

Smart Card & Security Basics

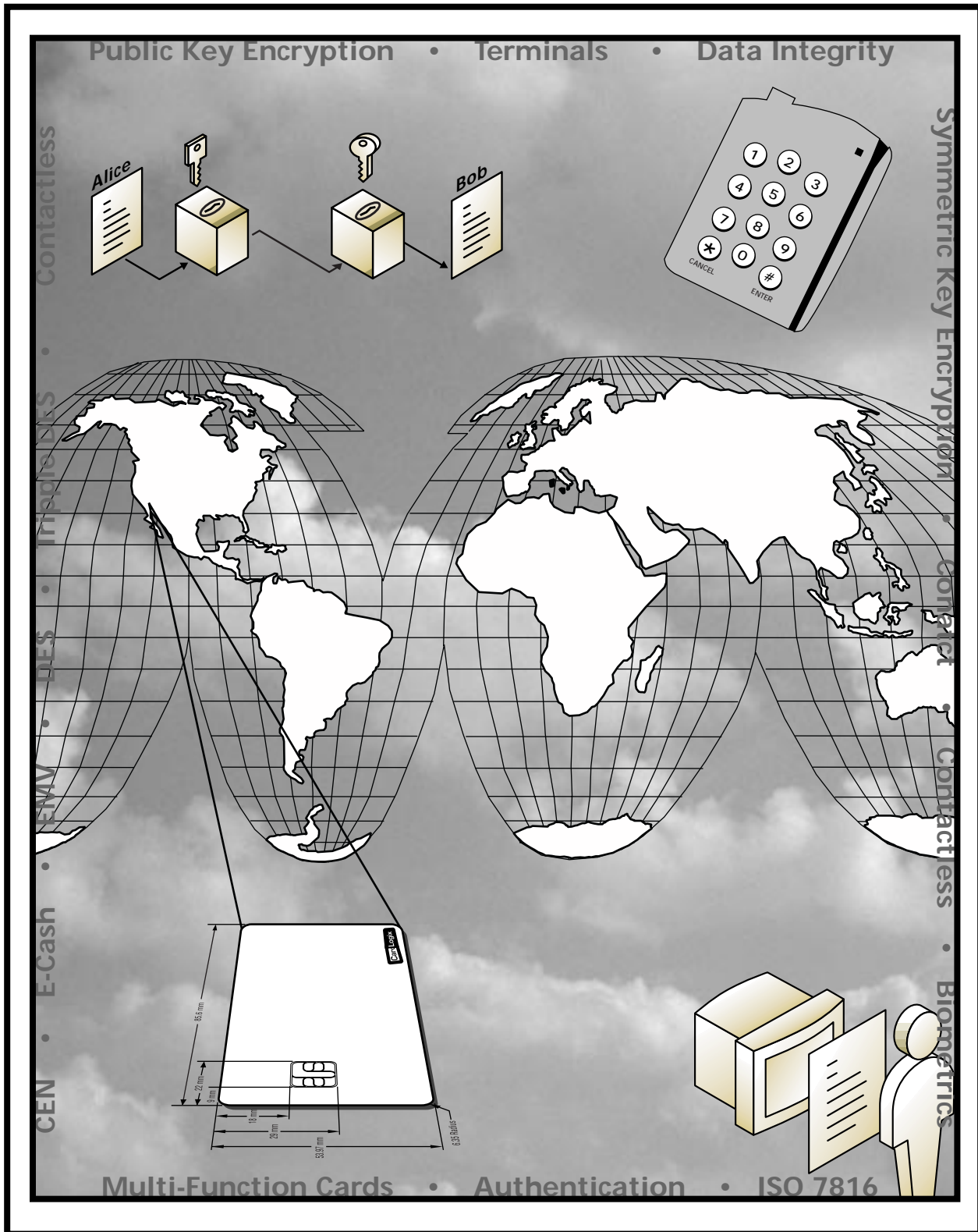


Table of Contents

| | |
|--|-----------|
| Introduction | 4 |
| Applications | 4 |
| Why Smart Cards | 5 |
| Loyalty and Stored Value | 5 |
| Securing Information and Physical Assets | 5 |
| E-Commerce | 5 |
| Personal Finance | 6 |
| Health Care | 6 |
| Telecommuting And Corporate Network Security | 6 |
| Campus Badging and Access | 6 |
| Types of Chip Cards | 7 |
| Straight Memory Cards | 7 |
| Protected / Segmented Memory Cards | 7 |
| Stored Value Memory Cards | 7 |
| CPU/MPU Microprocessor Multifunction Cards | 7 |
| Reader and Terminal Basics | 8 |
| Standards | 8 |
| System Planning & Deployment | 9 |
| Basic Set-Up | 9 |
| Security | 10 |
| Value Applications | 10 |
| General | 10 |
| Deployment | 11 |
| Security Basics | 11 |
| What Is Security? | 11 |
| What Is Information Security? | 12 |
| The Mechanisms Of Data Security | 12 |
| The Elements of Data Security | 12 |
| Data Integrity | 13 |

| | |
|------------------------------------|----|
| Authentication | 13 |
| Non-Repudiation | 13 |
| Authorization and Delegation | 13 |
| Auditing and Logging | 14 |
| Management | 14 |
| Confidentiality/Cryptography | 14 |

Smart Cards For Data Security 15

| | |
|--|----|
| Host-Based System Security | 16 |
| Card-Based System Security | 16 |
| Threats To Cards and Data Security | 16 |
| Threats To Cards and Data Security (cont.) | 18 |
| Security Architectures | 18 |

Conclusion 21

Glossary 20

Introduction

A smart card is a type of plastic card embedded with a computer chip that stores and transacts data between users. This data is associated with either value or information or both and is stored and processed within the card's chip, either a memory or microprocessor. The card data is transacted via a reader that is part of a computing system. Smart card-enhanced systems are in use today in several key applications, including healthcare, banking, entertainment and transportation. To various degrees, all applications can benefit from the added features and security that smart cards provide. According to Dataquest, the worldwide smart card market will grow to 4.7 Billion units and \$6.8 Billion by 2002.

Applications

First introduced in Europe over a decade ago, smart cards debuted as a stored value tool for pay phones to reduce theft. As smart cards and other chip-based cards advanced, people found new ways to use them, including charge cards for debit purchases and for record keeping in place of paper.

In the U.S., consumers have been using smart cards for everything from visiting libraries to buying groceries to attending movies, firmly integrating them into our everyday lives. Several states have smart card programs in progress for government applications ranging from the Department of Motor Vehicles to Electronic Benefit Transfer (EBT). Many industries have implemented the power of smart cards into their products such as the new GSM digital cellular phones to TV-satellite decoders.

Why Smart Cards

Smart cards greatly improve the convenience and security of any transaction. They provide tamper-proof storage of user and account identity. Smart cards also provide vital components of system security for the exchange of data throughout virtually any type of network. They protect against a full range of security threats, from careless storage of user passwords to sophisticated system hacks. Multifunction cards can also serve as network system access and store value and other data. People worldwide are now using smart cards for a wide variety of daily tasks, these include:

Loyalty and Stored Value

A primary use of smart cards is stored value, particularly loyalty programs that track and incentivize repeat customers. Stored value is more convenient and safer than cash. For issuers, float is realized on unspent balances and residuals on balances that are never used.

For multi-chain retailers that administer loyalty programs across many different businesses and Point of sale systems, smart cards can centrally locate and track all data. The applications are numerous, from parking and laundry to gaming, as well as all retail and entertainment uses.

Securing Information and Physical Assets

In addition to information security, smart cards achieve greater physical security of services and equipment, because the card restricts access to all but the authorized user(s). E-mail and PCs are being locked-down with smart cards. Information and entertainment is being delivered via to the home or PC. Home delivery of service is encrypted and decrypted per subscriber access. Digital video broadcasts accept smart cards as electronic keys for protection. Smart cards can also act as keys to machine settings for sensitive laboratory equipment and dispensers for drugs, tools, library cards, health club equipment etc.

E-Commerce

Smart cards make it easy for consumers to securely store information and cash for purchasing. The advantages they offer consumers are:

The card can carry personal account, credit and buying preference information that can be accessed with a mouse click instead of filling out forms.

Cards can manage and control expenditures with automatic limits and reporting.

Internet loyalty programs can be deployed across multiple vendors with disparate POS systems and the card acts as a secure central depository for points or rewards.

"Micro Payments" - paying nominal costs without transaction fees associated with credit cards or for amounts too small for cash ,like reprint charges.

Personal Finance

As banks compete in newly opened markets such as investment brokerages, they are securing transactions via smart cards at an increased rate.

This will improve customer service. Customers can use secure smart cards for fast, 24-hour electronic funds transfers over the Internet.

Reduced costs: transactions that normally would require a bank employee's time and paperwork can be managed electronically by the customer with a smart card.

Health Care

The explosion of digital health care data brings up new challenges to the efficiency of patient care and privacy safeguards. Smart cards solve both challenges with secure storage and distribution of everything from emergency data to benefits status.

Rapid identification of patients; improved treatment

A convenient way to carry data between systems or to sites without networked systems.

Reduction of records maintenance costs.

Telecommuting And Corporate Network Security

Business to business Intranets and Virtual Private Networks "VPNs" are enhanced by the use of smart cards. Users can be authenticated and authorized to have access to specific information based on preset privileges. Additional applications range from secure email to electronic commerce

Campus Badging and Access

Businesses and universities of all types need simple identity cards for all employees and students. Most of these people are also granted access to certain data, equipment and departments according to their status. Multifunction, microprocessor-based smart cards incorporate identity with access privileges and also store value for use in various locations, such as cafeterias and stores.

Types of Chip Cards

Smart cards are defined according to the type of chip implanted in the card and its capabilities. There is a wide range of options to choose from when designing your system.

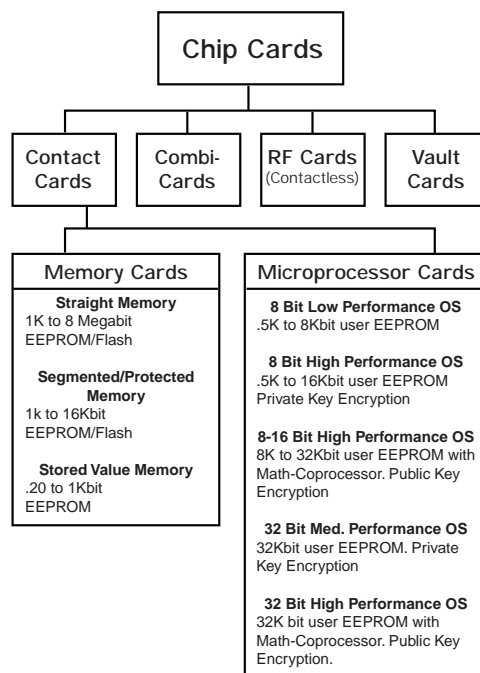
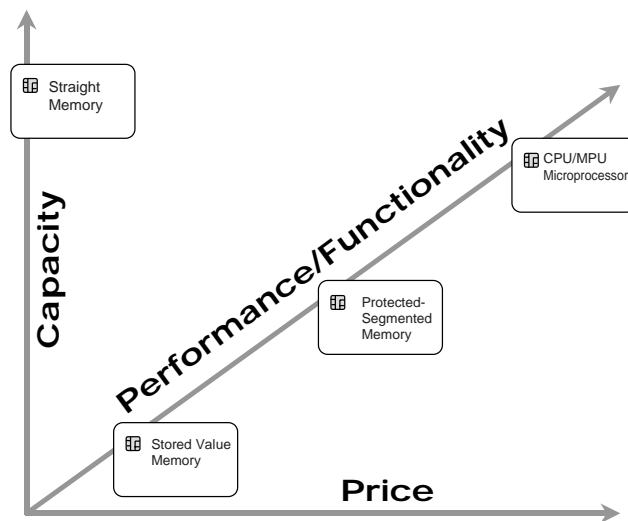


Image courtesy of CardLogix, Inc.

Increased levels of processing power, flexibility and memory add cost. Single function cards are often the most cost-effective solution. Choose the right type of smart card for your application by evaluating cost versus functionality and determine your required level of security. The following chart demonstrates the general rules of thumb.

Card Function Trade-Offs



Memory Cards

Memory cards have no processing power and cannot manage files dynamically. All memories communicate to readers through synchronous protocols. There are three primary types of memory cards:

Straight Memory Cards

These cards just store data and have no data processing capabilities. These cards are the lowest cost per bit for user memory. They should be regarded as floppy disks of varying sizes without the lock mechanism. These cards cannot identify themselves to the reader, so your host system has to know what type of card is being inserted into a reader.

Protected / Segmented Memory Cards

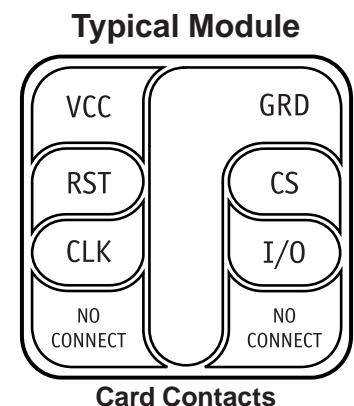
These cards have built-in logic to control the access to the memory of the card. Sometimes referred to as Intelligent Memory cards these devices can be set to write protect some or all of the memory array. Some of these cards can be configured to restrict access to both reading and writing. This is usually done through a password or system key. Segmented memory cards can be divided into logical sections for planned multi-functionality

Stored Value Memory Cards

These cards are designed for the specific purpose of storing value or tokens. The cards are either disposable or rechargeable. Most cards of this type incorporate permanent security measures at the point of manufacture. These measures can include password keys and logic that is hard-coded into the chip by the manufacturer. The memory arrays on these devices are set-up as decremeters or counters. There is little or no memory left for any other function. For simple applications such as a telephone card the chip has 60 or 12 memory cells, one for each telephone unit. A memory cell is cleared each time a telephone unit is used. Once all the memory units are used, the card becomes useless and is thrown away. This process can be reversed in the case of rechargeable cards.

CPU/MPU Microprocessor Multifunction Cards

These cards have on-card dynamic data processing capabilities. Multifunction smart cards allocate card memory into independent sections assigned to a specific function or application. Within the card is a microprocessor or microcontroller chip that manages this memory allocation and file access. This type of chip is similar to those found inside all personal computers and when implanted in a smart card, manages data in organized file structures, via a card operating system (COS). Unlike other operating systems, this software controls access to the on-card user memory. This capability permits different and multiple functions and/or different applications to reside on the card, allowing businesses to issue and maintain a diversity of 'products'



through the card. One example of this is a debit card that also enables building access on a college campus. Multifunction cards benefit issuers by enabling them to market their products and services via state-of-the-art transaction technology. Specifically, the technology permits information updates without replacement of the installed base of cards, greatly simplifying program changes and reducing costs. For the card user, multifunction means greater convenience and security, and ultimately, consolidation of multiple cards down to a select few that serve many purposes.

CardLogix focuses on software and hardware solutions designed to implement multi-application card systems with a low degree of risk. The M.O.S.T.™ Card Family from CardLogix features a powerful 8, 16 and 32-bit CMOS microcontrollers that have the CardLogix operating system fused into the chip. The operating system command set is further enhanced by the use of the Winplex and Cardplex Application Program Interface (API).

Reader and Terminal Basics

For the sake of clearly defining all of the different hardware devices that smart cards can be plugged into, the industry has adopted the following definitions:

The term “reader” is used to describe a unit that interfaces with a PC for the majority of its processing requirements. In contrast, a “terminal” is a self-contained processing device.

Both terminals and readers read and write to smart cards. Readers come in many form factors and in a wide variety of capabilities. The easiest way to describe a reader is by the method of its interface to a PC. Smart Card Readers are available that interface to RS232 serial ports, USB ports, PCMCIA slots, floppy disk slots, parallel ports, infrared (IRDA) ports and keyboards and keyboard wedge readers. Another difference in reader types is the on-board intelligence and capabilities or lack thereof. Large price and performance differences exist between an industrial strength intelligent reader that supports a wide variety of card protocols and a home style win-card reader that only works with microprocessor cards. These are typically “dumb” readers.

The options in terminal choices are just as wide. Most have their own operating systems and development tools. They typically support other functions such as magstripe reading, modem functions and transaction printing.

Standards

Primarily, smart card standards govern physical card properties and communication characteristics of the embedded chip. This standard is known as ISO 7816-1,2,3.

Application-specific properties are being debated with many large organizations and groups proposing their standards. Open system card interoperability should apply at several levels; 1) to the card itself, its access terminals (readers), the networks and the card issuers’ own systems. This will only be achieved by conformance to international standards. This site’s sponsors are committed to compliance with ISO and CEN standards as well as industry initiatives such as EMV, the Open Card Framework and PC/SC specifications.

These organizations are active in smart card standardization:

The International Standards Organization (ISO) facilitates the creation of voluntary standards through a process that is open to all parties. ISO 7816 is the international standard for integrated-circuit cards (commonly known as smart cards) that use electrical contacts. Anyone interested in obtaining a technical understanding of smart cards needs to become familiar with what ISO 7816 does NOT cover as well as what it does. Copies of these documents can be purchased through ANSI American National Standards Institute. ANSI’s address and phone is: 11 West 42nd Street, New York, NY 10036 - (212) 642-4900.

National Institute of Standards and Technology (NIST) publishes a document known as FIPS 140-1, “Security Requirements for Cryptographic Modules”. This concerns physical security of a smart card chip, defined as a type of cryptographic module.

Europay, MasterCard and Visa have created their “Integrated Circuit Card Specifications for Payment Systems”. The specification is intended to create a common technical basis for card and system implementation of a stored value system. Integrated Circuit Card Specifications for Payment Systems can be obtained from a Visa, MasterCard or Europay member bank.

Microsoft has proposed a standard for cards and readers, called the PC/SC specification. This proposal only applies to CPU cards.

CEN or the (Comite’ Europe’ en de Normalisation) and ETSI (European Telecommunications Standards Institute) is focused on telecommunications, as with the GSM SIM for cellular telephones. GSM 11.11 and ETSI300045. CEN can be contacted at Rue de Stassart,36 B-1050 Brussels, Belgium, attention to the Central Secretariat.

ISO 7816 Summary This is a quick overview of what the 7816 specifications cover. Some of these are frozen and some are in revision; please check with ANSI for the most current revision. ISO 7816 has six parts. Some have been completed; others are currently in draft stage.

Part 1: Physical characteristics-ISO 7816-1:1987 defines the physical dimensions of contact smart cards and their resistance to static electricity, electromagnetic radiation and mechanical stress. It also describes the physical location of an IC card's magnetic stripe and embossing area.

Part 2: Dimensions and Location of Contacts- ISO7816-2:1988 Defines the location, purpose and electrical characteristics of the card's metallic contacts (see above illustration).

Part 3: Electronic Signals and Transmission Protocols- ISO 7816-3:1989 defines the voltage and current requirements for the electrical contacts as defined in Part 2 and asynchronous half-duplex character transmission protocol (T=0). Amendment 1:1992 Protocol type T=1, asynchronous half duplex block transmission protocol. Smart cards that use a proprietary transmission protocol carry the designation, T=14. Amendment 2:1994 Revision of protocol type selection.

Part 4: Inter-industry Commands for Interchange ISO 7816-4establishes a set of commands for CPU cards across all industries to provide access, security and transmission of card data. Within this basic kernel, for example, are commands to read, write and update records.

Part 5: Numbering System and Registration Procedure for Application Identifiers- ISO 7816-5:1994 establishes standards for Application Identifiers (AIDs). An AID has two parts. The first is a Registered Application Provider Identifier (RID) of five bytes that is unique to the vendor. The second part is a variable length field of up to 11 bytes that RIDs can use to identify specific applications.

Part 6: Inter-industry data elements- ISO 7816-6 Details the physical transportation of device and transaction data, answer to reset and transmission protocols. The specifications permit two transmission protocols: character protocol (T=0) or block protocol (T=1). A card may support either but not both. (Note: Some card manufacturers adhere to neither of these protocols. The transmission protocols for such cards are described as T=14).

System Planning and Deployment

Smart card system design requires advance planning to be successful and to avoid problems. It is highly recommended that you graphically diagram the flow of information for your new system. The first question is always: Will the card and system transact information, or value, or both? If it stores keys or value i.e. gift certificates or sports tickets, greater design detail is required than in data-only systems. When you combine information types on a single card, other issues arise. The key to success is not to overrun the system with features that can confuse users and cause problems in management. We recommend that you phase-in each feature set as each one is working. To properly implement a functional smart card system you should be able to answer the following questions. **NOTE:** These are only general guidelines, provided as a basis for your individual planning. Many other steps may be involved and are not mentioned here.

Basic Set-Up

1. Is there a clear business case? Including financial and consumer behavior factors?
2. Will the system be single or multi-application?
3. What information do I want to store in the cards?
4. How much memory is required for each application?
5. If multi-application, how will I separate different types of data?
6. Will card data be obtained from a database? Or loaded every time?
7. Will this data concurrently reside on a database?
8. How many cards will be needed?
9. Are card/infrastructure vendors identified? What are the lead times?

Security

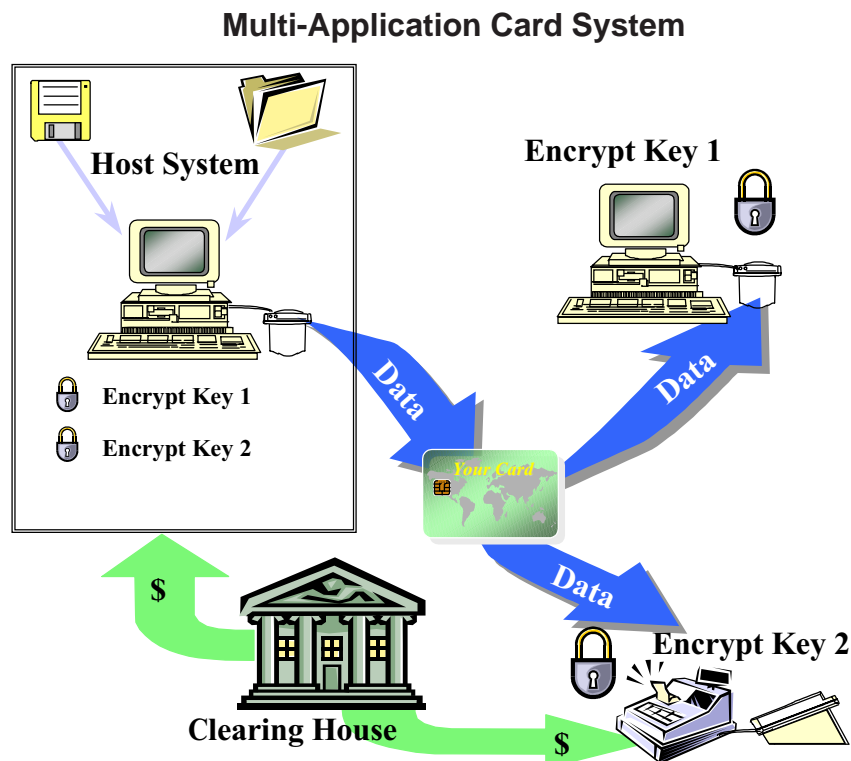
1. What are the security requirements?
2. Does all, or only some of the data need to be secure?
3. Who will have access to this information?
4. Who will be allowed to change this information?
5. In what manner shall I secure this data i.e. encryption, Host passwords, card passwords/PINs or all of these?
6. Should the keys/PINs be customer or system-activated?
7. What form of version control do I want?

Value Applications

1. Should the value in the cards be reloadable or will the cards be disposable?
2. How will I distribute the cards?
3. How will cards be activated and loaded with value?
4. What type of card traceability should I implement?
5. What is the minimum and maximum value to store on each card?
6. Will there be a refund policy?

General

1. How many types of artwork will be included in the issuance?
2. Who will do the artwork?
3. What is needed on the card? For example signature panels, Mag-Stripe, Embossing etc.
4. It is highly recommended that you graphically diagram the flow of information.



Building a smart card system that stores value i.e. gift certificates, show tickets, redemption points or cash equivalents requires an attention to detail not necessary in other information management systems. The key to success is not to overrun the system with features that can confuse users and cause problems in management. We recommend that you phase-in each feature set after the first one is working. Here is a list of some questions that are pertinent to these systems in addition to the above questions.

Deployment

- A. We recommend as the minimum steps in deploying a Stored Value or Multi-Application System.
- B. Establish clear achievable program objectives
- C. Make sure the organization has a stake in the project's success and that management buys into the project.
- D. Set a budget.
- E. Name a project manager.
- F. Assemble a project team and create a team vision.
- G. Graphically create an information - card and funds-flow diagram.
- H. Assess the card and reader options.
- I. Write a detailed specification for the system.
- J. Set a realistic schedule with inch-stones and mile-stones.
- K. Establish the security parameters for both people and the system.
- L. Phase-in each system element, testing as you deploy.
- M. Reassess for security leaks.
- N. Deploy the first phase of cards and test, test.
- O. Train the key employees responsible for each area.
- P. Set-up a system user manual.
- Q. Check the reporting structures.
- R. Have contingency plans should problems arise.
- S. Deploy and announce.
- T. Advertise and market your system.

Security Basics

Smart cards provide computing and business systems the enormous benefit of portable and secure storage of data and value. At the same time, the integration of smart cards into your system introduces its own security management issues, as people access card data far and wide in a variety of applications.

The following is a basic discussion of system security and smart cards, designed to familiarize you with the terminology and concepts you need in order to start your security planning.

What Is Security?

Security is basically the protection of something valuable to ensure that it is not stolen, lost, or altered. The term "data security" governs an extremely wide range of applications and touches everyone's daily life. Concerns over data security are at an all-time high, due to the rapid advancement of technology into virtually every transaction, from parking meters to national defense.

Data is created, updated, exchanged and stored via networks. A network is any computing system where users are highly interactive and interdependent and by definition, not all in the same physical place. In any network, diversity abounds, certainly in terms of types of data, but also types of users. For that reason, a system of security is essential to maintain computing and network functions, keep sensitive data secret, or simply maintain worker safety. Any one company might provide an example of these multiple security concerns: Take, for instance, a pharmaceutical manufacturer:

Example: Pharmaceutical Manufacturer Security Concerns

| Type of Data | Security Concern | Type of Access |
|-------------------------------------|---|--|
| Drug Formula | Basis of Business income. Competitor Spying | Highly Selective list of executives |
| Accounting, Regulatory | Required by law | Relevant executives and departments |
| Personnel Files | Employee Privacy | Relevant executives and departments |
| Employee I.D. | Non-employee access. Inaccurate payroll, benefits assignment. | Relevant executives and departments |
| Facilities | Access authorization | Individuals per function and clearance |
| Building safety, emergency response | All employees | |

What Is Information Security?

Information security is the application of measures to ensure the safety and privacy of data by managing its storage and distribution. Information security has both technical and social implications. The first simply deals with the 'how' and 'how much' question of applying secure measures at a reasonable cost. The second grapples with issues of individual freedom, public concerns, legal standards and how the need for privacy intersects them. This discussion covers a range of options open to business managers, system planners and programmers that will contribute to your security strategy. The ultimate choice rests with the system designer and issuer.

The Elements Of Data Security

When implementing a security system, all data networks deal with the following main elements:

1. **Hardware**, including servers, redundant mass storage devices, communication channels and lines, hardware tokens (smart cards) and remotely located devices (e.g., thin clients or Internet appliances) serving as interfaces between users and computers
2. **Software**, including operating systems, database management systems, communication and security application programs.
3. **Data**, including databases containing customer - related information.
4. **Personnel**, to act as originators and/or users of the data; professional personnel, clerical staff, administrative personnel, and computer staff.

The Mechanisms Of Data Security

Working with the above elements, an effective data security system works with the following key mechanisms to answer:

1. **Has My Data Arrived Intact?** (Data Integrity) This mechanism ensures that data was not lost or corrupted when it was sent to you.
2. **Is The Data Correct And Does It Come From The Right Person?** (Authentication) This proves user or system identities.
3. **Can I Confirm Receipt Of The Data And Sender Identity Back To The Sender?** (Non-Repudiation)
4. **Can I Keep This Data Private?** (Confidentiality) – Ensures only senders and receivers have access to the data. This is typically done by employing one or more encryption techniques to secure your data.
5. **Can I Safely Share This Data If I Choose?** (Authorization and Delegation) You can set and manage access privileges for additional users and groups.
6. **Can I Verify The That The System Is Working?** (Auditing and Logging) Provides a constant monitor and troubleshooting of security system function.
7. **Can I Actively Manage The System?** (Management) Allows administration of your security system.

Data Integrity

This function verifies the characteristics of a document and a transaction. Characteristics of both are inspected and confirmed for content and correct authorization. Data Integrity is achieved with electronic cryptography that assigns a unique identity to data like a fingerprint. Any attempt to change this identity signals the change and flags any tampering.

Authentication

This inspects, then confirms, the proper identity of people involved in a transaction of data. In Authentication, a Digital Signature verifies data at its origination by producing an identity that can be mutually verified by all parties involved in the transaction. A cryptographic hash algorithm produces a Digital Signature.

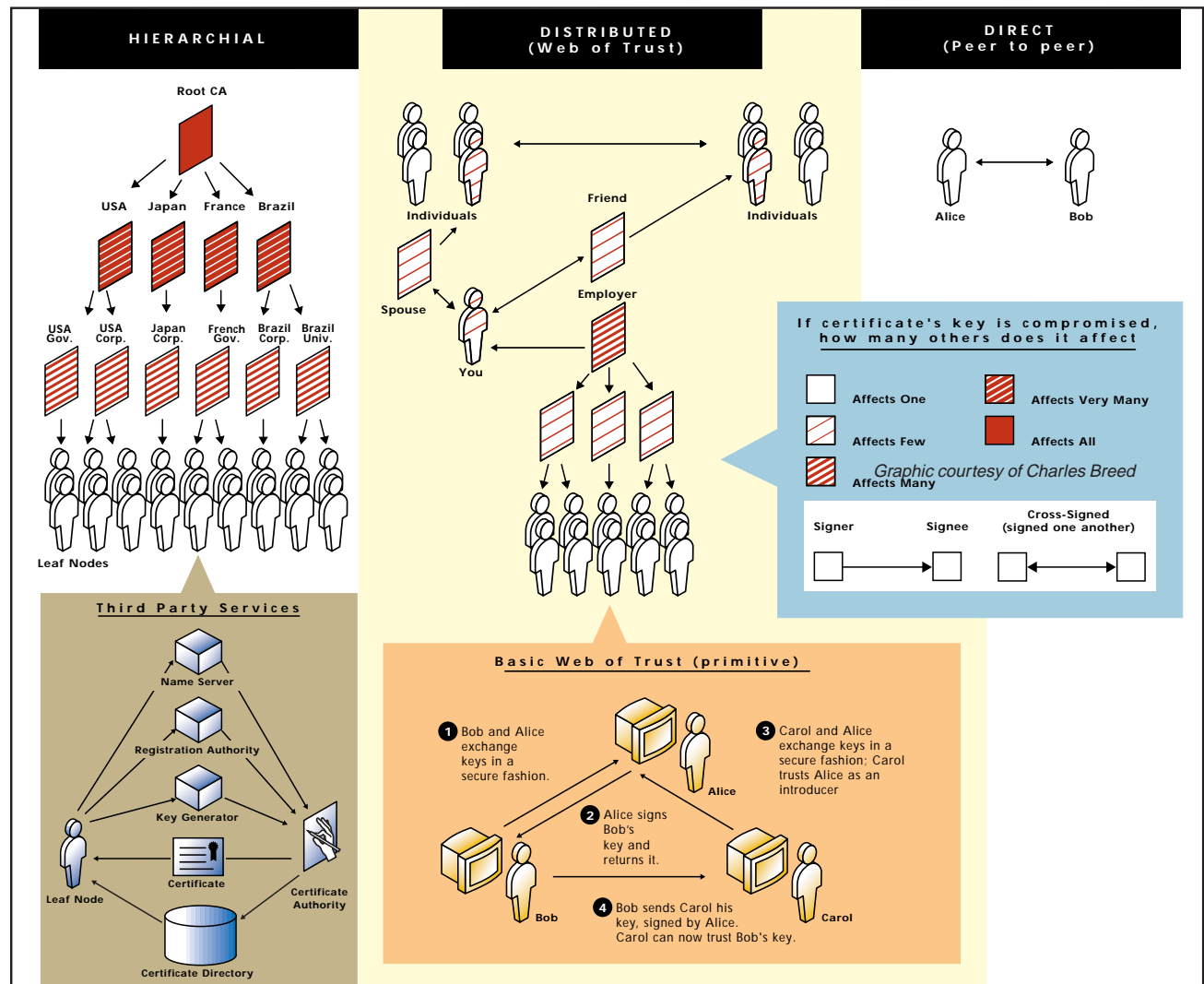
Non-Repudiation

This eliminates the possibility of a transaction being repudiated, or invalidated by incorporating a Digital Signature that a third party can verify as correct. Similar in concept to registered mail, the recipient of data re-hashes it, verifies the Digital Signature, and compares the two to see that they match.

Authorization and Delegation

Authorization is the processes of allowing access to specific data within a system. Delegation is the utilization of a third party to manage and certify each of the users of your system, (Certificate Authorities - CA).

Authorization and Trust Model



Graphic courtesy of Charles Breed

Auditing and Logging

This is the independent examination and recording of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

Management

Is the oversight and design of the elements and mechanisms discussed above and below.

Confidentiality/Cryptography

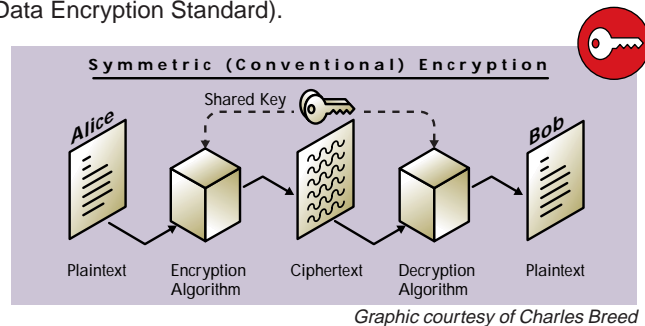
Confidentiality is the use of encryption to protect information from unauthorized disclosure. Plain text is turned into cipher text via an algorithm, then decrypted back into plain text using the same method.

Cryptography is the method of converting data from a human readable form to a modified form, and then back to its original readable form, to make unauthorized access difficult. Cryptography is used in the following ways:

- Ensure data privacy, by encrypting data
- Ensures data integrity, by recognizing if data has been manipulated in an unauthorized way
- Ensures data uniqueness by checking that data is “original”, and not a “copy” of the “original”. The sender attaches a unique identifier to the “original” data. This unique identifier is then checked by the receiver of the data.

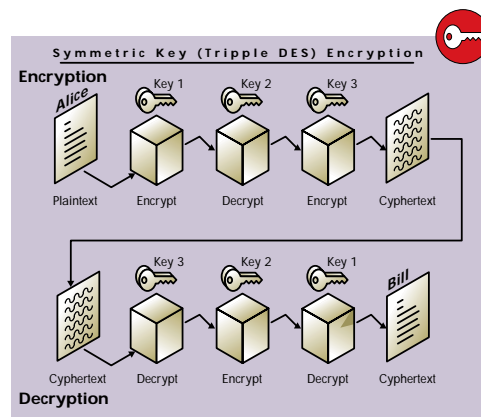
The original data may be in a human-readable form, such as a text file, or it may be in a computer-readable form, such as a database, spreadsheet or graphics file. The original data is called **unencrypted data** or **plain text**. The modified data is called **encrypted data** or **cipher text**. The process of converting the unencrypted data is called **encryption**. The process of converting encrypted data to unencrypted data is called **decryption**.

In order to convert the data, you need to have an encryption algorithm and a key. If the same key is used for both encryption and decryption that key is called a **secret key** and the algorithm is called a **symmetric algorithm**. The most well-known symmetric algorithm is DES (Data Encryption Standard).

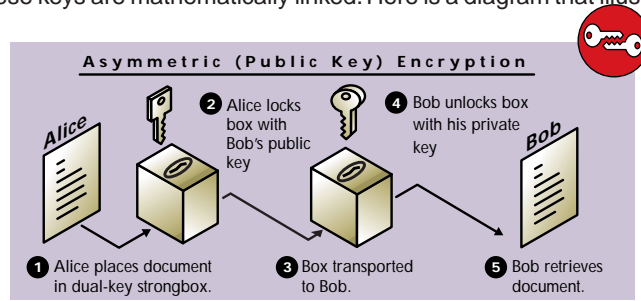


The Data Encryption Standard (DES) was invented by the IBM Corporation in the 1970's. During the process of becoming a standard algorithm, it was modified according to recommendations from the National Security Agency (NSA). The algorithm has been studied by cryptographers for nearly 20 years. During this time, no methods have been published that describe a way to break the algorithm, except for brute-force techniques. DES has a 56-bit key, which offers 2^{56} or 7×10^{16} possible variations. There are a very small numbers of weak keys, but it is easy to test for these keys and they are easy to avoid. Please contact CardLogix directly for more details.

Triple-DES is a method of using DES to provide additional security. Triple-DES can be done with two or with three keys. Since the algorithm performs an encrypt-decrypt-encrypt sequence, this is sometimes called the EDE mode. This diagram shows Triple-DES three-key mode used for encryption:



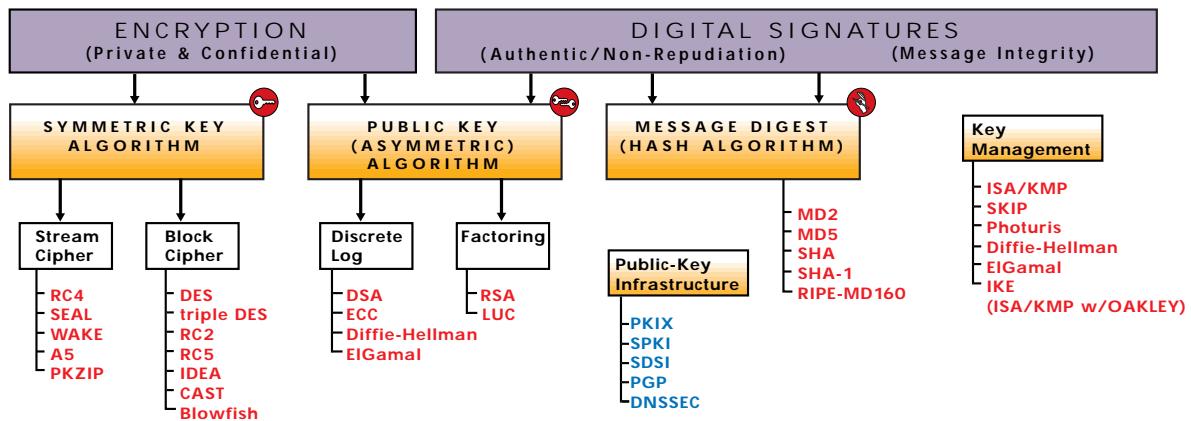
If different keys are used for encryption and decryption, the algorithm is called an **asymmetric algorithm**. The most well-known asymmetric algorithm is RSA, named after its three inventors (Rivest, Shamir, and Adleman). This algorithm uses two keys, called the **private key**. These keys are mathematically linked. Here is a diagram that illustrates an asymmetric algorithm:



Graphic courtesy of Charles Breed

Asymmetric algorithms involve extremely complex mathematics typically involving the factoring of large prime numbers. Asymmetric algorithms are typically stronger than a short key length symmetric algorithm. But because of their complexity they are used in signing a message or a certificate. They not ordinarily used for data transmission encryption.

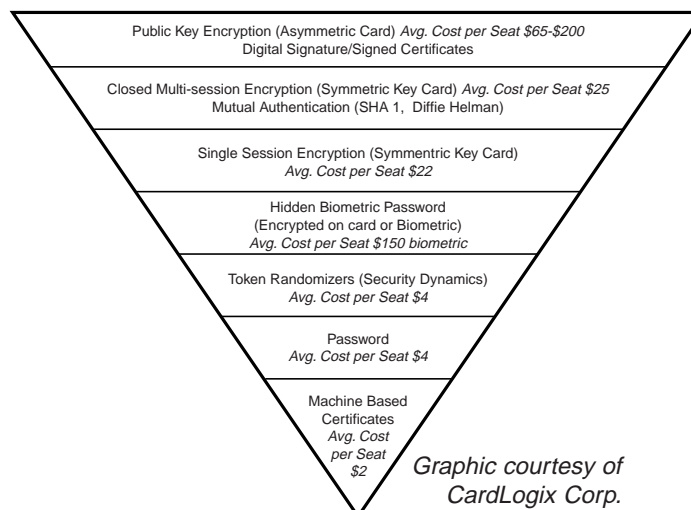
Data Security Mechanisms And Their Respective Algorithms



Graphic courtesy of Charles Breed

Smart Cards For Data Security

As the card issuer, you must define all of the parameters for card and data security. There are two methods of using cards for data system security, host-based and card-based. The safest systems employ both methodologies.



Graphic courtesy of CardLogix Corp.

Host-Based System Security

A host-based system treats a card as a simple data carrier. Because of this, straight memory cards can be used very cost-effectively for many systems. All protection of the data is done from the host computer. The card data may be encrypted but the transmission to the host can be vulnerable to attack. A common method of increasing the security is to write in the clear (not encrypted) a key that usually contains a date and/or time along with a secret reference to a set of keys on the host. Each time the card is re-written the host can write a reference to the keys. This way each transmission is different. But parts of the keys are in the clear for hackers to analyze. This security can be increased by the use of smart memory cards that employ a password mechanism to prevent unauthorized reading of the data. Unfortunately the passwords can be sniffed in the clear. Access is then possible to the main memory. These methodologies are often used when a network can batch up the data regularly and compare values and card usage and generate a problem card list.

Card-Based System Security

These systems are typically microprocessor card-based. A card, or token-based system treats a card as an active computing device. The Interaction between the host and the card can be a series of steps to determine if the card is authorized to be used in the system. The process also checks if the user can be identified, authenticated and if the card will present the appropriate credentials to conduct a transaction. The card itself can also demand the same from the host before proceeding with a transaction. The access to specific information in the card is controlled by **A)** the card's internal Operating System and **B)** the preset permissions set by the card issuer regarding the files conditions.

There are predominately two types of card operating systems. One type of card OS is the most cost-effective in many businesses because you only pay for the size and functions that you specify. This **Classic** approach treats each card as a secure computing and storage device. Files and permissions to these files are all set by the issuer in advance. The only access to the cards is through the operating system. There are no back doors, no reconfiguration of file structures on the card. Data is read or written to the card through permissions set only by the issuers. The operating system performs a set of "applications" such as authentication and encryption as requested through commands sent to the card. The CardLogix M.O.S.T. OS is one example of this type.

The second methodology is the **Disk Drive** approach to card operating systems. The card is a computing device with an active memory manager this allows you to load onto the card specific "applications" and files. The card operating system allows for active file allocation and management. It is designed for card programs that have a long expected user life (4 years +). Java Cards and the Microsoft Windows Card OS are examples of this approach. These cards have a much higher risk of tampering due to the ability to introduce active applets and or viruses into the card. You could conceivably replace a purse or file with a low value with a new purse that has the same name with a higher value.

Initial issuance of these cards is costly, due to the sophistication of the OS. The advantage of this approach is that card replacement costs can possibly go down through the use of in field upgrades. These card architectures need a larger memory for future unplanned upgrades and a larger program memory to upload applets. This translates to larger semiconductors at a higher cost. These approaches also come with a licensing burden that is ultimately paid by the card issuer. Also, the security infrastructure costs are much higher to manage due to the multiple points of entry to card system functions.

Threats To Cards and Data Security

Effective security system planning takes into account the need for authorized users to access data reasonably easily, while considering the many threats that this access presents to the integrity and safety of the information. There are basic steps to follow to secure all smart card systems, regardless of type or size.

Analysis: Type(s) of data to secure; users, points of contact, transmission. Relative risk/impact of data loss

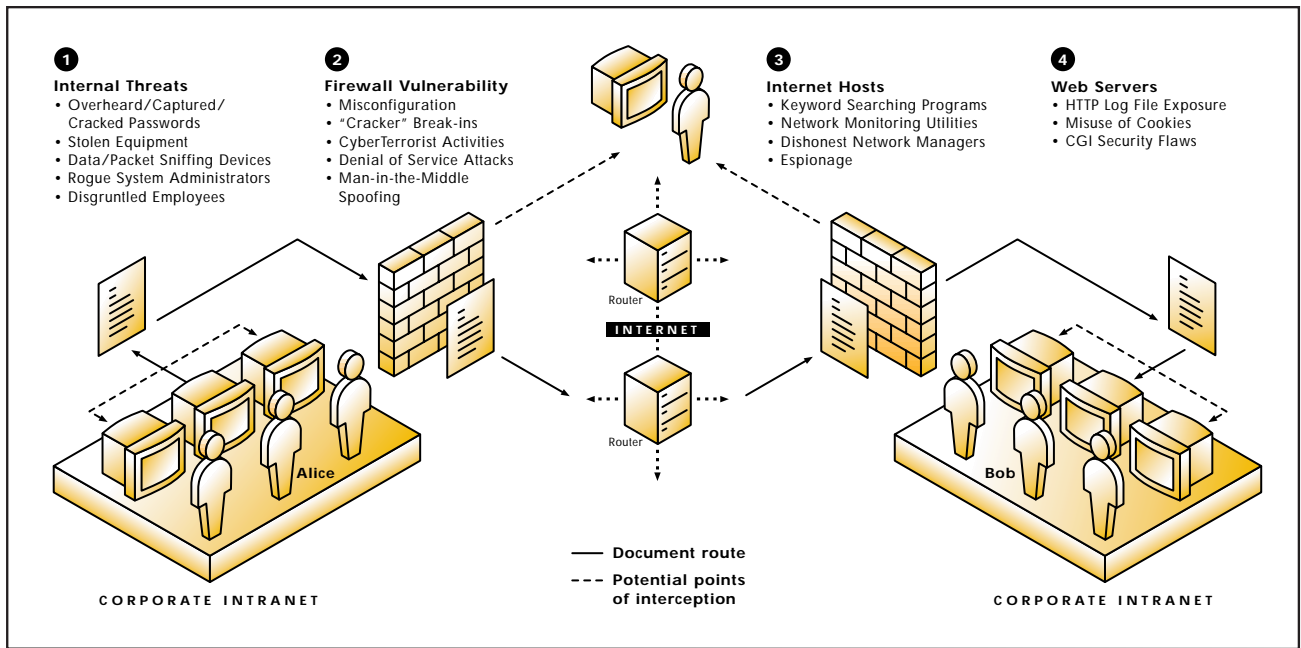
Deployment of your proposed system

Road Test: Attempt to hack your system; learn about weak spots, etc.

Synthesis: Incorporate road test data, re-deploy

Auditing: Periodic security monitoring, checks of system, fine-tuning

When analyzing the threats to your data an organization should look closely at two specific areas: Internal attacks and external attacks. The first and most common compromise of data comes from disgruntled employees. Knowing this, a good system manager separates all back-up data and back-up systems into a separately partitioned and secured space. The introduction of viruses and the attempted formatting of network drives is a typical internal attack behavior. By deploying employee cards that log an employee into the system and record the time, date and machine that the employee is on, a company automatically discourages these type of attacks.



Graphic courtesy of Charles Breed

External attacks are typically aimed at the weakest link in a company's security armor. The first place an external hacker looks at is where they can intercept the transmission of your data. In a smart card enhanced system this starts with the card.

Key Lengths

| Symmetric Cipher (Conventional) | Public Key | |
|------------------------------------|---------------------------|----------------|
| | Asymmetric (RSA, DSA, DH) | Elliptic Curve |
| 40 bits | 274 bits | 57 bits |
| 56 bits | 384 bits | 80 bits |
| 64 bits | 512 bits | 106 bits |
| 80 bits | 1024 bits | 132 bits |
| 96 bits | 1536 bits | 160 bits |
| 112 bits | 2048 bits | 185 bits |
| 120 bits | 2560 bits | 237 bits |
| 128 bits | 3072 bits | 256 bits |

Average Time for Exhaustive Key Search

| Key Length... | Number of Possible Keys | Time required at 1 encryption/ μ sec | Time required at 10^6 encryptions/ μ sec |
|---------------|--------------------------------|---|--|
| 32 bits | $2^{32} = 4.3 \times 10^9$ | $2^{31} \mu$ sec = ~36 min | ~2 millisc |
| 56 bits | $2^{56} = 7.2 \times 10^{16}$ | $2^{55} \mu$ sec = 1142 yrs | ~10 hours |
| 128 bits | $2^{128} = 3.4 \times 10^{38}$ | $2^{127} \mu$ sec = $\sim 5 \times 10^{24}$ | $\sim 5 \times 10^{18}$ yrs |

Brute Force Attack

Average Times needed to search half the symmetric key-space (worst case scenario would be twice as long)

| Key Length (bits) | ATTACKER'S CAPABILITY | | | | |
|-------------------|-----------------------|-------------|------------------|---------------|------------------------------|
| | Individual Attacker | Small Group | Academic Network | Large Company | Military Intelligence Agency |
| 40 | weeks | days | hours | milliseconds | microseconds |
| 56 | centuries | decades | years | hours | seconds |
| 64 | millennia | centuries | decades | days | minutes |
| 80 | infeasible | infeasible | infeasible | centuries | centuries |
| 128 | infeasible | infeasible | infeasible | infeasible | millennia |

Assumptions are based on 1997 technology:
Individual Attacker: one high-end desktop machine and software ($2^{17} - 2^{24}$ keys/second)
Small Group: 16 high-end machines and software ($2^{21} - 2^{24}$ keys/second)
Academic Network: 256 high-end machines and software ($2^{25} - 2^{28}$ keys/second)
Large Company: \$1,000,000 hardware budget (2^{43} keys/second)
Military Intelligence Agency: \$1,000,000,000 hardware budget and advanced technology (2^{55} keys/second)

Passphrase Guessing (dictionary attack)

Using easy-to-remember English words results in approximately 1.3 bits of entropy per character, (word space) vs. purely random characters (total space).

| Strong | OK | Weak | example | # of characters | complexity | word space | total space | time-to-break total space |
|--------|----|------|----------------|-----------------|--------------------|------------|-------------|-------------------------------------|
| | | | "dogie" | 5 | 25 (lowercase) | 12 bits | 23.5 bits | 40 minutes |
| | | | "br1a9Az" | 7 | 62 (alphanumeric) | 24 bits | 41.7 bits | 22 years |
| | | | ".,THX1lb<V+." | 10 | 95 (full keyboard) | 40 bits | 65.7 bits | Infeasible (3.8×10^8 yrs) |

Graphic courtesy of Charles Breed

Threats To Cards and Data Security (cont.)

The following sets of questions are relevant to your analysis. Is the data on the card transmitted in the clear or is it encrypted? If the transmission is sniffed, is each session secured with a different key? Does the data move from the reader to the PC in the clear? Does the PC or client transmit the data in the clear? If the packet is sniffed, is each session secured with a different key? Does the operating system have a back door? Is there a mechanism to upload and download functioning code? How secure is this system? Does the OS provider have a good security track record? Does the card manufacturer have precautions in place to secure your data? Do they understand the liabilities? Can they provide other security measures that can be implemented on the card and or module? When the card is subjected to *Differential Power* attacks and *Differential Thermal* attacks does the OS reveal any secrets? Will the semiconductor utilized meet this scrutiny? Do your suppliers understand these questions?

Other types of problems that can be a threat to your assets include:

- Improperly secured passwords (writing them down, sharing)
- Assigned PINs and the replacement mechanisms
- Delegated Authentication Services
- Poor data segmentation
- Physical Security (the physical removal or destruction of your computing hardware)

Security Architectures

When designing a system a planner should look at the total cost of ownership this includes:

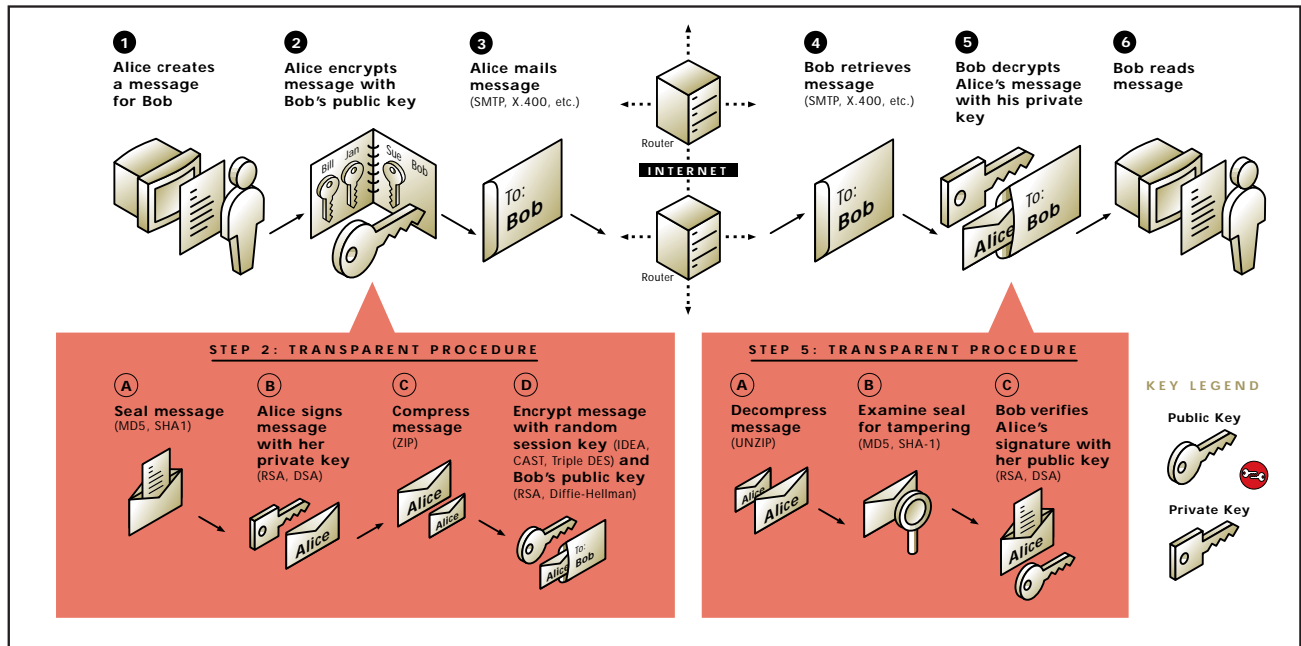
- Analysis
- Installation and Deployment
- Delegated Services
- Training
- Management
- Audits and Upgrades
- Infrastructure Costs (Software and Hardware)

Over 99% of all U.S.- based financial networks are secured with a Private Key Infrastructure. This is changing over time, based on the sheer volume of transactions managed daily and the hassles that come with private key management. Private Key-based systems make good sense if your expected user base is less than 500,000 participants.

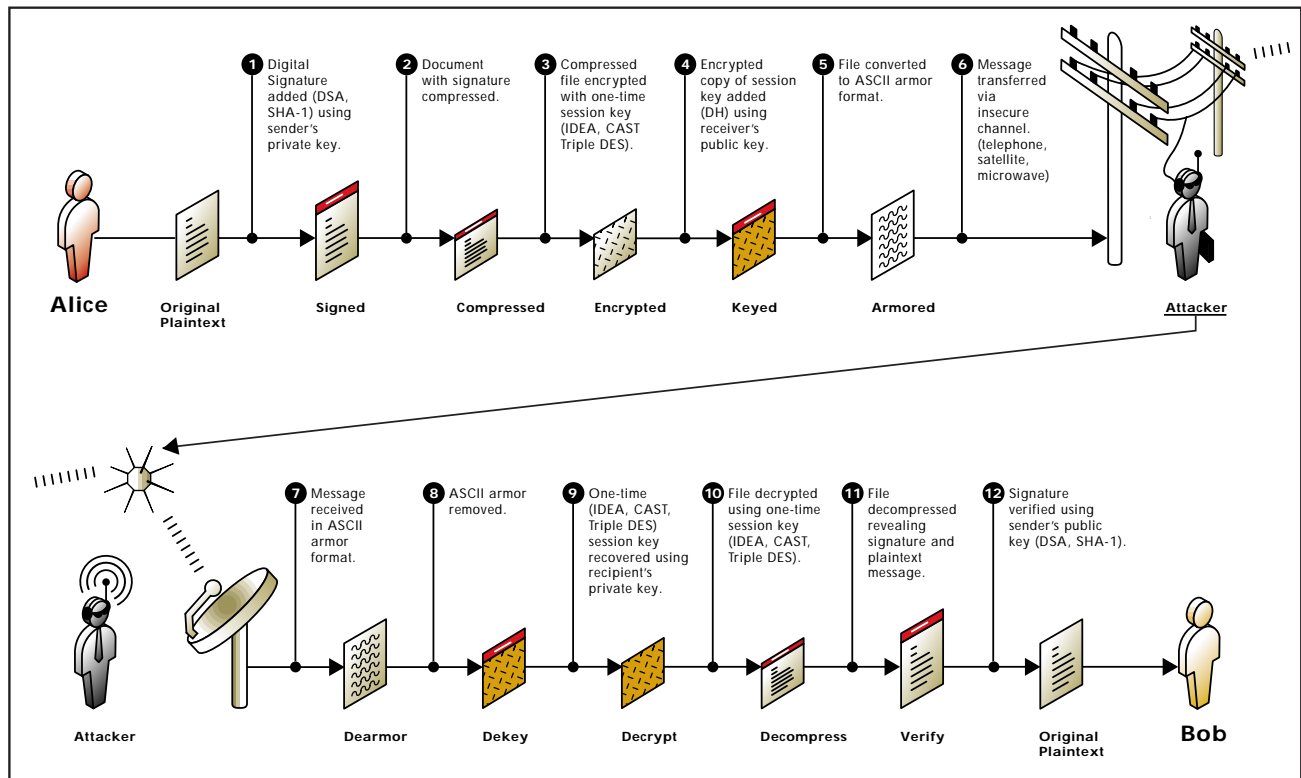
Public Key Systems are typically cost effective only in large volumes or where the value of data is so high that its worth the higher costs associated with this type of deployment. What most people don't realize is that Public Key systems still rely heavily on Private Key encryption for all transmission of data. The Public Key encryption algorithms are only used for non-repudiation and to secure data integrity. Public Key infrastructures as a rule employ every mechanism of data security in a nested and coordinated fashion to insure the highest level of security available today.

Public Key infrastructure

How it works. Typical System (example)



Graphic courtesy of Charles Breed



Graphic courtesy of Charles Breed

Conclusion

Smart cards can add convenience and safety to any transaction of value and data; but the choices facing today's managers can be daunting. We hope this booklet has adequately presented the options and given you enough information to make informed evaluations of performance, cost and security that will produce a smart card system that fits today's needs and those of tomorrow. It is our sincere belief that informed users make better choices, which leads to smarter business for everybody.

Glossary

This glossary is an amalgamation of information from many sources The primary two being the US government N.I.S.T. site on security terms and the CardLogix Corporation Smart Card Glossary. This list is always growing...so if you don't find your answer, check back with us soon.

Active Attack

An attack which results in an unauthorized state change, such as the manipulation of files, or the adding of unauthorized files

Administrative Security

The management constraints and supplemental controls established to provide an acceptable level of protection for data.

AIS

Automated Information System - any equipment of an interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, control, display, transmission, or reception of data and includes software, firmware, and hardware.

Alert

A formatted message describing a circumstance relevant to network security. Alerts are often derived from critical audit events.

Ankle-Biter

A person who aspires to be a hacker/cracker but has very limited knowledge or skills related to AIS's. Usually associated with young teens who collect and use simple malicious programs obtained from the Internet.

Anomaly Detection Model

A model where intrusions are detected by looking for activity that is different from the user's or system's normal behavior.

Application Level Gateway

(Firewall) A firewall system in which service is provided by processes that maintain complete TCP connection state and sequencing. Application level firewalls often re-address traffic so that outgoing traffic appears to have originated from the firewall, rather than the internal host.

ASIM

Automated Security Incident Measurement - Monitors network traffic and collects information on targeted unit networks by detecting unauthorized network activity.

Assessment

Surveys and Inspections; an analysis of the vulnerabilities of an AIS. Information acquisition and review process designed to assist a customer to determine how best to use resources to protect information in systems.

Assurance

A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy.

Attack

An attempt to bypass security controls on a computer. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.

Audit

The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

Audit Trail

In computer security systems, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.

Authenticate

To establish the validity of a claimed user or object.

Authentication

To positively verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

Authentication Header (AH)

A field that immediately follows the IP header in an IP datagram and provides authentication and integrity checking for the datagram.

Automated Security Monitoring

All security features needed to provide an acceptable level of protection for hardware, software, and classified, sensitive, unclassified or critical data, material, or processes in the system.

Availability

Assuring information and communications services will be ready for use when expected.

Back Door

A hole in the security of a computer system deliberately left in place by designers or maintainers. Synonymous with trap door; a hidden software or hardware mechanism used to circumvent security controls.

Bell-La Padula Security Model

Formal-state transition model of computer security policy that describes a formal set of access controls based on information sensitivity and subject authorizations.

Biba Integrity Model

A formal security model for the integrity of subjects and objects in a system.

Bomb

A general synonym for crash, normally of software or operating system failures.

Breach

The successful defeat of security controls which could result in a penetration of the system. A violation of controls of a particular information system such that information assets or system components are unduly exposed.

Buffer Overflow

This happens when more data is put into a buffer or holding area, then the buffer can handle. This is due to a mismatch in processing rates between the producing and consuming processes. This can result in system crashes or the creation of a back door leading to system access.

Bug

An unwanted and unintended property of a program or piece of hardware, especially one that causes it to malfunction.

C2

Command and Control

C2-attack

Prevent effective C2 of adversary forces by denying information to, influencing, degrading or destroying the adversary C2 system.

C2-protect

Maintain effective command and control of own forces by turning to friendly advantage or negating adversary effort to deny information to, influence, degrade, or destroy the friendly C2 system. (Pending approval in JP 1-02)

CGI

Common Gateway Interface - CGI is the method that Web servers use to allow interaction between servers and programs.

CGI Scripts

Allows for the creation of dynamic and interactive web pages. They also tend to be the most vulnerable part of a web server (besides the underlying host security).

Check_Password

A hacking program used for cracking VMS passwords.

Chernobyl Packet

Also called Kamikaze Packet. A network packet that induces a broadcast storm and network meltdown. Typically an IP Ethernet datagram that passes through a gateway with both source and destination Ethernet and IP address set as the respective broadcast addresses for the subnetworks being gated between.

Circuit Level Gateway

One form of a firewall. Validates TCP and UDP sessions before opening a connection. Creates a handshake, and once that takes place passes everything through until the session is ended.

Clipper chip

A tamper-resistant VLSI chip designed by NSA for encrypting voice communications. It conforms to the Escrow Encryption Standard (EES) and implements the Skipjack encryption algorithm.

COAST

Computer Operations, Audit, and Security Technology - is a multiple project, multiple investigator laboratory in computer security research in the Computer Sciences Department at Purdue University. It functions with close ties to researchers and engineers in major companies and government agencies. Its research is focused on real-world needs and limitations, with a special focus on security for legacy computing systems.

Command and Control Warfare

(C2W) The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare is an application of information operations in military operations and is a subset of information warfare. C2W is both offensive and defensive.

Compromise

An intrusion into a computer system where unauthorized disclosure, modification or destruction of sensitive information may have occurred

Computer Abuse

The willful or negligent unauthorized activity that affects the availability, confidentiality, or integrity of computer resources. Computer abuse includes fraud, embezzlement, theft, malicious damage, unauthorized use, denial of service, and misappropriation.

Computer Fraud

Computer-related crimes involving deliberate misrepresentation or alteration of data in order to obtain something of value.

Computer Network Attack

(CNA) Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (DODD S-3600.1 of 9 Dec 96)

Computer Security

Technological and managerial procedures applied to computer systems to ensure the availability, integrity and confidentiality of information managed by the computer system.

Computer Security Incident

Any intrusion or attempted intrusion into an automated information system (AIS). Incidents can include probes of multiple computer systems.

Computer Security Intrusion

Any event of unauthorized access or penetration to an automated information system (AIS).

Confidentiality

Assuring information will be kept secret, with access limited to appropriate persons.

COPS

Computer Oracle and Password System - A computer network monitoring system for Unix machines. Software tool for checking security on shell scripts and C programs. Checks for security weaknesses and provides warnings.

COTS Software

Commercial Off the Shelf - Software acquired by government contract through a commercial vendor. This software is a standard product, not developed by a vendor for a particular government project.

Countermeasures

Action, device, procedure, technique, or other measure that reduces the vulnerability of an automated information system. Countermeasures that are aimed at specific threats and vulnerabilities involve more sophisticated techniques as well as activities traditionally perceived as security.

Crack

A popular hacking tool used to decode encrypted passwords. System administrators also use Crack to assess weak passwords by novice users in order to enhance the security of the AIS.

Cracker

One who breaks security on an AIS.

Cracking

The act of breaking into a computer system.

Crash

A sudden, usually drastic failure of a computer system.

Cryptanalysis

Definition 1) The analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including cleartext.

Definition 2) Operations performed in converting encrypted messages to plain text without initial knowledge of the crypto-algorithm and/or key employed in the encryption.

Cryptographic Hash Function

A process that computes a value (referred to as a hashword) from a particular data unit in a manner that, when a hashword is protected, manipulation of the data is detectable.

Cryptography

The art of science concerning the principles, means, and methods for rendering plain text unintelligible and for converting encrypted messages into intelligible form.

Cryptology

The science which deals with hidden, disguised, or encrypted communications.

Cyberspace

Describes the world of connected computers and the society that gathers around them. Commonly known as the INTERNET.

Dark-side Hacker

A criminal or malicious hacker.

DARPA

Defense Advanced Research Projects Agency.

Data Driven Attack

A form of attack that is encoded in innocuous seeming data which is executed by a user or a process to implement an attack. A data driven attack is a concern for firewalls, since it may get through the firewall in data form and launch an attack against a system behind the firewall.

Data Encryption Standard

Definition 1) (DES) An unclassified crypto algorithm adopted by the National Bureau of Standards for public use.

Definition 2) A cryptographic algorithm for the protection of unclassified data, published in Federal Information Processing Standard (FIPS) 46. The DES, which was approved by the National Institute of Standards and Technology (NIST), is intended for public and government use.

Defense Information Infrastructure (DII)

The shared or interconnected system of computers, communications, data applications, security, people, training and other support structures serving DoD local, national, and worldwide information needs. DII connects DoD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to the subscribers over the Defense Information Systems Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DoD information. (Pending approval in JP 1-02)

Defensive Information Operations

A process that integrates and coordinates policies and procedures, operations, personnel, and technology to protect information and defend information systems. Defensive information operations are conducted through information assurance, physical security, operations security, counter-deception, counter-psychological operations, counter-intelligence, electronic protect, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. (Pending approval in JP 1-02)

Demon Dialer

A program which repeatedly calls the same telephone number. This is benign and legitimate for access to a BBS or malicious when used as a denial of service attack.

Denial of Service

Action(s) which prevent any part of an AIS from functioning in accordance with its intended purpose.

Derf

The act of exploiting a terminal which someone else has absent mindedly left logged on.

DES

See Data Encryption Standard

Differential Power

Differential Thermal

DNS Spoofing

Assuming the DNS name of another system by either corrupting the name service cache of a victim system, or by compromising a domain name server for a valid domain.

Electronic Attack (EA)

That division of EW involving the use of electromagnetic, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. EA includes: actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception and employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency, particle beams).

Electronic Protection (EP)

That division of EW involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of EW that degrade, neutralize, or destroy friendly combat capability.

Electronic Warfare (EW)

Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are electronic attack, electronic protection, and electronic warfare support.

Electronic Warfare Support (ES)

That division of EW involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving EW operations and other tactical actions such as threat avoidance, targeting and homing. ES data can be used to produce signals intelligence. (JP 1-02)

Encapsulating Security Payload

(ESP) A mechanism to provide confidentiality and integrity protection to IP datagrams.

Ethernet Sniffing

This is listening with software to the Ethernet interface for packets that interest the user. When the software sees a packet that fits certain criteria, it logs it to a file. The most common criteria for an interesting packet is one that contains words like login or password.

False Negative

Occurs when an actual intrusive action has occurred but the system allows it to pass as non-intrusive behavior.

False Positive

Occurs when the system classifies an action as anomalous (a possible intrusion) when it is a legitimate action.

Fault Tolerance

The ability of a system or component to continue normal operation despite the presence of hardware or software faults.

Firewall

A system or combination of systems that enforces a boundary between two or more networks. Gateway that limits access between networks in accordance with local security policy. The typical firewall is an inexpensive micro-based Unix box kept clean of critical data, with many modems and public network ports on it, but just one carefully watched connection back to the rest of the cluster.

Fishbowl

To contain, isolate and monitor an unauthorized user within a system in order to gain information about the user.

Fork Bomb

Also known as Logic Bomb - Code that can be written in one line of code on any Unix system; used to recursively spawn copies of itself, "explodes" eventually eating all the process table entries and effectively locks up the system.

G (No Entries)**Hacker**

A person who enjoys exploring the details of computers and how to stretch their capabilities. A malicious or inquisitive meddler who tries to discover information by poking around. A person who enjoys learning the details of programming systems and how to stretch their capabilities, as opposed to most users who prefer to learn on the minimum necessary.

Hacking

Unauthorized use, or attempts to circumvent or bypass the security mechanisms of an information system or network.

Hacking Run

A hack session extended long outside normal working times, especially one longer than 12 hours.

Host

A single computer or workstation; it can be connected to a network

Host Based

Information, such as audit data from a single host which may be used to detect intrusions

IDEA

(International Data Encryption Algorithm) - A private key encryption-decryption algorithm that uses a key that is twice the length of a DES key.

IDIOT

Intrusion Detection In Our Time. A system that detects intrusions using pattern-matching.

Indicators & Warnings (I & W)

I & W refers to how an event or series of events can provide enough information to classify it as an incident.

Information Assurance (IA)

Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DODD S-3600.1 of 9 Dec 96)

Information Operations (IO)

Actions taken to affect adversary information and information systems while defending one's own information and information systems. (DODD S-3600.1 of 9 Dec 96)

Information Security

The result of any system of policies and/or procedures for identifying, controlling, and protecting from unauthorized disclosure, information whose protection is authorized by executive order or statute.

Information Superiority

The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (DODD S-3600.1 of 9 Dec 96)

Information Warfare (IW)

Definition 1) Actions taken to achieve information superiority by affecting adversary information, information based processes, and information systems, while defending our own information, information based processes, and information systems. Any action to deny, exploit, corrupt, or destroy the enemy's information and its functions, protect themselves against those actions; and exploiting their own military information functions.

Definition 2) Information Operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. (DODD S-3600.1 of 9 Dec 96)

Integrity

Assuring information will not be accidentally or maliciously altered or destroyed

Internet Worm

A worm program (see: Worm) that was unleashed on the Internet in 1988. It was written by Robert T. Morris as an experiment that got out of hand.

Intrusion

Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.

Intrusion Detection

Pertaining to techniques which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.

IP Splicing / Hijacking

An action whereby an active, established, session is intercepted and co-opted by the unauthorized user. IP splicing attacks may occur after an authentication has been made, permitting the attacker to assume the role of an already authorized user. Primary protections against IP splicing rely on encryption at the session or network layer.

IP Spoofing

An attack whereby a system attempts to illicitly impersonate another system by using IP network address.

J (No Entries)

Key

A symbol or sequence of symbols (or electrical or mechanical correlates of symbols) applied to text in order to encrypt or decrypt

Key Escrow

The system of giving a piece of a key to each of a certain number of trustees such that the key can be recovered with the collaboration of all the trustees.

Keystroke Monitoring

A specialized form of audit trail software, or a specially designed device, that records every key struck by a user and every character of the response that the AIS returns to the user.

LAN

Local Area Network - A computer communications system limited to no more than a few miles and using high-speed connections (2 to 100 megabits per second). A short-haul communications system that connects ADP devices in a building or group of buildings within a few square kilometers, including workstations, front-end processors, controllers, switches, and gateways.

Leapfrog Attack

Use of user id and password information obtained illicitly from one host to compromise another host. The act of TELNETing through one or more hosts in order to preclude a trace (a standard cracker procedure).

Letterbomb

A piece of email containing live data intended to do malicious things to the recipient's machine or terminal. Under UNIX, a letter bomb can also try to get part of its contents interpreted as a shell command to the mailer. The results of this could range from silly to denial of service.

Logic Bomb

Also known as a Fork Bomb - A resident computer program which, when executed, checks for a particular condition or particular state of the system which, when satisfied, triggers the perpetration of an unauthorized act

Mailbomb

The mail sent to urge others to send massive amounts of email to a single system or person, with the intent to crash the recipient's system. Mail bombing is widely regarded as a serious offense.

Malicious Code

Hardware, software, or firmware that is intentionally included in a system for an unauthorized purpose; e.g. a Trojan horse

Metric

A random variable x representing a quantitative measure accumulated over a period.

Mimicking

Synonymous with Impersonation, Masquerading or Spoofing.

Misuse Detection Model

The system detects intrusions by looking for activity that corresponds to a known intrusion techniques or system vulnerabilities. Also known as Rules Based detection.

Mockingbird

A computer program or process which mimics the legitimate behavior of a normal system feature (or other apparently useful function) but performs malicious activities once invoked by the user.

Multihost Based Auditing

Audit data from multiple hosts may be used to detect intrusions.

Nak Attack

Negative Acknowledgment - A penetration technique which capitalizes on a potential weakness in an operating system that does not handle asynchronous interrupts properly and thus, leaves the system in an unprotected state during such interrupts.

National Computer Security Center (NCSC)

Originally named the DoD Computer Security Center, the NCSC is responsible for encouraging the widespread availability of trusted computer systems throughout the Federal Government. (AF9K_JBC.TXT) (NCSC) With the signing of NSDD-145; the NCSC is responsible for encouraging the widespread availability of trusted computer systems throughout the Federal Government. (NCSC-WA-001-85)

National Information Infrastructure (NII)

The nation-wide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The NII encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, monitors, printers and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the NII. (Pending approval in JP 1-02)

NCSC

See National Computer Security Center

Network

Two or more machines interconnected for communications.

Network Based

Network traffic data along with audit data from the hosts used to detect intrusions.

Network Level Firewall

A firewall in which traffic is examined at the network protocol (IP) packet level.

Network Security

Protection of networks and their services from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side-effects. Network security includes providing for data integrity.

Network Security Officer

Individual formally appointed by a designated approving authority to ensure that the provisions of all applicable directives are implemented throughout the life cycle of an automated information system network.

Network Weaving

Another name for "Leapfrogging"

Non-Discretionary Security

The aspect of DOD security policy which restricts access on the basis of security levels. A security level is composed of a read level and a category set restriction. For read-access to an item of information, a user must have a clearance level greater than or equal to the classification of the information and also have a category clearance which includes all of the access categories specified for the information.

Non-Repudiation

Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.

Open Security

Environment that does not provide environment sufficient assurance that applications and equipment are protected against the introduction of malicious logic prior to or during the operation of a system.

Open Systems Security

Provision of tools for the secure internetworking of open systems.

Operational Data Security

The protection of data from either accidental or unauthorized, intentional modification, destruction, or disclosure during input, processing, or output operations.

Operations Security

Definition 1) The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities.

Definition 2) An analytical process by which the U.S. Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting evidence of the planning and execution of sensitive activities and operations.

Operations Security (OPSEC)

A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. Identify those actions that can be observed by adversary intelligence systems. b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (JP 1-02)

Orange Book

See Trusted Computer Security Evaluation Criteria

OSI

Open Systems Interconnection. A set of internationally accepted and openly developed standards that meet the needs of network resource administration and integrated network utility.

Packet

A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.

Packet Filter

Inspects each packet for user defined content, such as an IP address but does not track the state of sessions. This is one of the least secure types of firewall.

Packet Filtering

A feature incorporated into routers and bridges to limit the flow of information based on pre-determined communications such as source, destination, or type of service being provided by the network. Packet filters let the administrator limit protocol specific traffic to one network segment, isolate email domains, and perform many other traffic control functions.

Packet Sniffer

A device or program that monitors the data traveling between computers on a network

Passive Attack

Attack which does not result in an unauthorized state change, such as an attack that only monitors and/or records data.

Passive Threat

The threat of unauthorized disclosure of information without changing the state of the system. A type of threat that involves the interception, not the alteration, of information.

PEM (Privacy Enhanced Mail)

An IETF standard for secure electronic mail exchange.

Penetration

The successful unauthorized access to an automated system.

Penetration Signature

The description of a situation or set of conditions in which a penetration could occur or of system events which in conjunction can indicate the occurrence of a penetration in progress.

Penetration Testing

The portion of security testing in which the evaluators attempt to circumvent the security features of a system. The evaluators may be assumed to use all system design and implementation documentation, that may include listings of system source code, manuals, and circuit diagrams. The evaluators work under the same constraints applied to ordinary users.

Perimeter Based Security

The technique of securing a network by controlling access to all entry and exit points of the network. Usually associated with firewalls and/or filters.

Perpetrator

The entity from the external environment that is taken to be the cause of a risk. An entity in the external environment that performs an attack, i.e. hacker.

Personnel Security

The procedures established to ensure that all personnel who have access to any classified information have the required authorizations as well as the appropriate clearances.

PGP (Pretty Good Privacy)

A freeware program primarily for secure electronic mail.

Phage

A program that modifies other programs or databases in unauthorized ways; especially one that propagates a virus or Trojan horse.

PHF

Phone book file demonstration program that hackers use to gain access to a computer system and potentially read and capture password files.

PHF hack

A well-known and vulnerable CGI script which does not filter out special characters (such as a new line) input by a user.

Phracker

An individual who combines phone phreaking with computer hacking.

Phreak(er)

An individual fascinated by the telephone system. Commonly, an individual who uses his knowledge of the telephone system to make calls at the expense of another.

Phreaking

The art and science of cracking the phone network.

Physical Security

The measures used to provide physical protection of resources against deliberate and accidental threats.

Piggy Back

The gaining of unauthorized access to a system via another user's legitimate connection.

Ping of Death

The use of Ping with a packet size higher than 65,507. This will cause a denial of service.

Plaintext

Unencrypted data.

Private Key Cryptography

An encryption methodology in which the encryptor and decryptor use the same key, which must be kept secret. This methodology is usually only used by a small group.

Probe

Any effort to gather information about a machine or its users for the apparent purpose of gaining unauthorized access to the system at a later date.

Procedural Security

See Administrative Security.

Profile

Patterns of a user's activity which can detect changes in normal routines.

Promiscuous Mode

Normally an Ethernet interface reads all address information and accepts follow-on packets only destined for itself, but when the interface is in promiscuous mode, it reads all information (sniffer), regardless of its destination.

Protocol

Agreed-upon methods of communications used by computers. A specification that describes the rules and procedures that products should follow to perform activities on a network, such as transmitting data. If they use the same protocols, products from different vendors should be able to communicate on the same network.

Prowler

A daemon that is run periodically to seek out and erase core files, truncate administrative logfiles, nuke lost+found directories, and otherwise clean up.

Proxy

A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it. A software agent that acts on behalf of a user, typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination.

Psychological Operations (PSYOP)

Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. (JP 1-02)

Public Key Cryptography

Type of cryptography in which the encryption process is publicly available and unprotected, but in which a part of the decryption key is protected so that only a party with knowledge of both parts of the decryption process can decrypt the cipher text.

Q (No Entries)**Red Book**

See Trusted Network Interpretation.

Reference Monitor

A security control concept in which an abstract machine mediates accesses to objects by subjects. In principle, a reference monitor should be complete (in that it mediates every access), isolated from modification by system entities, and verifiable. A security kernel is an implementation of a reference monitor for a given hardware base.

Replicator

Any program that acts to produce copies of itself examples include; a program, a worm, a fork bomb or virus. It is even claimed by some that UNIX and C are the symbiotic halves of an extremely successful replicator.

Retro-Virus

A retro-virus is a virus that waits until all possible backup media are infected too, so that it is not possible to restore the system to an uninfected state.

Rexd

This Unix command is the Sun RPC server for remote program execution. This daemon is started by inetd whenever a remote execution request is made.

Risk Assessment

A study of vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of security measures. The process of evaluating threats and vulnerabilities, known and postulated, to determine expected loss and establish the degree of acceptability to system operations.

Risk Management

The total process to identify, control, and minimize the impact of uncertain events. The objective of the risk management program is to reduce risk and obtain and maintain DAA (Designated Approving Authority) approval.

Rootkit

A hacker security tool that captures passwords and message traffic to and from a computer. A collection of tools that allows a hacker to provide a backdoor into a system, collect information on other systems on the network, mask the fact that the system is compromised, and much more. Rootkit is a classic example of Trojan Horse software. Rootkit is available for a wide range of operating systems.

Router

An interconnection device that is similar to a bridge but serves packets or frames containing certain protocols. Routers link LANs at the network layer.

Routing Control

The application of rules during the process of routing so as to chose or avoid specific networks, links or relays.

RSA Algorithm

RSA stands for Rivest-Shamir-Aldeman. A public-key cryptographic algorithm that hinges on the assumption that the factoring of the product of two large primes is difficult.

Rules Based Detection

The intrusion detection system detects intrusions by looking for activity that corresponds to known intrusion techniques (signatures) or system vulnerabilities. Also known as Misuse Detection.

Samurai

A hacker who hires out for legal cracking jobs, snooping for factions in corporate political fights, lawyers pursuing privacy-rights and First Amendment cases, and other parties with legitimate reasons to need an electronic locksmith.

SATAN

Security Administrator Tool for Analyzing Networks - A tool for remotely probing and identifying the vulnerabilities of systems on IP networks. A powerful freeware program which helps to identify system security weaknesses.

Secure Network Server

A device that acts as a gateway between a protected enclave and the outside world.

Secure Shell

A completely encrypted shell connection between two machines protected by a super long pass-phrase.

Security

A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.

Security Architecture

A detailed description of all aspects of the system that relate to security, along with a set of principles to guide the design. A security architecture describes how the system is put together to satisfy the security requirements.

Security Audit

A search through a computer system for security problems and vulnerabilities.

Security Countermeasures

Countermeasures that are aimed at specific threats and vulnerabilities or involve more active techniques as well as activities traditionally perceived as security

Security Domains

The sets of objects that a subject has the ability to access.

Security Features

The security-relevant functions, mechanisms, and characteristics of AIS hardware and software.

Security Incident

Any act or circumstance that involves classified information that deviates from the requirements of governing security publications. For example, compromise, possible compromise, inadvertent disclosure, and deviation.

Security Kernel

The hardware, firmware, and software elements of a Trusted Computing Base that implement the reference monitor concept. It must mediate all accesses, be protected from modification, and be verifiable as correct.

Security Label

Piece of information that represents the sensitivity of a subject or object, such as its hierarchical classification (CONFIDENTIAL, SECRET, TOP SECRET) together with any applicable non-hierarchical security categories (e.g., sensitive compartmented information, critical nuclear weapon design information).

Security Level

The combination of a hierarchical classification and a set of non-hierarchical categories that represents the sensitivity of information.

Security Officer

The ADP official having the designated responsibility for the security of and ADP system

Security Perimeter

The boundary where security controls are in effect to protect assets.

Security Policies

The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security Policy Model

A formal presentation of the security policy enforced by the system. It must identify the set of rules and practices that regulate how a system manages, protects, and distributes sensitive information.

Security Requirements

Types and levels of protection necessary for equipment, data, information, applications, and facilities.

Security Service

A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers.

Security Violation

An instance in which a user or other person circumvents or defeats the controls of a system to obtain unauthorized access to information contained therein or to system resources.

Server

A system that provides network service such as disk storage and file transfer, or a program that provides such a service. A kind of daemon which performs a service for the requester, which often runs on a computer other than the one which the server runs.

Signaling System 7 (SS-7)

A protocol used by phone companies. Has three basic functions: Supervising, Alerting and Addressing. Supervising monitors the status of a line or circuit to see if it is busy, idle, or requesting service. Alerting indicates the arrival of an incoming call. Addressing is the transmission of routing and destination signals over the network in the form of dial tone or data pulses.

Simple Network Management Protocol (SNMP)

Software used to control network communications devices using TCP/IP

Skipjack

An NSA-developed encryption algorithm for the Clipper chip. The details of the algorithm are unpublished.

Smurfing

A denial of service attack in which an attacker spoofs the source address of an echo-request ICMP (ping) packet to the broadcast address for a network, causing the machines in the network to respond en masse to the victim thereby clogging its network.

Snarf

To grab a large document or file for the purpose of using it with or without the author's permission.

Sneaker

An individual hired to break into places in order to test their security; analogous to tiger team.

Sniffer

A program to capture data across a computer network. Used by hackers to capture user id names and passwords. Software tool that audits and identifies network traffic packets. Is also used legitimately by network operations and maintenance personnel to troubleshoot network problems.

Spam

To crash a program by overrunning a fixed-site buffer with excessively large input data. Also, to cause a person or newsgroup to be flooded with irrelevant or inappropriate messages.

Special Information Operations (SIO)

Information Operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process. (DODD S-3600.1 of 9 Dec 96)

SPI

Secure Profile Inspector - A network monitoring tool for Unix, developed by the Department of Energy.

Spoofing

Pretending to be someone else. The deliberate inducement of a user or a resource to take an incorrect action. Attempt to gain access to an AIS by pretending to be an authorized user. Impersonating, masquerading, and mimicking are forms of spoofing.

SSL (Secure Sockets Layer)

A session layer protocol that provides authentication and confidentiality to applications.

Subversion

Occurs when an intruder modifies the operation of the intrusion detector to force false negatives to occur.

SYN Flood

When the SYN queue is flooded, no new connection can be opened.

TCP/IP

Transmission Control Protocol/Internetwork Protocol. The suite of protocols the Internet is based on.

tcpwrapper

A software tool for security which provides additional network logging, and restricts service access to authorized hosts by service.

Term Rule-Based Security Policy

A security policy based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users.

Terminal Hijacking

Allows an attacker, on a certain machine, to control any terminal session that is in progress. An attack hacker can send and receive terminal I/O while a user is on the terminal.

Threat

The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security.

Threat Agent

Methods and things used to exploit a vulnerability in an information system, operation, or facility; fire, natural disaster and so forth.

Threat Assessment

Process of formally evaluating the degree of threat to an information system and describing the nature of the threat.

Tiger

A software tool which scans for system weaknesses.

Tiger Team

Government and industry - sponsored teams of computer experts who attempt to break down the defenses of computer systems in an effort to uncover, and eventually patch, security holes.

Tinkerbell Program

A monitoring program used to scan incoming network connections and generate alerts when calls are received from particular sites, or when logins are attempted using certain ID's.

Topology

The map or plan of the network. The physical topology describes how the wires or cables are laid out, and the logical or electrical topology describes how the information flows.

Trace Packet

In a packet-switching network, a unique packet that causes a report of each stage of its progress to be sent to the network control center from each visited system element.

Traceroute

An operation of sending trace packets for determining information; traces the route of UDP packets for the local host to a remote host. Normally traceroute displays the time and location of the route taken to reach its destination computer.

Tranquillity

A security model rule stating that the security level of an active object cannot change during the period of activity.

Tripwire

A software tool for security. Basically, it works with a database that maintains information about the byte count of files. If the byte count has changed, it will identify it to the system security manager.

Trojan Horse

An apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data.

Trusted Computer System Evaluation Criteria

(TCSEC) A system that employs sufficient hardware and software assurance measures to allow its use for simultaneous processing of a range of sensitive or classified information.

Trusted Computing Base (TCB)

The totality of protection mechanisms within a computer system including hardware, firmware, and software - the combination of which are responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system.

Trusted Network Interpretation

The specific security features, the assurance requirements and the rating structure of the Orange Book as extended to networks of computers ranging from isolated LANs to WANs.

TTY Watcher

A hacker tool that allows hackers with even a small amount of skill to hijack terminals. It has a GUI interface.

U (No Entries)

Vaccines

Program that injects itself into an executable program to perform a signature check and warns if there have been any changes.

Virus

A program that can "infect" other programs by modifying them to include a, possibly evolved, copy of itself.

Vulnerability

Hardware, firmware, or software flaw that leaves an AIS open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

Vulnerability Analysis

Systematic examination of an AIS or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

WAIS

Wide Area Information Service - An Internet service that allows you to search a large number of specially indexed databases.

WAN

Wide Area Network. A physical or logical network that provides capabilities for a number of independent devices to communicate with each other over a common transmission-interconnected topology in geographic areas larger than those served by local area networks.

War Dialer

A program that dials a given list or range of numbers and records those which answer with handshake tones, which might be entry points to computer or telecommunications systems.

Worm

Independent program that replicates from machine to machine across network connections often clogging networks and information systems as it spreads.

X (No Entries)**Y (No Entries)****Z (No Entries)**

Doodle

Thinking Space

Passwords

Quality

CardLogix Corporation is absolutely committed to providing defect free products and services to our customers in partnership with equally committed suppliers and authorized dealers.

CardLogix

Corporate Office (USA)
16 Hughes, Suite 100, Irvine, CA 92618
Ph: (949) 380-1312 • Fax: (949) 380-1428
sales@cardlogix.com • <http://www.cardlogix.com>
<http://www.smarttoolz.com>