Cryptography Standards and Infrastructures for the Twenty-First Century

The Internet is opening up new ways for consumers, industry, and governments to conduct business and to exchange information electronically. Electronic ordering and payments can be handled efficiently and conveniently over the network. Electronic mail and informational Web pages have become institutional resources. Yet the full benefits of electronic commerce and information exchanges will not be realized until users have sufficient trust and confidence in the security and privacy of their information.

The President's Commission on Critical Infrastructure Protection recently issued a report on the threats to telecommunications, energy, banking and finance, and other systems critical to the government and economy of the U.S. The Commission warned that people may not be willing to use the Internet for commerce if they do not have confidence that their communications and data are safe from unauthorized access or modification. Further, the Commission noted that secure and reliable telecommunications networks must have effective ways for authenticating information and assuring the confidentiality of information. There is no single technology or technique that will produce the needed security and reliability of networks. A range of technologies, including cryptography, improved identification and authentication technologies, and firewalls, will be required, along with trusted encryption key and security management infrastructures.

Cryptography has had, and will continue to have, an important role in protecting information both within a computer system and when information is sent over the Internet and other unprotected communications channels. Cryptography serves many functions in secure business transactions by providing ways to assure data confidentiality, data integrity, authentication of message originator, user authentication, electronic certification of data, and nonrepudiation.

This bulletin reports on the progress being made by NIST and by its government and industry partners to advance the development of electronic commerce systems in which users will have confidence. There are efforts underway to update existing standards for cryptography; to develop new and stronger forms of encryption; and to create infrastructures that will support safe electronic transactions in future networks.

Data Encryption Standard

The two basic components of cryptography are the algorithm or cryptographic methodology used, and the key. In modern systems, algorithms are complex mathematical formulae and keys are strings of bits. The Data Encryption Standard (DES), issued in 1977, provides an encryption algorithm for protecting federal unclassified information from unauthorized disclosure or undetected modification during transmission or while in storage. The standard is based on secret key cryptography. The algorithm is publicly known; the key system is symmetric with the same key used for encrypting and decrypting information, and the keys must be kept secret. The standard was initially issued for government use. It was subsequently adopted as a voluntary industry standard (American National Standard X3.92 1981/R1987) and has been widely implemented by the private sector. It is based on the work of the International Business Machines Corporation.

Under the provisions of the DES, NIST is required to conduct a review every five years to determine whether the cryptographic algorithm specified by the standard should be affirmed, revised, or withdrawn. The first review resulted in the reaffirmation of the standard in 1983; the standard was again reaffirmed in 1988 following a second review; as a result of the third review, which was completed in 1993, the DES was reaffirmed for use through 1998 as Federal Information Processing Standard (FIPS) 46-2.

Triple DES. A more secure method for using the DES algorithm in three operations, called Triple DES, has been developed by the private sector. Triple Data Encryption Algorithm mode of operations and implementation methods have been documented and specified as draft American National Standards (X9.52 and X9.65) by Accredited Standards Committee X9 for Financial Services. This committee develops cryptography and public key infrastructure standards for the banking community. Federal organizations that need security beyond that provided by the DES can use these standards.

Strength of the DES. The continued security of the DES has been questioned as the result of various attempts to break the algorithm. The security provided by DES cryptographic systems depends on the mathematical soundness of the algorithm, length of the keys, key management, mode of operation, and implementation. It is expected that people will continue to try to attack the DES, and other encryption algorithms as well. Successful attacks on the DES have been brute force attacks, which have tried all possible keys for a given encryption until the correct key is found. Motivated by a well-publicized competition in 1997, successful attackers organized teams of people and tens of thousands of computers that worked for months to break one message. In July 1998, the New York Times reported that a group of computer experts had succeeded in breaking a DES-encoded message by building a cracking machine costing $250,000. The machine, consisting of 27 boards each holding 64 chips, took 56 hours to recover a DES key and decipher an encrypted message. This most recent attack appears to demonstrate that a single determined attacker can develop an effective DES cracking machine. In some cases, the attack may not pose an immediate or significant threat. However, organizations may wish to consider making the transition to the use of Triple DES, matching the strength of the protective measures against the associated risks.

In consultation with other organizations, NIST is developing plans for its next steps concerning the DES. One option under consideration is to revise the applicability provisions of the standard to recommend that agencies use multiple DES iterations, such as Triple DES, to protect highly sensitive data and data that requires long-term protection for confidentiality.

Escrowed Encryption Standard

FIPS 185, Escrowed Encryption Standard, specifies the SKIPJACK algorithm which federal agencies can use for protecting the confidentiality of data. When originally issued, the SKIPJACK algorithm and the Key Exchange Algorithm used with SKIPJACK were classified secret. Recently, the Department of Defense announced that it had declassified both algorithms in an effort to encourage the development of reasonably priced and interoperable computer protection products for the Defense Message System and other Department of Defense applications.

Review of FIPS 140-1, Security Requirements for Cryptographic Modules

Issued in 1994, FIPS 140-1 specifies the overall requirements for the design and implementation of modules that use cryptographic algorithms and methods. The standard identifies requirements for four security levels for cryptographic modules to provide for different sensitivity levels of data from low value to high value, and for many different applications. Like the DES, this standard also calls for a review by NIST every five years.

The first planned review of FIPS 140-1 will be announced in the Federal Register later this year. Public comments will be solicited on the continued usefulness of the standard and on any requirements for revisions that may be needed to meet the challenges of technological and economic change.

NIST has established a program to validate cryptographic modules for correct implementation of cryptography standards. This effort is carried out under the auspices of the National Voluntary Laboratory Accreditation Program (NVLAP), and in cooperation with the Communications Security Establishment (CSE) of the Government of Canada. A list of validated products is maintained by NIST and is available on the Web site listed at the end of this bulletin.

Expansion of the Digital Signature Standard

Public key cryptography uses two keys: a private key and a public key. The private key cannot be derived from the public key. FIPS 186, Digital Signature Standard (DSS), specifies the Digital Signature Algorithm (DSA), that is used in conjunction with FIPS 180-1, Secure Hash Algorithm, for applications requiring the authentication of data integrity and the identity of the signer. FIPS 186 provides cryptographic techniques based on public key cryptography for generating and verifying electronic signatures, which can be used to verify the origin and contents of a message. FIPS 180-1 specifies a Secure Hash Algorithm (SHA-1) which can be used to generate a condensed representation of a message called a message digest. These techniques, that were developed for the federal government, are also implemented in commercial products and used by both the public and private sectors.

Last year, NIST proposed expanding the Digital Signature Standard to include additional signature algorithms that the federal government could endorse to authenticate electronic information and transactions and to assure high levels of integrity. Most of the federal organizations responding to our request for comments supported the addition of alternative signature algorithms. We have identified RSA and Elliptic Curve Cryptography technology as potential new algorithms for inclusion in a revised FIPS 186. Both techniques have been proposed as voluntary industry standards. Seeking to be consistent with the actions in the voluntary standards community, we are awaiting the completion of the industry standardization processes before proceeding with the revision of the FIPS to include the RSA technique and Elliptic Curve Cryptography technology. When approved by the American National Standards Institute (ANSI) as voluntary industry standards, we intend to take appropriate steps to gain approval and to advise federal agencies that they can use these standards in addition to the DSA.

Development of the Advanced Encryption Standard

Last year, we also announced that we would begin a multi-year project to develop an Advanced Encryption Standard (AES) which would provide cryptographic protection for data well into the next century. Planned as a government and industry cooperative effort, the AES project has elicited considerable public attention and involvement. More than fifty public comments were received on the minimum acceptability requirements and the criteria that were drafted to evaluate candidate algorithms for the AES. More than 75 individuals from industry and government agencies attended a workshop held in April 1997 to refine the requirements and criteria.

A call for candidate algorithms based on the jointly developed requirements and criteria was announced in the Federal Register (September 12, 1997, Volume 62, Number 177, Pages 48051-48058). By the submission deadline of June 15, 1998, we had received 21 submissions, including many from U.S. industry. Fifteen of these met NIST's submission requirements and minimum acceptability criteria. The fifteen candidate algorithms were announced at a conference held in Ventura, California, on August 20-22, 1998. We plan to work with the cryptographic research community in evaluating the candidate proposals. After reviews and tests of implementations for efficiency, we will narrow the candidate proposals to approximately five, and invite further review and analysis. The AES is planned to be an unclassified, publicly disclosed symmetric key encryption algorithm that will be available royalty-free worldwide.

Key Agreement or Exchange

Cryptographic services depend on the secure generation and distribution of keys (public and private). Key management services are needed to support authentication, integrity, and confidentiality of information. NIST has solicited comments on technologies that could be considered for the design and implementation of federal key agreement and exchange systems for public key-based cryptography. Key exchange technologies under consideration are RSA, Elliptic Curve, and Diffie-Hellman technologies to give federal organizations broad flexibility in using cryptographic systems. We will await the completion of the voluntary standards processes before proposing a federal standard for key agreement and exchange.

Public Key Infrastructure (PKI)

Several activities are underway to support the development of a public key infrastructure which provides the means to bind the public keys used in cryptographic functions to their owners and to distribute keys in large heterogeneous networks. The use of PKI technology can help to increase confidence in electronic transactions and allow parties without prior knowledge of each other to conduct verifiable transactions.

PKI Pilots. NIST is working with the Federal PKI Steering Committee (a committee established by the Government Information Technology Services [GITS] Board) to promote the consideration and use of public key technology by federal agencies in the performance of intra-agency and interagency business and in transactions with trading partners and the public. Established under Executive Order 13011, GITS is conducting demonstration projects, pilots, and proof-of-concept projects in support of the Administration's National Partnership for Reinventing Government (formerly the National Performance Review) initiative to make government work better and cost less by reengineering through information technology. NIST also works with industry groups including the Internet Engineering Task Force PKIX Working Group and the Accredited Standards Committee X9.

Interoperability Specifications. In conjunction with ten research partners under a cooperative research and development agreement (CRADA), NIST completed a Minimum Interoperability Specification for Public Key

Infrastructure Components (MISPC). Based on analysis of implementations of PKI components provided by the CRADA participants, the specification provides a minimal set of features, transactions, and data formats for various certificate management components that make up a PKI. The MISPC can be used by industry and government organizations in acquiring PKI components and services. NIST is developing a laboratory-based reference implementation of the MISPC as a proof of concept and to enable developers of PKI systems to test their implementations. Future laboratory work will be directed toward developing a test suite to provide the means for the validation of the interoperability of PKI systems.

PKI product developers are beginning to incorporate parts of the MISPC into their products. This is the start of the development of secure, interoperable PKI implementations that will provide security services for confidentiality and digital signatures and enable secure electronic business transactions. Under a second CRADA with 16 industry partners, we are expanding the MISPC to incorporate support for confidentiality components. In addition, we are defining technical security requirements for PKI components.

Key Recovery

NIST is exploring the use of key recovery technology through a broad agency announcement for several agency pilot projects and with the help of a technical advisory committee. An announcement in the Commerce Business Daily last year solicited proposals for products and services that will demonstrate the viability of an infrastructure for key recovery.
NIST has participated in a Key Recovery Demonstration Project involving several government agencies to demonstrate techniques to recover keys used in data encryption and to identify, test, and evaluate different key recovery products and services. Planned laboratory work includes development of conformance tests and techniques for integrating key recovery components into larger functional systems.

This effort supports the Administration's policies on privacy, commerce, security, and public safety in the Global Information Infrastructure. Concerned about potential harm to law enforcement and national security from the use of unrecoverable encryption, the Administration backs the development of a key management infrastructure to protect U.S. national security, foreign policy, and law enforcement interests. A technical advisory committee to develop a FIPS for the federal key management infrastructure has been established to provide industry advice on encryption key recovery techniques for use by federal government agencies. The Committee currently includes 20 industry members. The Committee has developed a draft key recovery model and specifications for the security and functionality of key recovery components. The draft specifications are available to industry organizations that wish to develop products that meet customer requirements for key recovery. The specifications are available for review at the Web site listed at the end of this bulletin.

Export Controls on Cryptography

The Administration has announced changes to the export control rules for encryption items on the U.S. Munitions List. Except for those items specifically designed, developed, configured, adapted, or modified for military applications, control of the export of encryption items has been transferred to the Department of Commerce. One of the options allowed under the revised rules is the export and re-export of non-recoverable encryption items up to 56-bit key length DES or equivalent strength after a one-time review of the strength of the item and if the exporter makes satisfactory commitments to build and/or market recoverable encryption items, to support an international key management infrastructure. This policy applies to hardware and software and will last through December 31, 1998. Many U.S. vendors are planning key recovery products as part of the licensing provisions under the Department of Commerce's export control regulations.

The Department of Commerce continues to review the export control policies and recently announced that it had completed guidelines to allow the export of U.S.-manufactured encryption products of any bit-length when used by banks, financial institutions, and their branches around the world to secure private electronic transactions. The new guidelines will allow for the export of strong encryption products, with or without recovery features, to eligible institutions without a license, after a one-time review. Eligible institutions include banks, security firms, brokers, and credit card companies in 45 countries. The 45 eligible countries are either members of the international anti-money laundering accord, the Financial Action Task Force, or have enacted anti-money laundering laws.

Summary

As the use of information technology expands rapidly, the need for advanced cryptography and high-quality security techniques and services increases. NIST is working with government and industry organizations to make cryptography and security services available for all to use in exploiting fully the benefits of the Internet.