The Importance of Security Standards

Presented by Douglas Kozlay

Principal Engineer, Information Resource Engineering, Inc.

Member: ANSI X9F

INFORMATION RESOURCE ENGINEERING, INC.

The Importance of Security Standards

Presented by Douglas Kozlay
Principal Engineer, IRE
Member: ANSI X9F

In evaluating the many options for network security solutions, it is essential to understand and consider the role of security standards. The growth in distributed computing and the ensuing increase in computer crime has led to legislation and regulations that establish legal requirements for network and data security. The various ANSI, FIPS and ISO network security standards have undergone extensive peer review and represent the strongest security design thinking available in the commercial marketplace. Use of standards-compliant network security provides the best assurance of high quality, strong security for your network, conforming to legal requirements and standards of "due care." This white paper summarizes legal considerations and security standards, security services and standards, and considerations in the selection of standards.

Legal Considerations

There are now laws governing security of information in banking, corporate and government applications. The use of standards-based security is an important consideration in meeting legal requirements.

In banking, there is very specific law requiring use of standards-compliant security. For example, use of standards-based systems protects banks against liability for electronic financial losses. The Uniform Commercial Code (UCC) provides legal standards for most types of financial transactions. Under UCC Section 4A-202: "...a payment order is effective as the order of the customer, whether or not authorized, if the security procedure is a commercially reasonable method of providing security against unauthorized payment orders."

The liability for wire transfer losses is assigned by UCC4A as follows:

- If the bank follows a commercially reasonable security procedure as agreed to with its customers, the bank is not liable in the event of a loss during a fund transfer.

- If the bank accepts an unauthorized funds transfer without verifying it is in compliance with a security procedure, the loss falls on the bank.

Commercially reasonable security standards have been defined by the international banking community through adoption of ANSI and ISO standards. These standards provide methods of data encryption, message authentication and user identification to protect against the risks encountered during electronic funds transfers. Use of the ANSI X9 standards, developed under the auspices of the American Banking Association, is the best way to assure "commercial reasonableness," the best protection against legal liability, and the best protection for data that is transmitted during funds transfers.

In the corporate world, organizations and employees are required to meet their fiduciary responsibility by protecting assets, including information assets. Again, the use of standards-based security provides excellent evidence that "due care" has been exercised by employing methods endorsed by national, government and international standards bodies and in use by "similarly situated" corporations.

In the Federal Government environment, compliance with FIPS (Federal Information Processing Standards) standards is a procurement requirement. FIPS are adopted and promulgated by the National Institute of Standards and Technology (NIST).

Security Standards Organization

The following organizations set security standards for national and international network applications.

- ANSI - American National Standards Institute sets standards for the banking industry.
- FIPS - Federal Information Processing Standards. This organization sets standards for U.S. Government use.
- ISO/IEC - International Standards Organization and the International Electrotechnical Commission set international standards.
- IETF - Internet Engineering Task Force. This organization is responsible for setting standards for Internet users.

Security Services

Security services are used to achieve a desired business outcome. Business goals for network applications and the corresponding security services are:

Business Goal	Security Service
• Keep communications private	• Data Encryption
• Information that is received is exactly what was sent	• Authentication
• You are who you claim to be	• User Authentication
• Legally binding electronic transactions	• Digital Signatures

The table below identifies the various areas of security standardization. It also illustrates the standards that are in common across the different standards bodies:

	Standards			
Security Service	**ANSI**	**FIPS**	**ISO/IEC**	**IETF**
Data Encryption Standard	X3.92, X3.106	FIPS 46, 74, 81	8372, 10116	1829
User Authentication	X9.26	FIPS JJJ (draft)	9798, 11131	1334
Message Authentication	X9.9, X9.19	FIPS 113, 180-1	9797, 8731	1826, 1827, 1828, 1852
Key Management - Secret	X9.17, X9.24	FIPS 171	8732, 11568	—
Key Management - Public	X9.42 (draft)	—	9594-8, 11770-3	Oakley+ISAKMP (IPSEC drafts)

The standard for automated key management, accepted worldwide, is ANSI X9.17/ISO DIS 8732/FIPS 171. This standard provides for secure automatic, periodic, electronic changes of encryption and authentication keys.

ANSI X9.17/ISO DIS 8732/FIPS 171 has been formally reviewed and adopted by both standards organizations and the major users of commercial encryption technology, large banks and financial institutions. ANSI X9.17 is in use for applications such as:

- Electronic Funds Transfers
- Payment Authorization
- Automated Clearinghouse Transactions
- Secure Remote Access for users such as Auditors, Law Enforcement Agencies (FBI, Secret Service), Diplomats, Sales Organizations
- Securities Trading

Public key management standards are now emerging, but have not yet been accepted. ANSI X9.42 and IETF Oakley+ISAKMP exist only in draft form and have not been approved through the peer review process. A working group of the IETF is revising the ISAKMP+Oakley draft (no RFC number is yet assigned) so that it may be proposed and formally adopted later in 1997.

Considerations in Selection of Standards

There are considerations to review when selecting among the various standards. Over the years, most encryption algorithms and protocols have proven to be weaker than their designers thought. Cryptographers, as well as hackers, work diligently to find and exploit any weaknesses. Security standards have been investigated by committees of cryptographers and potential users; therefore, these standards tend to be more resistant to attack.

Encryption Standards

Data Encryption/Confidentiality (keeping communications private) - protects data from unauthorized disclosure. Data encryption is a process in which the data is "scrambled or coded" before it passes through the network. The information is decoded at the receiving location and read "in the clear." It is based on encryption algorithms such as the Data Encryption Standard (ANSI X3.92) or the Rivest-Shamir-Adleman (RSA) or IDEA algorithm. Encryption algorithms are the series of mathematical steps that are employed to transform data into encrypted form or are used to generate a Message Authentication Code (MAC).

User Authentication - This is a process for identifying a user prior to initiating a secure session and/or randomly during the session (i.e., to make sure you are still talking to the same user). Standards in this area include ANSI X9.26 in the banking environment and Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) in the Internet community. The CHAP and PAP are protocols for authenticating a user to a central hub/site when dialing into a network, but not end-to-end or a host. ANSI X9.26 is a challenge-response protocol that carries out the exchange using DES encryption. CHAP is based on a similar process using an algorithm called MD5. PAP is a weak authentication protocol lacking encryption and passing passwords in the clear. A draft Federal Information Processing Standards (FIPS) - currently called JJJ - is being made available by NIST to use the Digital Signature Standard for user authentication (X9.30).

Message Authentication - ANSI X9.9 (based on DES) and FIPS JJJ are examples of authentication algorithms. These algorithms are a sort of cryptographic check sum - simply put, this is another way of authenticating data (not to be confused with an arithmetic checksum that is easily spoofed or impersonated).

Non-Repudiation - This service is implemented using Digital Signatures. Two standards exist in this arena: DSS, the Digital Signature Standard (ANSI X9.30); and, RSA Signatures (ISO 9796). Digital signatures bind the user with the data file, providing both proof of data integrity and the origin of data that can be verified by any third party at any time. This function is critical for audit control in an electronic commerce environment.

UCC-4A "Similarly Situated Banks" Consideration

UCC-4A also states that an important factor in determining the security methods that are "commercial reasonable method" is the security method in use by "similarly situated banks for similarly situated customers". With the rapid adoption of IRE Network Security Systems and similar systems by many banks across the U.S., a standard for commercially reasonable security is emerging. IRE products are used by 7 of the 10 largest U.S. banks and by 18 of the top 25 banks to secure EFTs.

Internet Considerations

As recently noted by security expert, Dr. Donn Parker of SRI, the standard that is emerging for network security in particular use of the Internet is the standard of "due care." That is, what approach is being used by similar organizations in similar situations for similar systems. Thus, the growing body of legislation and regulation is an indication of the dramatically increasing need to implement network security systems. Close adherence to national and international standards results in the best protection against threats to secure data communications. In addition, the use of systems that comply with these standards is the best protection against legal liability.

A Summary of IRE Experience in Financial Applications

Citibank, North America has extensive experience with IRE systems. The Bank has use IRE network security systems since 1988. The products are used in numerous applications including the bank's corporate cash management, data processing and international communications operations. The Bank has provided over 1200 encryptors to Citibank corporate clients for use in securing electronic funds transfers.

After a world-wide review of potential data security suppliers, **Bank of Montreal** selected IRE as its vendor of a data security system used to protect corporate cash management transactions in asynchronous dial networks and in an X.25 network. In 1989, the Bank was IRE's first client for System A.25 that provides encryption for host computers with X.25 interfaces.

J.P. Morgan & Company selected IRE as the Bank's provider of security for corporate cash management applications. The Bank uses IRE's data encryption, message authentication and smartcard user authentication products to secure customer EFTs in Value-Added Networks including the GEIS store-and-forward network. To date, IRE has delivered over $500,000 of products to Morgan.

Euroclear, the world's largest security clearinghouse, has begun deployment of IRE's Network Security System to over 1000 users in 35 countries. Euroclear requires the use of an IRE Remote Security Device by all users who perform funds transfers using the Euclid Cash service. IRE provides 24 hour support for this worldwide installation. Currently, approximately 800 security devices have been installed.

The **Chicago Clearing House Association** and a consortium of 13 banks use IRE products to secure its EDIBANX service. EDIBANX is the first electronic service to provide true EDI with both payments and remittance information in one transaction.

IRE products are used by a rapidly growing number of banks in electronic funds transfer applications. In addition to the financial institutions described earlier, **First Union**, **PNC Bank**, **Northern Trust**, **Mellon Bank**, **Bank of New York**, **Wachovia Bank**, **State Street Bank**, **First National Bank of Maryland**, **First Bank**, the **Bank of Butterfield** (Bermuda), **La Caixa** (Spain) and **National City Corporation** have installed IRE systems to secure corporate cash management , wire transfer, ACH and other EFT and remote access applications.

The **Federal Reserve System** has selected the IRE AX400 and SafeNet/Dial Secure Modems to protect remote access by Bank Examiners to sensitive information located on LANs at Federal Reserve sites. This permits these employees to report their audit data while working from remote sites.

The **Internal Revenue Service** selected IRE secure remote access products using advanced digital signature technology to enable remote access by agents who work from client sites, field offices and their homes. The IRE has publicly commented that they anticipate purchase of 10,000+ IRE secure modems. The IRS performed an extensive evaluation including two laboratory tests an a field trial by users of products from IRE and three other companies prior to choosing the IRE AX product family.

The **U.S. Department of the Treasury - Financial Management Service** selected IRE to provide a Message and User Authentication System for the Service's Electronic Certification System. This security system is used to protect electronic payment invoices totaling approximately $4 Billion for all U.S. Government payments made by the Treasury Department. IRE has provided a smartcard-based authentication system that the Treasury Department and individual federal agencies use to electronically certify that the Treasury should process electronic payments of behalf of each agency. To date, IRE has delivered over $2M of products to FMS.