1.264 Lecture 27

Security protocols
Symmetric cryptography

Next class: Anderson chapter 10. Exercise due <u>after</u> class

Exercise: hotel keys

- What is the protocol?
- What attacks are possible?
  - Copy
  - Cut and paste
  - Replay
- What is the effect of encryption?

Solution: hotel keys

- **Protocol:**
  - C (card) -> D (door) : N1, N2, *N3, N4*, T
    - where N1 is the current code
    - N2, *N3 and N4* are previous codes *(if they can fit)* and
    - T is the number of days the room is reserved
  - If N2 is correct, N1 is written to door unit, door opens
  - If N1 is correct and days<T, door opens
- **Attacks:**
  - Copied card can be used. No protection in this protocol.
  - Attacker can change value of T. Works unless another guest is given the room.
  - Replay is possible. Attacker can intercept card-door interaction, write it to new card, and enter room. Mag stripe readers emit radiation.
  - Encryption doesn't prevent copy or replay; it makes cut and paste harder
- **Unexpected problem: unused rooms/keys**

Basic key management example

- **Alice and Bob wish to communicate**
  - Sam is a trusted third party (shares keys with Alice and Bob)
  - A key is a secret number that both encrypts and decrypts
- **Alice calls Sam, asks for key to talk with Bob**
  - A -> S: A, B (A and B are principals or names)
- **Sam sends Alice pair of certificates (ciphertexts)**
  - Each contains copy of key
    - First is encrypted so only Alice can read it: K_{AS}
    - Second is encrypted so only Bob can read it: K_{BS}
  - S -> A: $\{A, B, K_{AB}, T\}_{K_{AS}}$, $\{A, B, K_{AB}, T\}_{K_{BS}}$ (T is time)
- **Alice retrieves her key, sends Bob the second certificate**
  - She then sends him a message that he can decrypt
  - A -> B: $\{A, B, K_{AB}, T\}_{K_{BS}}$, $\{M\}_{K_{AB}}$

(Can be replayed; no freshness)

Kerberos

- **Two kinds of trusted servers:**
  - **Authentication server to which users log on**
  - **Ticket-granting server, which gives access to files and programs (authorization)**
    - **This is more scalable than a single server**
  - **Alice asks ticket server for access to Bob**
    - **A -> S: A, B**
  - **Server sends ticket, encrypted with A’s password (key), granting access to B at time T for lifetime L of ticket**
    - **S -> A: $\{T_S, L, K_{AB}, B, \{T_S, L, K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$**
  - **Alice sends timestamp to resource B, which confirms it’s alive**
    - **A -> B: $\{T_S, L, K_{AB}, A\}_{K_{BS}}, \{A, T_A\}_{K_{AB}}$**
  - **Bob sends timestamp incremented by one**
    - **B -> A: $\{T_A+1\}_{K_{AB}}$**

Kerberos, cont

- This avoids replay attacks and compromised keys by using timestamps
  - Compromised keys are a problem only for their lifetime L, typically measured in hours
  - However, clocks must now be synchronized
- Kerberos is used for Microsoft security and many single login systems
  - Why don’t we use Kerberos for Internet and Web security?
  - Kerberos requires a central key server trusted by all parties
    - If it is broken, all communications are exposed
    - If it is down, no one can initiate secure connections
    - Who would such a trusted party be on the Internet?
    - It would be expensive
  - We use a different protocol, SSL (next lectures)

Passwords as a protocol: issues

- The simplest security protocol is a username and password
  - Often the most vulnerable piece of security
  - Often used to protect other security measures
    - Your browser SSL certificate is protected by a password
    - Kerberos/Microsoft security key is your password
- User issues
  - Social engineering
    - Users disclose passwords to third parties
      - By accident, on purpose, or through deception
      - Deception common in health care, insurance, banking
  - Reliable password entry
    - Users mistype passwords; password resets
  - Remembering passwords
    - Users write down passwords, choose weak passwords

Passwords: solutions

- There are 26 letters, 10 digits: 36 possible characters at each location in a password
  - This should be about 5 bits ($2^5 = 32$ combinations)
  - Because of patterns, it's usually only 1.5-2 bits/char
- An 8 character password is less than a 16 bit key
  - Easily broken (see the book for many attacks)
- Solutions
  - Passphrases
  - Hardware password generators
  - Biometrics (which can also be attacked)

Cryptographic primitives

- Symmetric key encryption
  - Used to encrypt sessions
- Asymmetric (public) key encryption
  - Used to distribute symmetric keys
  - Basis for digital signatures
- Stream or block ciphers
  - Used to apply key to message
- Message digests (hashes)
  - Used to verify message integrity
- Digital signatures (certificates)
  - Used to verify identity of principals
  - Covered as part of Secure Sockets Layer (SSL)

Cryptography issues

- Cryptography protects against eavesdropping, tampering (cut and paste)
- It does not protect against replay (need freshness for that) or necessarily against man-in-the-middle attacks
- Nothing protects against denial of service attacks except shutting down the attacker

Managing network risks: Cryptography

- Definitions
  - Plaintext: original message
  - Ciphertext: encrypted message
  - Cryptographic algorithm: function converting plaintext to ciphertext
  - Key: number used by algorithm to encrypt and/or decrypt
    - Not the same as a database key (primary or foreign!)
- Encryption process

  - Symmetric: sender and receiver use same secret key
  - Asymmetric: sender and receiver use different, but related keys. Receiver key public, used by all senders to that receiver

Symmetric encryption

- Symmetric algorithms use same key to encrypt and decrypt
  - DES (Data Encryption Standard): 56 bit key
    - Splits data into pieces, reshuffles
    - Cracked in 1998 after 30 years of use: faster hardware
  - Triple DES: encrypt/decrypt/encrypt with 3 DES keys: 168 bit effective key length
    - Backward compatible with DES in banking, etc.
  - RC2, RC4, RC5: 40-2048 bit keys, in common use by encrypting Web servers and browsers
  - AES: Current US government standard, uses Rijndael algorithm
- Problems with symmetric keys
  - Must be exchanged in advance, via secure method
  - Multi-way communication not supported effectively:
    - If many users must communicate with server, compromising any one can compromise all

Exercise (very simplified from real thing!)

- Plaintext: 73628495
- Key: 31
  - k1= 3, k2= 1
- Sender algorithm:
  - Shift digits by k1 to the left. (Wrap around as needed.)
  - Subtract k2 from each digit
- Ciphertext: _______________
- Receiver algorithm:
  - Add k2 to each digit
  - Shift digits by k1 to the right. (Wrap around as needed.)
- Plaintext: ________________

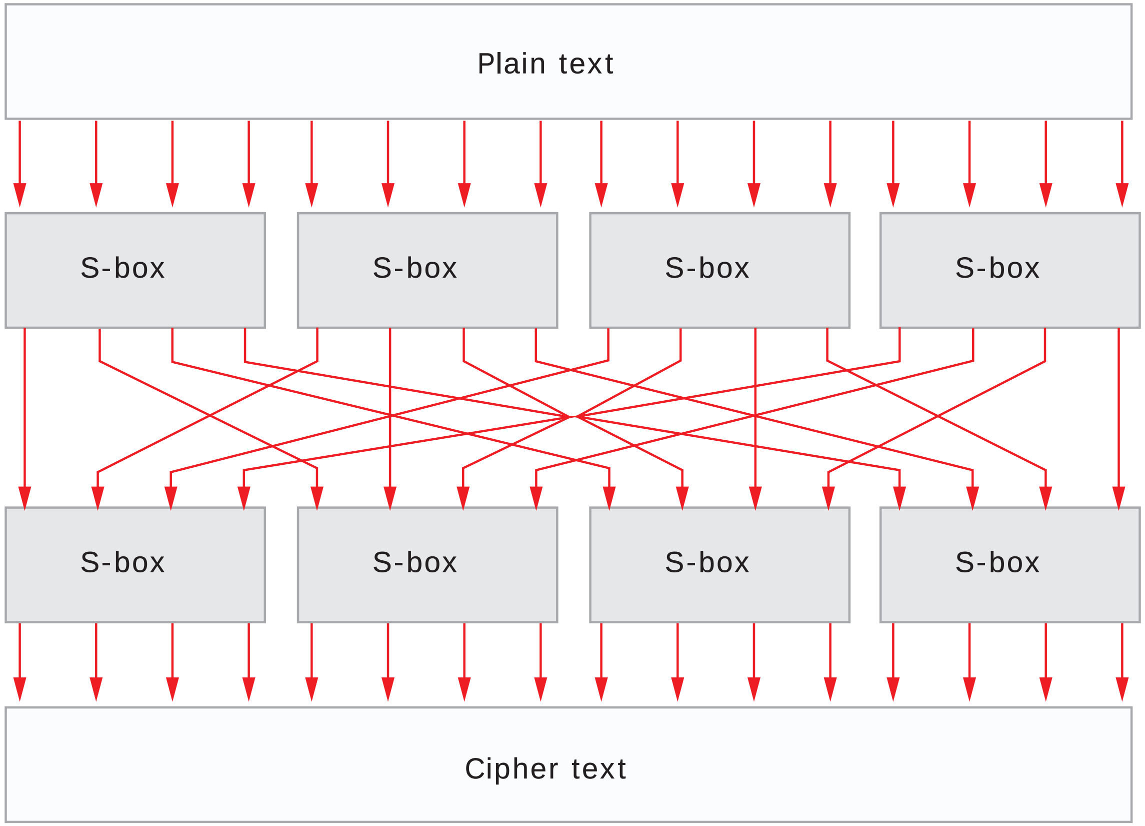
(Real symmetric algorithms chop, shift, add/subtract in complex patterns to remove statistical patterns in data—see text: S-boxes)

Solution

- Plaintext: 73628495
- Key: 31
  - k1= 3, k2= 1
- Sender algorithm:
  - Shift digits by k1 to the left
  - Subtract k2 from each digit
- Ciphertext: 28495736 -> 17384625
- Receiver algorithm:
  - Add k2 to each digit
  - Shift digits by k1 to the right
- Plaintext: 62517384 -> 73628495

(Real symmetric algorithms chop, shift, add/subtract in complex patterns to remove statistical patterns in data---see text: S-boxes)

S Boxes



An example of a 16-bit SP-network (substitution-permutation network) block cipher.

Image by MIT OpenCourseWare.

Also see AES Wiki entry

MIT OpenCourseWare
http://ocw.mit.edu

1.264J / ESD.264J Database, Internet, and Systems Integration Technologies
Fall 2013

For information about citing these materials or our Terms of Use, visit: http://ocw.mit.edu/terms.