Data Encryption

Added Material

Data Encryption

- *Encryption:* the translation of data into a secret code that cannot be read without the use of a password or secret key.
- Unencrypted data is called *plain text*
- Encrypted data is called *cipher text*
- Short sample of cipher text:
  FdgvdIC7sDv7G1Z7pCNzFLp0lgB9ACm8r5RZOBi

Why is Encryption Needed?

- Encryption is intended to prevent unauthorized individuals from accessing sensitive data
- Good encryption methods with strong keys make any "brute force" attempt to break the encryption key impossible from a practical perspective
  - It would take many years of high-speed processing to find the right key by sequentially guessing possibilities

Reasons for Encryption

- **Legal Protection**
  - **The Privacy Act of 1974 (and its Amendments)**
    - Prohibits government agencies from disclosing personally identifiable information without the subject individual's consent, with twelve specific exceptions.
  - **The Health Insurance Portability and Accountability Act (HIPAA)**
    - Requires the protection of health information and related personal identifiable information, including three required types of security safeguards.

Reasons for Encryption

- **Legal Protection**
  - **The Gramm-Leach-Bliley Act**
    - Requires financial institutions to explain their information disclosure practices to customers and to safeguard sensitive data.
  - **The Family Educational Rights and Privacy Act (FERPA)**
    - Requires protection of academic records.
  - **Maintenance of an Organization's Reputation**
    - Security breaches undermine the public's trust in an organization. This can result in loss of market share, or in extreme cases, the inability to continue operating

Reasons for Encryption

- **Industry Standards and Regulations**
  - **The PCI Standards Council**
    - Provides payment card industry compliance standards and guidelines for the protection of account information, including the PCI DSS (Data Security Standard)
  - **The American Bankers Association**
    - Provides compliance solutions, tools, training, and other resources for the banking industry.
  - **The International Organization for Standardization (ISO)**
    - Provides the ISO 27000 family of standards to help organizations keep information assets secure.

Encryption Algorithms

- ***Encryption algorithm***: A program that converts plain text into cipher text. Process:
  1. Convert all the characters in the plain text message into numbers.
  2. Use a sequence of mathematical operations to convert the plain text into cipher text
     - Scrambles the data so that it is unreadable until a reverse of the encryption steps are performed to change the cipher text back into plain text.

Encryption Keys

- To make encryption unique, at least one key is required.
- Key is simply a very large number that is used as part of the calculations performed by the algorithm.
- Most modern encryption keys are computed using two very large prime numbers
  - Makes keys more difficult to break because a prime number can be evenly divided by only two numbers – itself and the number 1.

DES Algorithm

- ***DES*** (Data Encryption Standard):
  - Original DES standard was developed in the 1970s using 56 bit keys (plus 8 parity bits for a total key size of 64 bits).
  - Published as Federal Information Processing (FIPS) standard in 1977.
  - Key size turned out to be too small and the algorithm was easily breakable, as publicly proven
  - Double DES released in 1999, which doubled the size of the key
  - Later replaced by Triple DES, which tripled the size of the key. Triple DES still used today, but waning.

RSA Algorithm

- Named using the first letters of the last names of the three people who developed it (Ron Rivest, Adi Shamir, and Leonard Adleman),
- First publicly described in 1977.
- Based a factoring technique using two large prime numbers along with an auxiliary value.
- Became the de facto standard for encrypting data transmitted over the internet.
- Pretty Good Privacy (PGP): a publicly available encryption application using RSA
  - Written in 1991 by Phil Zimmermann
  - Can use keys as large as 1024 bits

Blowfish Algorithm

- ***Blowfish:*** an algorithm intended to replace DES
  - Cipher splits messages into blocks of 64 bits and encrypts each block individually
  - Known for its speed and effectiveness
  - Many claim it has never been defeated
  - Common in e-commerce and in password management tools, where it is used to protect passwords

Twofish Algorithm

- ***Twofish*** is a successor to Blowfish
  - Developed by the same security expert, Bruce Schneier.
  - Uses a 256 bit key
  - Bundled in encryption software such as:
    - PhotoEncrypt
    - GPG (GNU Privacy Guard)
    - TrueCrypt

AES Standard

- ***AES*** (Advanced Encryption Standard) is the algorithm currently used as the standard by the U.S. Government and numerous other organizations.
  - Runs very efficiently using a 128-bit key
  - Can uses keys of 192 and 256 bits for higher security

Evolving Techniques

- ***Honey Encryption***
  - Deters hackers by returning readable fake data for every incorrect guess of the key code, in the form of an incorrect plain text password or encryption key
    - Slows hackers down by burying them with seemingly useful data
    - Makes it difficult to recognize correct data should they guess the correct key.
- ***Quantum Key Distribution***
  - Shares keys by embedding them in photons sent over a fiber optic cable network

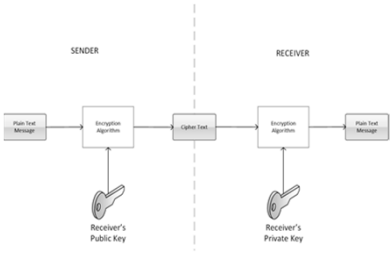
Types of Encryption

- ***Symmetric key encryption***
  - Uses a single key to encrypt plain text and to decrypt cipher text.
  - Often adequate for internal use within an organization, it is generally considered inadequate for the secure transfer of information across a public telecommunications network because both parties possess the same key.
  - The ability to decrypt proves only one thing – whoever encrypted the message had the key required to do so.
  - Triple DES, Blowfish, Twofish and AES use symmetric key encryption.

Types of Encryption

- ***Asymmetric key encryption***
  - Often called ***public-key encryption***
  - Uses a pair of keys—a ***public*** key and a ***private*** key.
    - Public key is given to anyone with which an enterprise does business
    - Private key remains confidential and internal to the enterprise
  - What the public key encrypts, the private key can decrypt, and vice versa.
  - If message encrypted with recipient's public key, only the intended recipient has the required key (their private key) for decryption

Asymmetric Key Encryption



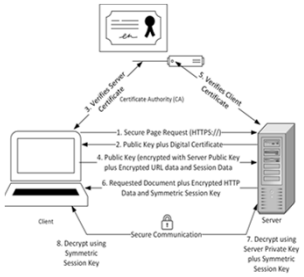
The Need for Certificates

- A single pair of keys is inadequate to fully protect data.
  - To prove message came from sender, it must also be encrypted with sender's private key
  - Receiver then decrypts once using sender's public key, and again with their private key
  - ***Certificate authority*** (CA): a third party that vouches for the authenticity of the sender by electronically signing the certificate and providing a public-private key pair for use with the certificate.
    - Certificate authorities usually charge for this service

HTTPS Security

- HTTPS: HTTP with SSL (Secure Sockets Layer)
  - Client and server use certificates and a certificate authority to authenticate each other
  - Once authenticated, they exchange a symmetric session key (within a message encrypted using public-key encryption) to be used for the remainder of the session.
  - Asymmetric key encryption is known to be slow, particularly the RSA algorithm.
    - Switching to symmetric keys improves performance, while maintaining a secure exchange of information. Here is an illustration:

Diagram: HTTPS Encryption



Encryption Guidelines

- Encryption keys should be as long as possible.
  - The longer the key, the more secure it is considered to be (within reason).
  - However, longer keys lengthen the decryption process, so there is a tradeoff.
  - Keys up to 128 bits have been routinely broken using various techniques.
  - Most experts recommend at least 256 bit keys, longer if your algorithm and time requirements allow for longer keys.
- The loss of a symmetric or private key should be treated with the same seriousness as the loss of the data that it was used to encrypt.

Encryption Guidelines

- Sensitive data should be encrypted whenever it is permanently stored
  - Security classification should be made by the business people who own the data, with the advice of legal counsel, not by the DBA
  - In general, any personal data (such as Social Security numbers and birthdates) that can be used for identity theft should be considered sensitive
  - Don't forget to encrypt backup media (tapes, CDs, DVDs, and so forth) – they are often more vulnerable to loss or theft than the primary storage devices

Encryption Guidelines

- All data not considered public knowledge should be encrypted whenever transported electronically across network connections that are not otherwise encrypted.
  - SFTP (Secure FTP) can be used if the file is not encrypted
  - It is wise to assume that the bad guys are routinely monitoring public networks.
- E-mail is not considered secure
  - Any sensitive information to be sent via e-mail should be in an encrypted attachment
  - Alternatively, some e-mail systems support encrypted and signed messages.