amendment information and Type 3 mode for all other sensitive unclassified information. Type 3 Secure Telephone Terminals may also be procured by the U.S. government if they contain and are built to applicable Federal Information Processing Standards. These terminals should also be used in accordance with applicable NIST standards.

Type 3 secure terminals may be purchased within the U.S. for the protection of commercial information and for interoperability with compatible Type 2 STU-III terminals. Type 4(E) terminals may be purchased anywhere for use in commercial applications overseas and for interoperability with secure terminals within the U.S. that support a compatible Type 4(E) algorithm.

Type 1 STU-III terminals may not be resold and Type 2 STU-III terminals can be resold only to those approved by NSA. Type 3 secure terminals may be sold and resold anywhere in the U.S. Type 4(E) secure terminals may be sold anywhere.

Commercial products are being manufactured which provide a wide range of security. Users should be aware of the benefits and limitations of commercial security products. Federal users should procure and use only appropriate government-approved security devices for protecting federal classified or unclassified, but sensitive, information.

REFERENCES

Computer Security Act of 1987, Public Law 100-235.

Federal Information Processing Standard 46-1, Data Encryption Standard (DES).

Federal Information Processing Standard 81, DES Modes of Operation.

Draft Federal Information Processing Standard 140-1, Security Requirements for Cryptographic Modules.

National Security Directive 42 (Issued by the National Security Telecommunications and Information Systems Security Committee).

National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 3013, Operational Security Doctrine for the Type 1 STU-III Terminal.

Draft NSTISSI, Interim Operational Security Doctrine for the Type 2 STU-III Terminal.

Office of Management and Budget Circular A-130, Management of Federal Information Resources.

POINTS OF CONTACT

STU-III Users Support: (800) 328-7883 (Outside MD)

(301) 684-7073 (Inside MD)

NIST Computer Security Division: (301) 975-2934