Protecting Information Assets
- Week 12 -

Cryptography, Public Key Encryption and Digital Signatures

MIS5206 Week 12

- Team Presentation
- Cryptography, Public Key Encryption and Digital Signatures
- Test Taking Tip
- Quiz

Reading

- Vacca Chapter 24 - 27
- “In the News” article
- Case 2 – Prepare Analysis: SECURITY BREACH AT TJX
- SANS Assignments 6, 7

Cryptography, Public Key Encryption and Digital Signatures

Cryptography allows people to carry over the confidence found in the physical world to the electronic world. It allows people to do business electronically without worries of deceit and deception. Every day hundreds of thousands of people interact electronically, whether it is through e-mail, e-commerce, ATM machines or cellular phones using Cryptography.

Cryptography Overview

- Reasons for Cryptography
- Terms
- Symmetric and Asymmetric Algorithms
- Hashing
- PKI Concepts
- Attacks on Cryptosystems

Reasons to Use Cryptography

Reason	Explanation
Confidentiality	Only authorized entities are allowed to view
Integrity	Ensures the message was not altered by unauthorized individuals
Authenticity	Sequence that controls the operation and behavior of the cryptographic algorithm
Nonrepudiation	Establishes sender identity so that the entity cannot deny having sent the message
Access Control	Access to an object requires access to the associated crypto keys in many systems (e.g. login)
Cryptosystem	The combination of algorithm, key, and key management functions used to perform cryptographic operations

Cryptography Terms

TERM	DEFINITION
Plaintext	A message in its natural format readable by an attacker
Ciphertext	Message altered to be unreadable by anyone except the intended recipients
Key	Sequence that controls the operation and behavior of the cryptographic algorithm
Keyspace	Total number of possible values of keys in a crypto algorithm
Initialization Vector	Random values used with ciphers to ensure no patterns are created during encryption
Cryptosystem	The combination of algorithm, key, and key management functions used to perform cryptographic operations

Symmetric versus Asymmetric Encryption

Symmetric

- Same key used for encryption and decryption
- Secure key distribution is a problem

Asymmetric

- Mathematically related key pairs for encryption and decryption
- Public and private keys

Cryptographic Methods

Hybrid

- Combines strengths of both methods
- Asymmetric distributes symmetric key
  - Also known as a ***session key***
- Symmetric provides bulk encryption
- Example:
  - SSL negotiates a hybrid method

Attributes of Strong Encryption

Confusion

- Change key values each round
- Performed through substitution
- Complicates plaintext/key relationship

Diffusion

- Change location of plaintext in ciphertext
- Done through transposition

Common Symmetric Algorithms

TERM	DEFINITION
DES (Data Encryption Standard)	- 64 bit key that is effectively 56 bits in strength - Algorithm is called DEA (Data Encryption Algorithm) - DES Modes • Electronic Code Book • Cipher Block Chaining (most commonly used for general purpose encryption) • Cipher Feedback • Output Feedback • Counter Mode (used in IPSec)
3DES	- 112-bit effective key length - Uses either 2 or 3 different smaller keys in one of several modes - Modes • EEE2/3 • EDE2/3
IDEA	- International Data Encryption Algorithm - Operates on 64 bit blocks in 8 rounds with 128 bit key - Considered stronger than DES and is used in PGP

Common Symmetric Algorithms

TERM	DEFINITION
AES	- NIST replaced DES in 1997 with this - Uses the Rijndael algorithm - Supports key/block sizes of 128, 192, and 256 bits - Uses 10/12/14 rounds as block size increases
Blowfish	64 bit block cipher with up to 448 bit key and 16 rounds

The Rijndael encryption algorithm was designed to replace the aging DES algorithm. Like DES, it is a block cipher. It uses 128-bit, 192-bit or 256-bit keys. This implementation encrypts 128-bit blocks. (DES used 56-bit keys and 64-bit blocks.)

Common Asymmetric Algorithms

TERM	DEFINITION
Diffie-Hellman	- First widely known public key cryptography algorithm - Computes discrete logarithms over a finite field - Provides means for secure key exchange over insecure channel
RSA	- Stands for inventors names, Rivest, Shamir, and Adleman - Relies on difficulty of finding prime factorization of large numbers
El Gamal	- Based on Diffie-Hellman method of computing discrete logarithms - Can also be used for message confidentiality and digital signature services
Elliptic Curve Cryptography	- Relies on computing discrete logarithms over elliptic curve group - Due to difficulty of problem, key sizes can be much smaller than RSA and still retain strength - Used in Mobile phone systems

What is Hashing?

A hash function is any algorithm that maps large data sets of variable length to smaller data sets of a fixed length.

The values returned by a hash function are called hash values, hash codes, hash sums, checksums or simply hashes.

Common Hashing Algorithms

MD5

- Computes 128-bit hash value
- Widely used for file integrity checking

SHA-1

- Computes 160-bit hash value
- NIST approved message digest algorithm

Birthday Attack

- Collisions
  - Two messages with the same hash value
- Based on the "birthday paradox"
- Hash algorithms should be resistant to this attack

The birthday paradox, also known as the birthday problem, states that in a random group of 23 people, there is about a 50 percent chance that two people have the same birthday.

Is the Birthday Attack Real?

- There are multiple reasons why this seems like a paradox.
- One is that when in a room with 22 other people, if a person compares his or her birthday with the birthdays of the other people it would make for only 22 comparisons—only 22 chances for people to share the same birthday.

When all 23 birthdays are compared against each other, it makes for much more than 22 comparisons. How much more? Well, the first person has 22 comparisons to make, but the second person was already compared to the first person, so there are only 21 comparisons to make. The third person then has 20 comparisons, the fourth person has 19 and so on. If you add up all possible comparisons (22 + 21 + 20 + 19 + … +1) the sum is 253 comparisons, or combinations. Consequently, each group of 23 people involves 253 comparisons, or 253 chances for matching birthdays.

Message Authentication Codes

- Small block of data generated with a secret key and appended to a message
- HMAC (RFC 2104)
  - Uses hash instead of cipher for speed
  - Used in SSL/TLS and IPSec

Digital Signatures

- Hash of message encrypted with private key
- Digital Signature Standard (DSS)
  - DSA/RSA/ECD-SA plus SHA
- DSS provides
  - Sender authentication
  - Verification of message integrity
  - Nonrepudiation

Encryption Management

- Key Distribution Center (KDC)
  - Uses master keys to issue session keys
  - Example: Kerberos
- ANSI X9.17
  - Used by financial institutions
  - Hierarchical set of keys
  - Higher levels used to distribute lower

ANSI X9.17-1985, Financial Institution Key Management (Wholesale), is a voluntary standard that utilizes the Data Encryption Standard (DES) to provide key management solutions for a variety of operational environments.

Public Key Infrastructure

- All components needed to enable secure communication
  - Policies and Procedures
  - Keys and Algorithms
  - Software and Data Formats
- Assures identity to users
- Provides key management features

PKI Components

Digital Certificates

- Contains identity and verification info

Certificate Authorities

- Trusted entity that issues certificates

Registration Authorities

- Verifies identity for certificate requests

Certificate Revocation List (CRL)

PKI Cross Certification

- Process to establish a trust relationship between CAs
- Allows each CA to validate certificates issued by the other CA
- Used in large organizations or business partnerships

Cryptanalysis

- The study of methods to break cryptosystems
- Often targeted at obtaining a key
- Attacks may be passive or active

Although the actual word "cryptanalysis" is relatively recent (it was coined by William Friedman in 1920), methods for breaking codes and ciphers are much older. The first known recorded explanation of cryptanalysis was given by 9th-century Arabian polymath, Al-Kindi (also known as "Alkindus" in Europe), in A Manuscript on Deciphering Cryptographic Messages. This treatise includes a description of the method of frequency analysis

Cryptanalysis

- Kerckhoff's Principle
  - The only secrecy involved with a cryptosystem should be the key
- Cryptosystem Strength
  - How hard is it to determine the secret associated with the system?

Cryptanalysis Attacks

- Brute force
  - Trying all key values in the keyspace
- Frequency Analysis
  - Guess values based on frequency of occurrence
- Dictionary Attack
  - Find plaintext based on common words

Cryptanalysis Attacks

- Replay Attack
  - Repeating previous known values
- Factoring Attacks
  - Find keys through prime factorization
- Known Plaintext
  - Format or content of plaintext available

Cryptanalysis Attacks

- Chosen Plaintext
  - Attack can encrypt chosen plaintext
- Chosen Ciphertext
  - Decrypt known ciphertext to discover key
- Differential Power Analysis
  - Side Channel Attack
  - Identify algorithm and key length

Cryptanalysis Attacks

- Social Engineering
  - Humans are the weakest link
- RNG Attack
  - Predict IV used by an algorithm
- Temporary Files
  - May contain plaintext

Early versions of Netscape's Secure Socket Layer (SSL) encryption protocol used pseudo-random quantities derived from a PRNG seeded with three variable values: the time of day, the process ID, and the parent process ID. These quantities are often relatively predictable, and so have little entropy and are less than random, and so that version of SSL was found to be insecure as a result.

Practical Cryptanalysis

- DES Cracker:
  - A DES key search machine
  - contains 1536 chips
  - Cost: $250,000.
  - could search 88 billion keys per second
  - won RSA Laboratory's "**DES Challenge II-2**" by successfully finding a DES key in 56 hours.

E-mail Security Protocols

- Privacy Enhanced Email (PEM)
- Pretty Good Privacy (PGP)
  - Based on a distributed trust model
  - Each user generates a key pair
- S/MIME
  - Requires public key infrastructure
  - Supported by most e-mail clients

Network Security

Link Encryption

- Encrypt traffic headers + data
- Transparent to users

End-to-End Encryption

- Encrypts application layer data only
- Network devices need not be aware

Network Security

SSL/TLS

- Supports mutual authentication
- Secures a number of popular network services

IPSec

- Security extensions for TCP/IP protocols
- Supports encryption and authentication
- Used for VPNs

Test Taking Tip

When one of the answer choices is “all of the above” and at least two statements are unquestionably true then choose “all of the above.”

- If 2 answers are true, then the additional effort required to certify the answer is not the best use of your time
- Moving quickly through questions you can easily answer saves time for questions that require additional scrutiny

Quiz