Designation: E 2086 – 00

An American National Standard

Standard Guide for Internet and Intranet Healthcare Security[1]

This standard is issued under the fixed designation E 2086; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This guide covers mechanisms that can be used to protect healthcare information which is being transmitted over networks using the Internet Protocol Suite (IPS). This includes the actual Internet itself, as well as corporate intranets constructed from off–the–shelf components implementing these protocols. An organization's security policy will determine when these mechanisms are used, based on risk analysis.

1.2 The Internet Engineering Task Force (IETF) is defining security standards for use with the IPS. This guide covers the relevant standards and recommends, where needed, particular options (such as cryptographic transformations) to be used with the standards. Most standards referenced here are proposed standards issued as Requests for Comments (RFCs). Some are in the draft stage, but are stable enough (and widely enough implemented) to be recommended for use at this time.

2. Referenced Documents

2.1 *IETF Standards:*[2]

RFC 1510 Kerberos Authentication Service
RFC 1777 Lightweight Directory Access Protocol (v2)
RFC 2251 Lightweight Directory Access Protocol (v3)
RFCs 1901–1910 Simple Network Management Protocol
RFC 1945 Hypertext Transfer Protocol
RFC 1964 Kerberos v5 GSS-API Mechanism
RFC 2246 The TLS Protocol Version 1.0
RFC 2401 Security Architecture for the Internet Protocol
RFC 2402 IP Authentication Header
RFC 2403 The Use of HMAC-MD5–96 within ESP and AH
RFC 2404 The Use of HMAC-SHA-196 within ESP and AH
RFC 2406 IP Encapsulating Security Payload (ESP)
RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP
RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2409 The Internet Key Exchange (IKE)
RFC 2411 IP Security Document Roadmap
RFC 2440 OpenPGP Message Format
RFC 2451 The ESP CBC-Mode Cipher Algorithms
RFC 2560 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol
RFC 2630 Cryptographic Message Syntax
RFC 2631 Diffie-Hellman Key Agreement Method
RFC 2632 S/MIME Version 3 Certificate Handling
RFC 2633 S/MIME Version 3 Message Specification
RFC 2634 Enhanced Security Services for S/MIME

2.2 *Other Standards:*

FIPS PUB 180–1 Secure Hash Algorithm

3. Terminology

3.1 *Definitions:*

3.1.1 *algorithm*—a clearly specified mathematical process for computation; a set of rules which, if followed, will give a prescribed result.

3.1.2 *asymmetric cryptography*—cryptographic algorithm that uses two related keys, a public key and a private key; the two algorithm keys have the property that, given the public key, it is computationally infeasible to derive the private key.

3.1.3 *authentication*—the corroboration that the source of data received is as claimed.

3.1.4 *authorization*—the granting of rights.

3.1.5 *cipher text*—data in its enciphered form.

3.1.6 *clear text*—data in its original, unencrypted form.

3.1.7 *confidentiality*—the property that information is not made available to or disclosed to unauthorized individuals, entities, and processes.

3.1.8 *cryptographic checkvalue*—a value computed using a shared secret key and a data unit, which can be used to provide data integrity and authentication services.

3.1.9 *cryptography*—the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification, prevent its unauthorized use or a combination thereof.

3.1.10 *datagram*—a data unit that is delivered independently of other data units transmitted over a network.

3.1.11 *data integrity*—a property whereby data has not been altered or destroyed.

[1] This guide is under the jurisdiction of ASTM Committee E31 on Healthcare Informatics , and is the direct responsibility of Subcommittee E31.25 on Healthcare Management, Security, Confidentiality, and Privacy.

Current edition approved April 10, 2000. Published June 2000.

[2] Available on line at ftp://ds.internic.net.

3.1.12 *decryption*—a process of transforming ciphertext into plaintext.

3.1.13 *digital signature*—a cryptographic transformation of data which, when associated with a data unit, provides the services of origin authentication, data integrity, and signer non–repudiation.

3.1.14 *encryption*—a process of transforming plain text (readable) into cipher text (unreadable) for the purpose of security or privacy.

3.1.15 *encryption key*—a binary number used to transform plain text into ciphertext.

3.1.16 *gateway*—a computer system or other device that acts as a translator between two systems that do not use the same communications protocols, data formatting, structures, languages, or architecture, or a combination thereof.

3.1.17 *intranet*—an internal corporate network which uses the Internet protocol suite (TCP, IP, etc.)

3.1.18 *non–repudiation*—this service provides proof of the integrity and origin of data, both in an unforgeable relationship, which can be verified by any party.

3.1.19 *plain text*—data in its original, unencrypted form.

3.1.20 *repudiation*—the denial by a user of having participated in part or all of a communication. (See *non–repudiation*, which has the opposite meaning.)

3.1.21 *replay*—the process of sending a previously sent message as a method of perpetrating a fraud.

3.1.22 *security association*—the relationship between two entities which allows the protection of information communicated between the entities.

3.1.22.1 *Discussion*—This relationship includes a shared symmetric key, and security attributes describing the relationship. The security association is used to negotiate the characteristics of these protection mechanisms, but does not include the protection mechanisms themselves.

3.1.23 *session*—logical relationship between two network endpoints that supports a user or network application.

3.1.24 *subnetwork*—a network segment, usually with its own address.

3.1.25 *symmetric encryption*—encryption using a single key to encrypt and decrypt which both the sender and receiver hold privately.

3.1.26 *virtual private network*—a network which uses the Internet as a carrier, but is operated as a dedicated point-to-point network.

3.1.26.1 *Discussion*—Encryption is used to segregate and protect the VPN's data when it is conveyed over the Internet.

3.2 *Acronyms:Acronyms:*

3.2.1 *AH*—Authentication Header

3.2.2 *API*—Application Programming Interface

3.2.3 *ASTM*—American Society for Testing and Materials

3.2.4 *ATM*—Asynchronous Transfer Mode

3.2.5 *DEC*—Digital Equipment Corporation

3.2.6 *DES*—Data Encryption Standard

3.2.7 *DSA*—Digital Signature Algorithm

3.2.8 *EDI*—Electronic Data Interchange

3.2.9 *ESP*—Encapsulating Security Payload

3.2.10 *FTP*—File Transfer Protocol

3.2.11 *GSS*—Generic Security Services

3.2.12 *HMAC*—Hashed Message Authentication Code

3.2.13 *HTTP*—HyperText Transfer Protocol

3.2.14 *IDUP*—Independent Data Unit Protection

3.2.15 *IETF*—Internet Engineering Task Force

3.2.16 *IP*—Internet Protocol

3.2.17 *IPS*—Internet Protocol Suite

3.2.18 *IPSEC*—Internet Protocol Security

3.2.19 *ISAKMP*—Internet Security Association and Key Management Protocol

3.2.20 *LAN*—Local Area Network

3.2.21 *MD*—Message Digest

3.2.22 *MIME*—Multipurpose Internet Mail Extension

3.2.23 *PCT*—Private Communications Technology

3.2.24 *PIN*—Personal Identification Number

3.2.25 *PKCS*—Public–Key Cryptography Standards

3.2.26 *RFC*—Requests for Comment

3.2.27 *RSA*—Rivest, Shamir, and Adelman

3.2.28 *SHA-1*—Secure Hash Algorithm

3.2.29 *S–HTTP*—Secure HyperText Transfer Protocol

3.2.30 *S/MIME*—Secure/Multipurpose Internet Mail Extensions

3.2.31 *SMTP*—Simple Mail Transfer Protocol

3.2.32 *SSL*—Secure Socket Layer

3.2.33 *TCP*—Transmission Control Protocol

3.2.34 *TLSP*—Transport Layer Security Protocol

3.2.35 *UDP*—User Datagram Protocol

3.2.36 *VPN*—Virtual Private Network

3.2.37 *WAN*—Wide Area Network

3.2.38 *WWW*—World Wide Web

4. Significance and Use

4.1 This guide recommends security mechanisms for protection of healthcare information transmitted using the IPS. The IPS consists of multiple protocol layers.

4.2 The lowest layer which can provide end–to–end security is the Internet Protocol (IP). IP may run over a variety of subnetwork technologies, such as Ethernet, X.25, ATM, and even asynchronous dial–up lines. While it is possible to provide security services directly over those technologies, such approaches only protect a single subnetwork and are not discussed further.

4.3 A variety of protocols may be run on top of IP. These include the Transmission Control Protocol (TCP), which provides reliable, sequenced data delivery (sessions), and the User Datagram Protocol (UDP), which provides unsequenced data delivery (datagrams). Other protocols at this layer include various routing and configuration protocols used by the network itself.

4.4 Application protocols typically make use of either TCP or UDP. A variety of standard application protocols have been defined for such applications as file transfer (FTP), electronic mail (SMTP), and the World Wide Web (HTTP). Some applications have their own security requirements, dictated by the structure of the application or its protocols.

4.5 The remainder of this guide is organized as follows: Section 5 discusses security threats and the countermeasures which can be used to protect against these threats. Section 6 presents a brief overview of cryptography, as most network security mechanisms rely on its use. Section 7 distinguishes

between network and application security and discusses when each level of security might be useful. The remaining sections recommend specific security protocols and mechanisms for both network and application security needs.

5. Threats and Countermeasures

5.1 This section covers the principal threats to a system. In some cases, security services can prevent an attack; in other cases, they merely detect an attack.

5.1.1 *Masquerade* occurs when an entity successfully pretends to be another entity. This includes impersonation of users or system components, as well as falsely claiming origination or acknowledging receipt of a message or transaction.

5.1.2 *Modification of information* can include modification of message or data content, as well as destruction of messages, data, or management information. This includes message sequencing threats, which occur when the order of messages is altered.

5.1.3 *Unauthorized disclosure* threats include revealing message contents or other data, as well as information derived from observing traffic flow, as well as revealing information held in storage on an open system.

5.1.4 *Repudiation* occurs when a user or the system denies having performed some action, such as origination or reception of a message.

5.1.5 *Denial of service* threats prevent the system from performing its functions. This may be accomplished by attacks on the underlying communications infrastructure, attacks on the underlying applications, or by flooding the system with extra traffic.

5.2 The following services protect against the threats described in 5.1.1-5.1.5.

5.2.1 *Peer entity authentication* provides proof of the identity of communicating parties. Various types of authentication exchanges have been discussed in the literature; most are based on digital signatures or other cryptographic mechanisms.

5.2.2 *Data origin authentication* counters the threat of masquerade and is provided using digital signatures or other cryptographic integrity mechanisms.

5.2.3 *Access control* counters the threat of unauthorized disclosure or modification of data. This is particularly appropriate on an end system. A variety of access control strategies can be found in the standards, including access control lists and security labels. Since access control is typically provided on an end system, it is not discussed further in this guide.

5.2.4 *Confidentiality* counters the threat of unauthorized disclosure, particularly during the transfer of information. Confidentiality can be applied to entire messages or other data units or to selected fields. Encryption is used to provide this service.

5.2.5 *Integrity* counters the threat of unauthorized modification of data. This can be provided with various types of integrity check values. To protect against deliberate modification, a cryptographic check value or digital signature should be used. This also provides the service of data origin authentication. As with confidentiality, this service may be applied to entire messages or selected fields. One particularly useful application of selective field integrity is message sequence integrity, in which the integrity service is applied to a sequence number or other sequencing information.

5.2.6 *Non–repudiation* of origin and delivery protect against an originator or recipient falsely denying originating or receiving a message. This service provides proof (to a third party) of origin or receipt, and is provided using digital signatures.

6. Cryptography Overview

6.1 Cryptography is the art or science of keeping data secure from disclosure, modification, and forgery. It is particularly appropriate in today's computing environment, given the increasing use of networks to connect systems (implying more, possibly unknown users may access data), the increasing amount of sensitive data being conveyed on these networks, legal requirements for protection of data, and the ease and low cost of network attack.

6.2 *Encryption* can be used to provide confidentiality and integrity services. Following are two types of encryption systems:

6.2.1 In *symmetric* (conventional) cryptography, the sender and recipient share a secret key. This key is used by the originator to encrypt a message and by the recipient to decrypt a message. The Data Encryption Standard (DES) is an example of a symmetric cryptosystem. Confidentiality is provided by encrypting the message under a shared key. Integrity and authentication are supported by computing a cryptographic checkvalue, or *authenticator*, over the message, using a key shared by the originator and recipient.

6.2.2 In *asymmetric* (public key) cryptography, different keys are used to encrypt and decrypt a message. Each user is associated with a pair of keys. One key (the *public key*) is publicly known and is used to encrypt messages destined for that user. The *private key* is known only to the user and is used to decrypt incoming messages. RSA (named after the inventors' initials) is the most well-known asymmetric algorithm.

6.3 Some asymmetric algorithms, such as RSA, can also provide authentication, integrity, and non-repudiation when used as follows:

6.3.1 To *sign* a data unit, the user encrypts it under his private key.

6.3.2 To *verify* the data unit, the recipient decrypts it with the originator's public key.

6.3.3 If the message is successfully decrypted, it must have been encrypted by the originator, who is the only entity that knows the corresponding private key.

6.3.4 A *digital signature* is, then, a piece of data appended to a message, generated from the message and the signer's private key, which allows the recipient to prove the origin of the message and to protect against modification and forgery.

6.4 Note the digital signature can be used to provide non–repudiation services. Unlike the authenticator discussed in 6.2, the private key used to sign a message is known only by the signer. This prevents the signer from claiming that another party (for example, the recipient) generated a given digital signature.

7. Network and Application Security

7.1 *Network Security*: