COMP 424

Computer Security
Lecture 09 & 10

Protocol

- An orderly sequence of steps agreed upon by two or more parties in order to accomplish a task
- Characteristics of a good protocol
  - Established in advance
  - All parties agree on it
  - Easy to understand
  - Complete: covers all that needs to be covered.
  - Secure: Does not permit actions that should not be allowed.

Key Management Protocols

- Key Exchange
- Done with or without a neutral third party
- Key distribution
  - Uses a centralized key distributor (Veri$ign)
- Key Escrow
  - Trusted agency holds copies of keys

Diffie-Hellman

- (does not require a third party

  1) A and B exchange two numbers p and g.

  2)Each chooses a 512-bit number, $s1$ and $s2$, and keeps it secret

  3)Each raises g to its secret number mod p. (g^{s1} mod p)

  4)They exchange these values and raise them to their secret numbers $(g^{s1} \bmod p)^{s2}$.

  5)They now have the same secret key with only one exchange.

Bucket brigade attack

- In intruder X can cause problems
  - A sends g^{KA} mod p to B, but it is intercepted by X who sends g^{KX} mod p to B.
  - B sends g^{KB} mod p to A, but it is intercepted by X who sends g^{KX} mod p to A.
  - X now shares a secret key with both A and B who are unaware of X
  - X now intercepts messages between A and B before passing them on (or not, or modifying them...)

Authentication with Digital Signatures

- A and B can use digital signatures to expose X.
  - A produces a hash, or fingerprint, of the message and encrypts it with A's private key.
  - B decrypts it with A's public key and can recompute the same hash on the message.
  - If it decrypts and has the same hash then
    - It must have been written by A
    - It could not have been changed since being written.

Properties of digital signatures

- Properties of Digital Signatures
  - Unforgeable
  - Authentic
  - Can't be modified once sent
  - Not reusable
  - Prevent repudiation

Key Distribution Protocols

- Key Distribution Center
- “Session” keys or long-term secret keys
- Session keys are for one session use only.
- Can use secret key (DH) or public key (RSA) protocols
- Can use authentication
- Kerberos

Key Escrow

- Encryption keys are *escrowed* to trustworthy agencies
- Requirements for a key escrow protocol
  - Encrypting source must be identified
  - The key is not identified
  - Key retrievable under ***k* of *n* protocol**

Clipper Encryption Protocol

- Strong public backlash
  - Loss of privacy from potential government intrusion
  - Unreleased algorithm
  - For Clipper $k = n = 2$
  - Skipjack algorithm uses an 80-bit key so is considered safe for at least 36 years.

Elections

- Necessary to have untraceable (anonymous), but legitimate communications
- Requirement for elections systems
  - Only authorized users
  - Each user can only vote once
  - Votes are private and secret
- Protocol uses public key encryption system