Glossary Terms

Access control: A cornerstone of security is the ability to determine who can access computer networks and systems. Control can be exercised through the use of access control protocols, computer applications that authenticate the user logging into a network. Access control lists (ACLs) define which users can access specific data and programs. Access codes are passwords, series of characters or numbers that enable a user to access the network

Accountability: An essential ingredient of security systems is the ability to determine who performed any given action and which actions occurred during a specific time interval. Organizations improve accountability by using the latest software applications, including intrusion detection and network auditing tools, to trace violations or attempted violations of computer security to individuals who then can be held responsible.

Administration: Personnel responsible for administering computer security define security parameters, maintain and monitor security systems, and modify policy information.

AES (Advanced Encryption Standard): In 1997, the National Institute of Standards and Technology (NIST) announced its intention to develop a Federal Information Processing Standard (FIPS) for a standard encryption method. Fifteen companies were invited to create and present alternatives to the 20-year-old Data Encryption Standard (DES). The new AES, a strong, 256-bit encryption able to protect sensitive government data, must be an unclassified, publicly disclosed algorithm available royalty-free worldwide. In 1998, the candidates presented their bids at a conference; open debate on the merits of each candidate's entry continues today. As of August 1999, NIST announced five finalists, which include IBM, RSA, Counterpane Systems, the University of Cambridge, and -- jointly -- Banksys/PWI and the Catholic University of Leuven, who will undergo further analysis and testing until the "winner" is announced by fall of 2000.

API (Application Programming Interface): Software applications, such as spreadsheets or word processing, use a special language and message format -- the API -- to communicate with the computer operating system, database management system or other system programs. Software system vendors provide APIs so that their customers can use various applications directly from their desktops. Development and use of standard APIs safeguards business-critical data.

Assurance: Security-conscious organizations provide assurance to users, partners and customers by demonstrating and periodically validating that the claimed level of security protection is being enforced. Virus protection, services and consulting support, and policy management are all assurance techniques.

Availability: To be secure, computer resources must be ready for use by authorized users when they need them. Availability covers systems, data, networks and applications.

Authentication: Authentication denotes a security procedure where an individual is identified. The process ensures that the individual is whom he or she claims to be, but does not affect the individual's access rights. User names, passwords and biometric scanning are all authentication techniques.

Authorization: This phase of security admits only legitimate user access to systems, data, applications or networks. After the user is authenticated, he or she is authorized, that is, granted access to a network resource. An identification number or password that is used to gain access to a local or remote computer system.

Biometrics: Biometrics is the study of measurable biological characteristics, used in computer security applications as an authentication technique. Most commonly, biometrics used in computer security systems entails computer analysis of fingerprints or speech. Biometrics is expected to become increasingly important in e-business transactions, as an effective way to detect fraudulent users.

CDSA (common data security architecture): CDSA denotes the overall security infrastructure for all components of the computer system or network, employing many security applications. A CDSA is based on cryptology and digital certificate management, and can support a variety of programming environments. Typically, a CDSA is made up of four layers, ranging from the bottom layer of the service provider modules' basic security programs, to the top layer, which includes secure digital certificate-based transactions.

Certificate: the most common kind of ***credential*** in the network computing environment. Certificates include standard information such as the owner's ***public key***, globally-accessible name, and expiration dates; certificates may also contain some application-unique data such as title, degree(s) earned, and professional licenses. Certificates are also called digital certificates.

Certificate authority: In the pre-Internet world, every secure transaction involved a trusted third party -- such as a notary, attorney or broker -- who could guarantee that both parties were who they purported to be. A Certificate Authority (CA) fills that same role in the digital world. A CA vendor, such as VeriSign or Entrust, issues certificates that contain the identities and affiliations of individuals, along with their public keys. These certificates are bound together with the digital signature and stored in a special directory. The sender's browser looks up the recipient's certificate in the directory, and the message can be encrypted using the key embedded in the certificate. The sender can then sign the message using his own private key, and the recipient can verify the signature by using the sender's public key that is vouched for by the CA.

Confidentiality: keeping information protected from unauthorized disclosure or viewing.

Content filtering: A content-filtering application accepts or rejects data by relying on a pattern through which data is blocked or allowed to pass through the filter. It is mainly used on the Internet to prevent access to certain sites, for example by parents who do not want their children to visit adult sites. There are two main content filtering methods -- URL list filtering and word-matching filtering. URL list filtering depends on the use of an allowed site and blocked site list. Word-matching filtering relies on finding and blocking inappropriate words and phrases.

Credentials: data associated with a user or resource that indicates identity and authority level. Credentials need to be issued by a trustworthy authority, as that authority is vouching for the identity and authorization level. A passport is a credential; it represents the bearer's identity and rights and is issued by a formally-recognized government agency. In network computing environments, the most common type of credential is a ***certificate*** that has been created and "signed" by a trusted ***certificate authority***.

Cryptography: Cryptography is the process of converting data into a secret code for transmission over a public network. The original text is converted into coded text, or cipher text, by an encryption algorithm.

Cryptography, known as the science for keeping data secure, provides the ability to store information or to communicate between parties in such a way that prevents other non-involved parties from understanding the stored information or accessing and understanding the communication. The encryption process takes understandable text and transforms it into an unintelligible piece of data (called ciphertext); the decryption process restores the understandable text from the unintelligible data. Both involve a mathematical formula or algorithm and a secret sequence of data called a ***key***. Cryptographic services provide ***confidentiality*** (keeping data secret), ***integrity*** (preventing data from being modified), ***authentication*** (proving the identity of a resource or a user), and ***non-repudiation*** (providing proof that a message or transaction was sent and/or received).

There are two types of cryptography:

- In shared/secret key (symmetric) cryptography there is only one key that is a shared secret between the two communicating parties. The same key is used for encryption and decryption.

- In public key (asymmetric) cryptography different keys are used for encryption and decryption. A party has two keys --a public key and a private key. The two keys are mathematically related, but it is virtually impossible to derive the private key from the public key. A message that is encrypted with someone's public key (obtained from some public directory) can only be decrypted with the associated private key. Alternately, the private key can be used to "sign" a document; the public key can be used as verification of the source of the document.

DCE (Distributed Computing Environment): DCE is an industry-standard software technology for setting up and managing computing and data exchange, primarily for large networks made up of different-sized servers in a number of locations. Users can access applications and data, and programmers can write code, without needing to know where data and applications are located. DCE also provides security services, including access-control listing, authentication and verification.

DES (Data Encryption Standard): DES is a popular technique for symmetric key encryption, a method whereby the sender and receiver of a message share a single common key that is used to encrypt and decrypt the message. DES was developed in 1975 and adopted by the American National Standards Institute (ANSI), an organization that creates standards for the computer industry, in 1981. Developers of competing techniques argue that DES, based on 56-bit computer architecture, is too weak to be a global standard. These rivals have hosted "challenge" events in which software developers and hackers are invited – sometimes successfully – to crack DES within a specified time period.

Denial of service: A denial of service occurs when a system can no longer respond to normal requests. This usually happens when a network is flooded with so many requests that it cannot keep traffic moving at a regular pace.

Digital certificate: Digital certificates allow a user to send an encrypted message. A digital certificate is an attachment to an electronic message that verifies the user is who they claim to be, and is used to ensure secure e-business transactions. The Certificate Authority (CA), which issues a user's digital certificate, makes known the user's public key, which another user employs to decode the digital certificate attached to a message. This process also verifies that the certificate was issued by the CA and allows users to obtain identification information of the certificate-holding sender. The recipient of the message can then send an encrypted reply.

Digital signature: Used for electronic commerce security and similar to a digital certificate, a digital signature is a code attached to an electronic message to verify the sender's identity. A digital signature is a computed version of the text that is encrypted and sent with the message. The recipient then decrypts the signature and recomputes the digest from the received text. Matching digests prove the authenticity of the message and the sender. To be effective, digital signatures must be impervious to forging.

Directory: A directory service is the "yellow pages" of computer network resources, stored on a server and often containing security-related data, such as phone numbers, electronic mail addresses, public keys, computer names and addresses. The data is presented hierarchically, much like a family tree, with one section providing key information about the files beneath it. To access a file, a user may need to produce the names of all the directories above it by specifying a path. To read information from or write information into a directory, the user must use operating system commands.

Directory Services: provide means of locating resources and users in a network or networks. They are analogous to telephone directories -- even though you look up a resource or user name, you still need to know something about its location to narrow the search. A directory can also include the public key of the user or resource in addition to location and other information.

Encryption: Encryption is the translation of data into a secret code, and is used to maintain the security of Internet transmissions and system data. Users must have access to special passwords called keys to encrypt the message and then to decrypt it -- turn it back into plain text. Encryption may be symmetric, where the same key is used to encrypt and decrypt, or asymmetric, where a private key and a public key are both needed to communicate. In asymmetric encryption, private and public keys are made to serve opposite functions: If the private key is used to encrypt the message, the public key is used to decrypt, and vice versa. In addition to DES, encryption standards include RSA's RCA, or the more internationally popular IDEA algorithm. The most commonly used type of encryption, the short form of SRA keys, consists of 512 bits. Longer keys, such as 1,024-bit, are used to protect sensitive military, banking and other data.

Evaluated Systems: refers to operating systems, networks or databases that, either separately or together have been evaluated against a security standard defined by the US Department of Defense in a book called the Orange Book, technically known as the Trusted Computer Systems Evaluation Criteria (TCSEC). The TCSEC defines a hierarchy of various levels of security functionality and assurance criteria. Progression up the hierarchy involves the addition of security functionality and more stringent assurance criteria to enable users to place progressively more trust in the higher rated systems. The complementary effort in Europe is called the ITSEC -- Information Technology Security Evaluation Criteria.

Firewall: A firewall is a hardware/software systems that manages the flow of information between the Internet and an organization's private network. Firewalls can prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets, and can block some virus attacks – as long as those viruses are coming from the Internet. A firewall also may be used to separate two or more parts of a local network to control data exchange between departments. Components of firewalls include filters or screens, each of which controls transmission of certain classes of traffic. Firewalls provide the first line of defense for protecting private information, but comprehensive security systems combine firewalls with encryption and other complementary services, such as content filtering, intrusion detection, etc.

Hack/Crack: To hack means to write one's own solution to a computer problem because no pre-written program or function exists to solve the problem. Programmers who are "hacking away" are starting from scratch and writing a new language or program to achieve the programming goal. However, "hacker" is often used to describe an unauthorized person who modifies a program by changing its code to corrupt or steal data. In self-defense, the hacking community has adopted the term "cracker" for someone whose sole aim is to break into secure systems. The simplest form of hacking -- extremely slow but ultimately effective -- is brute-forcing, in which the computer is programmed simply to try all possibilities until the correct solution is reached. Hackers and crackers looking for quick results use algorithms or other logical shortcuts. Following security measures, like data encryption, help prevent crackers from entering a system.

Integrate: To integrate generally means to merge two or more computer components into a single system. Any software product that is coined "integrated" means the product performs more than one type of task and offers seamless operation. IDE, and integrated development environment, refers to pieces of hardware that are connected to a larger network component.

Integrity: preventing data from being modified or tampered with.

Intrusion detection: Intrusion detection systems (IDS) monitor network system files and logins to locate intruders who attempt to break into or misuse a computer system. The two main types of intrusion detection systems are anomaly detection and misuse detection. Anomaly detectors catch behavior that deviates from normal system use. Misuse detectors look for behavior that matches a known attack scenario.

IKE (Internet Key Exchange): Internet Key Exchange is a security measure which employs two keys, a private key, and an exchange key that is used to encrypt private keys. Exchange of private keys is done over the Internet, where e-mail is used to deliver private passwords to users. The key exchange system allows a person to send keys to groups of people simultaneously, where the public/private system requires that each key is encrypted separately for each key recipient.

IPSec (Internet Protocol Pecurity): IPSec (Internet Protocol Security) comprises the set of protocols that ensure secure exchange of packets at the IP layer, where packets of information are exchanged according to the packet's header, or address. IPSec is developed and maintained by the Internet Engineering Task Force (IETF), the organization that upholds standards of information exchange on the Internet. IPSec employs public key encryption, where the sender and receivers share a key, a process made possible by a protocol called Internet Security Association and Key Management Protocol. This allows the receiver to obtain a public key and authenticate the sender using digital certificates.

Java Security: Specific security protocols are launched to protect programs using Java, a computer programming language mostly used for the World Wide Web. Java programs, which can be downloaded from a Web server and run on Java-compatible browsers, are run in a small, constrained area called a Sandbox. The Sandbox contains a security system that checks and verifies all codes coming into it. Java Security employs data encryption, where keys are needed to encrypt and read data.

Key: A key is a password needed to encrypt and decrypt data. Encryption keys may be private or public. A private key is one to which only the user has access, while a public key may be published or distributed on request. .

Key Escrow: the storing of a key (or parts of a key) with a trusted party or trusted parties in case of loss or destruction of the key.

Key Management: functions used for the care and feeding of keys, such as key expiration, ***key recovery, key escrow***, and so on.

Key Recovery: a process used to recover encrypted information that does not involve the storing of the key or any part of the key with a third party. Sometimes, important data needs to be recovered without normal access. The encryption key may have been lost accidentally, or an organization may need to audit its resources, or the data may be needed by law enforcement and other outside authorities. Key-recovery systems, like those proposed by National Institute for Standards and Technology (NIST), rely on close cooperation between certification authorities and user communities that share a public-key infrastructure (PKI). These groups would need to share components of encryption keys that are stored at separate locations.

Many organizations find key recovery a preferable process to ***key escrow***. The US government recently relaxed controls on the export of strong encryption based upon the development of key recovery technology by the computer industry.

LDAP (Lightweight Directory Access Protocol): LDAP is a set of protocols used for accessing information directories. It is a less comprehensive version of the standards within the X.500, another standard definition of global directories. LDAP also supports Transmission Control Protocol/ Internet Protocol (TCP/IP), the set of protocols necessary to connect hosts to the Internet. Although not yet widely used, LDAP has the potential to allow almost any application to run on any computer platform and obtain directory information, eventually leading the way to a global white pages.

Message Digest: A message digest is a fixed-size representation of a message, created by a keyless transformation function called a hash. A hash may condense a one-megabyte message into a 128- or 160-bit digest. To send a signed message, the message originator's computer generates a digest for the message, computes a digital signature as a function of the digest and the originator's private key, and transmits both message and signature. The recipient generates a digest for the received message, then uses the digest, the originator's public key, and the received signature to verify the originator's identity. Provided the original hash function is secure, signing a message digest provides the same security services as signing the message itself.

Mobile code: Mobile code carries the ability to download some programming languages, such as Java, from a source like the Internet and load them onto almost any type of computing environment. However, there is a security concern. Because of their transferable, flexible nature, mobile codes have the potential to transmit viruses and other applications that can destroy a system.

Non-repudiation: Non-repudiation occurs when a document or participant in an activity is valid. In digital cryptography, this applies to a person who uses a private key to protect access. This guarantees that any messages signed using that person's digital signature could only have come from them. In e-commerce, when the key-holder uses a digital signature in a financial transaction, it guarantees that the person making the transaction is who they claim to be.

Policy: A policy is a rule or regulation within an organization pertaining to computing and management of information, which contributes to the overall security of the organization's files. A good security system starts with a well-structured security policy. Many breaches occur when companies fail to recognize this. In a survey in 1998 of 1,600 information professionals by PricewaterhouseCoopers LLP, 73% reported security breaches during the past year, but fewer than 1 in 5 had a comprehensive security policy.

Privacy: Trust is at the heart of every satisfying e-business relationship, and trust depends on privacy for the secure and mutual exchange of value. Computer security measures protect privacy to the extent that they control who does and does not have the right and authorization to know and access certain data. Computer security measures, such as encryption, help ensure privacy of information on networks. Private-sector assistance programs, such as the Better Business Bureau Online, TRUSTe and the Online Privacy Alliance, provide a seal of approval that tells users that a given Web site maintains a privacy policy. Some vendors, including IBM, will only advertise on Web sites that post privacy policies.

Public Key: in asymmetric cryptography, the key that is made available for others to use to encrypt information. The owner of the associated private key is the only person that can decrypt the information.

Public Key Infrastructure (PKI): PKI is a system for verifying the authenticity of each party involved in an Internet transaction, protecting against fraud or sabotage, and for non-repudiation purposes so that consumers and retailers may protect themselves against denial of transactions. Trusted third-party organizations called certificate authorities issue digital certificates --attachments to electronic messages -- that specify key components of the user's identity. During an Internet transaction signed, encrypted messages from one party to another are automatically routed to the certificate authority, where the certificates are verified before the transaction can proceed. PKI can be embedded in software applications, or offered as a service or a product. E-business leaders agree that PKIs are critical for transaction security and integrity, and the software industry is moving to adopt open standards for their use. Simplifying the directory systems that contain PKI data remains a challenge.

Reference implementation: Standards-based software code that was successfully executed and now is used as a reference point for new implementation of an encryption or other standard.

Risk management: Risk management refers to the set of activities that provide security by identifying threats and safeguarding against attacks on a computer system. Risk management programs usually center around three fundamental elements: safeguard selection, certification and accreditation, and contingency planning. Safeguard selection refers to the election of cost-effective security tools that an organization judges to be the best way to mitigate system threats. Certification is the technical verification that the system safeguards are adequate and function properly, while is the official authorization of operation and suspension of security activities. Contingency planning ensures a continued processing capability for critical systems in the event of a network shutdown.

SET (Secure Electronic Transaction)™: SET is a recent standard that enables secure credit card transactions on the Internet, and is a key component of the security of e-commerce. SET employs digital signatures to enable merchants to verify the identity of buyers. It also protects buyers by enabling their credit card number to be transferred directly to the credit card issuer for verification and billing without revealing the number to the merchant.

SSO (Single Sign-On): In a single sign-on program, users only need one password to access multiple programs in the same network. To initially log into a network program, the user provides a global identification and a password. When the user requests access to additional systems, the sign-on system retrieves the user's password to sign on to the new program SSO alleviates user frustrations with keeping or remembering multiple passwords to their computing resources. Companies may call upon SSO technologies to reduce shared passwords or readily available passwords written on yellow stickies of computer monitors.

SSL (Secure Socket Layer): SSL is a protocol, first developed by Netscape, for transmitting private documents over the Internet. SSL uses a private key to encrypt data that's transferred over the SSL connection. SSL can also be used to obtain confidential user information, such as credit card numbers. Web pages that require an SSL connection start with http:. A newer security protocol, TLS (transaction layer security), is sometimes merged with SSL applications and may eventually set the standard for Internet security. TLS provides mail encryption and authentication for e-business transactions by using by using complex triple DES encryption to create a tunnel between client and host.

Smart card: A smart card is a small device the size of a credit card with built-in electronic memory of personal data, such as identification and financial information. It can store everything from digital cash, to be spent and used like a travelers check, to health records. To transfer and receive data, a smart card must be inserted into a smart card reader. Smart cards are more secure than a magnetic strip card since they can be programmed to self-destruct if the wrong password is entered too many times.

Solution: An integrated software package or integrated set of computer applications that collectively achieves a user's computing goal easily and seamlessly. For example, the owner of a small business might employ a security solution that offers interpretable anti-virus software with a firewall to secure business transactions or e-mail from business partners over the Internet. A solution is an integrated set of software programs created to work seamlessly together, where as a suite is a bundled set of complementary software programs that may not have been created to achieve a common goal.

Suite: Refers to a group of applications that might appear in one software package and work to achieve similar goals. For example, an office might select a software program that is touted as a suite of office programs, and hence contains a number of office-related applications contributing to the overall ease of office transactions. A suite is a bundled set of complementary software programs that may not have been created to achieve a common goal, while a solution is an integrated set of software programs created to work seamlessly together.

Tool box: A tool box implies a group of different applications that provide similar services. For example, a security tool box contains different security-related programs, which a user might employ as needed.

Transaction A transaction is an activity or request, usually pertaining to business, such as orders and purchases. Transaction processing systems respond to user requests and then complete a transaction, for example an automatic teller machine responding to a customer. New transactions update master files that are stored in the computer.

Trusted Third Party: a mechanism in which a trusted party creates a key and then keeps a copy of it in case of loss or destruction of the key, or legitimate request from law enforcement.

Vault: A vault is a remote location, separate from the user's computer, where user data are stored. The process of data vaulting sends data off site, where it can be protected from hardware failures, theft and other threats. To secure vaulted data, vaulting security software can compress and encrypt the data before it leaves the user's computer. The data is then stored in the vault by number.

Virus: A virus is a program or piece of code loaded into your computer against your wishes or without your knowledge. It can use up all system memory, wipe out data, and bring systems to a halt. Viruses can also transmit across networks and bypass some security systems. Hackers frequently infiltrate computer systems with Trojan-horse viruses -- programs with apparent useful functions, such as file-copying, but also with hidden functions that launch destructive processes in the target system. A recent, widespread virus washroom, which paralyzed computer systems worldwide by masquerading as e-mail. Computer users can buy applications -- anti-virus software -- that protect their computers by searching the hard disk and removing any viruses they find.

Virtual Private Network (VPN): A VPN is a networking architecture that uses public communications lines to connect remote and mobile users via the Internet. These users then can employ the public connection to transfer data back to the company's system. VPNs are being used increasingly by companies of all sizes as a way to network over long distances for a fraction of the cost of establishing private networks. VPN security today relies heavily on IKE (Internet Key Exchange) and IPSec (Internet Protocol Security).

Privacy | Legal | Contact |