Networked System Security

Cryptography, Key Exchange and Jamming

ROYAL INSTITUTE OF TECHNOLOGY

Module TAs: **Thanassis Giannetsos**, athgia@kth.se
Kewei Zhang, kewei@kth.se

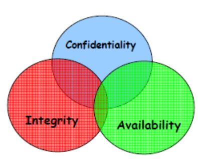
Panos Papadimitratos
http://www.ee.kth.se/nss

Outline

- Recap
  - Cryptography basics (Definitions, Security Services, etc.)
  - Hash functions, Data Integrity methods (MACs)
- Symmetric Encryption
  - Block Ciphers vs. Stream Ciphers
  - Design principles, DES, AES, Modes of operations
- Public key Cryptography
  - Diffie-Helman, RSA, El Gamal
  - Certificates
- Key Exchange
  - Symmetric vs. Asymmetric Key Exchange and Authentication
- Jamming
  - Physical Layer Security

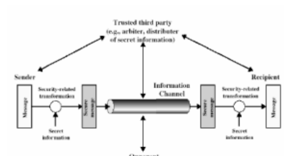
Security Goals (not only…)

- Derived requirements, e.g.,
  - Authentication: Who is who?
  - Access Control: Only selective access is authorized



- Security Services
  - Confidentiality – protection from passive attacks (eavesdropping)
    - Encryption
  - Authentication – you are who you say you are
  - Integrity – received as sent, no modifications, insertions, shuffling or replays
    - Message Authentication Code (MAC)
  - Non-repudiation – can't deny a message was sent or received
    - Digital Signatures
  - Access Control – ability to limit and control access to host systems and apps
  - Availability – attacks affecting loss or reduction on availability

Model for Network Security



- Models information flowing over an insecure communications channel, in the presence of possible opponents
  - An appropriate security transform (encryption algorithm) can be used, with suitable keys, possible negotiated using the presence of a trusted third party

Model for Network Security

- What is needed
  - Design a suitable algorithm for the security transformation
  - Generate the secret information (keys) used by the algorithm
  - Develop methods to distribute and share the secret key information
  - Specify a protocol enabling the principals to use the transformation and secret information for a security service
- Cryptosystem: An Encryption/Decryption algorithm plus the description of the format of messages and keys. Consists of:
  - Plaintext and Ciphertext message spaces
  - Set of possible encryption/decryption keys
  - An efficient key generation algorithm
  - Efficient encryption/decryption algorithms
- Can be categorized as symmetric key and public key (asymmetric)

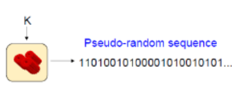
Symmetric Encryption

- Also known as private-key
- Sender and recipient share a common key
- All classical encryption algorithms are private-key
- $c = E_K(m)$ and $m = D_K(c)$
- Both E and D should be public
  - Secrecy of *m* given *c* depends totally on the secrecy of *k*.

- Stream and Block ciphers
  - Stream ciphers process messages a bit or byte at a time
  - Block ciphers work on a block at a time, each of which is then encrypted/decrypted

Stream vs. Block ciphers

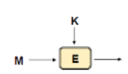
- Stream ciphers - properties
  - Replace the random key in one time pad by a pseudo-random sequence, generated by a cryptographic pseudo-random generator that is 'seeded' with the key
  - Short key, but only practical security
  - Statistically random, long period with no repetitions
  - Depends on large enough keys (must defend against brute force attacks)
  - Encryption in small quantities
  - No error propagation + Very fast
  - Reused Key Attack + Bit Flipping Attack



- Block ciphers
  - Typically blocks have length 64 or 128 bits.
  - They have a substitution-permutation network structure
  - Large chunks of data + "carry over" from previous blocks
- Many current ciphers are block ciphers, hence our focus

What is a block cipher?

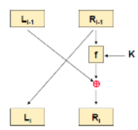
- Function E: $\{0,1\}^k \times \{0,1\}^L \rightarrow \{0,1\}^L$ that takes two inputs, a *k*-bit key K and an *L*-bit plaintext M, to return n *L*-bit encryption C = E(K, M)



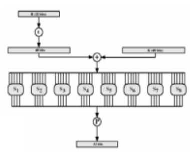
- A block cipher is a permutation on *l*-bit strings, which means that there exists an inverse function by E_K^{-1} or D.
- Hence $E_K^{-1}(E_K(M)) = M$ and $E_K(E_K^{-1}(C)) = C$
- The block cipher is a public and fully specified algorithm
- Security lies on the secrecy of the key, so the key recovery by an adversary should be a difficult problem

Block Cipher Principles

- Most symmetric block ciphers are based on a Feistel Cipher Structure
- Partitions input block into two halves. Then process through multiple rounds which
  - Perform a substitution on left data half based on round function of right half & sub key
  - Then have permutation swapping halves

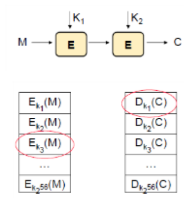


- Data Encryption Standard (DES)
  - Has a key length of k = 56 bits block length L = 64 bits
  - 56-bit keys have $2^{56} = 7.2 \times 10^{16}$ values (exhaustive search concerns)
  - $L_i = R_{i-1}$
    $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$



Double DES, Triple DES, AES

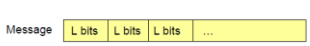
- Multiple encryptions with DES and multiple keys
  - 2- DES – $M \rightarrow E(K_1, M) \rightarrow E(K_2, E(K_1, M)) = C$
  - Not safe due to a Meet-in-the middle attack
    - Encrypt M using all 2^{56} possible keys ($M \rightarrow E(K_1, M)$)
    - Then, decrypt C using 2^{56} possible keys ($D(K_2, C) = D(K_2, E(K_2, E(K_1, M))) \rightarrow E(K_1, M)$)
    - Check for a match



- 3-DES with 3 different keys
  - $E(K3, D(K2, E(K1, M)))$
  - Decryption (?)
  - Cost of exhaustive search is of the order 2^{112}
- AES
  - Block cipher: 128-bit blocks, 128/192/256-bit keys
  - Strength 3-DES, efficiency much higher

Modes of Operation

- Block ciphers for a basic building block, which encrypt a fixed sized block of data (of length L)
  - Typically the block size is 64 or 128 bits
  - To use these in practise, we need to handle arbitrary amounts of data
  - To do that we use a block cipher in some mode of operation



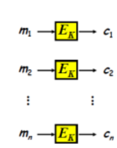
- Description of 2 of them that exhibit different kind of features
  - Electronic Code-Book (ECB)
  - Cipher Block Chaining (CBC)
  - CTR
  - In all cases the input string is a multiple of block length. If not padding is used (padding, however, introduces security risks)

Electronic Codebook Book (ECB)

- The message is broken into blocks which are encoded independently of the other blocks
- Deterministic mode
  - Repetitions in message may show in ciphertext
  - Blocks can be shuffled/ inserted without affecting the en/decryption of each block

```
Encrypt (<m1,m2,…,mn>)
for i=1 to n do
   ci = EK(mi)
return (<c1,c2,…,cn>)

Decrypt (<c1,c2,…,cn>)
for i=1 to n do
   mi = EK-1(ci)
return (<m1,m2,…,mn>)
```



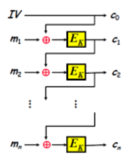
- Main use is when only a single block of info needs to be sent (e.g., a session key encrypted using a master key)

Cipher Block Chaining (CBC)

- Message is broken into blocks but these are linked together in the encryption operation
  - Each previous cipher block is chained with current plaintext block
  - *Attempts to make the ciphertext depend on all blocks before it*
- Random Initial Vector (IV) to start the process
- CBC mode is applicable whenever large amounts of data needs to be sent securely, provided that it's available in advance (e.g., mail, FTP, web, etc.)

```
Encrypt (<m_1,m_2,...,m_n>)
Let IV =_R {0,1}^L
for i=1 to n do
    c_i = E_K(m_i ⊕ c_{i-1})
return (<IV,c_1,c_2,...,c_n>)

Decrypt (<c_0,c_1,c_2,...,c_n>)
for i=1 to n do
    m_i = E_K^-1(c_i) ⊕ c_{i-1}
return (<m_1,m_2,...,m_n>)
```



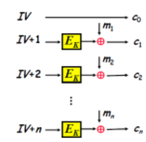
- Advantages – Disadvantages?

Counter (CTR)

- Counter mode uses an auxiliary value (IV) which is an integer in the range $0 \ldots 2^L$-1
  - In the following addition is done modulo 2^L
- Efficiency
  - Parallel encryptions
- Provides random access to encrypted data blocks
- Provable security
  - Must ensure never reuse key/ counter values, otherwise could break

```
Encrypt (<m_1,m_2,...,m_n>)
Let IV =_R {0,1}^L
for i=1 to n do
    c_i = E_K(IV+i)⊕ m_i
return (<IV,c_1,c_2,...,c_n>)

Decrypt (<c_0,c_1,c_2,...,c_n>)
for i=1 to n do
    m_i = E_K(IV+i)⊕ c_i
return (<m_1,m_2,...,m_n>)
```



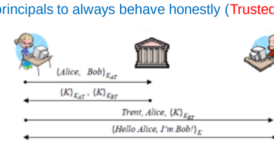
- Uses: high-speed network encryptions

Key Exchange and Authentication

- So for all cryptosystems discussed, we assumed the existence of a symmetric private key
  - All classical, and modern block and stream ciphers are of this form
  - *If the key is disclosed communications are compromised*
- How to achieve key establishment between entities?
  - Process by which two parties agree on a secret key as a means for building a secure communication channel between them
  - Generally, is a sub-task of entity authentication protocols for bootstrapping higher secure communications
  - Also form important protocol messages which should be the subject for data-origin authentication
- Classical vs. Public key exchange and authentication

Authentication Servers

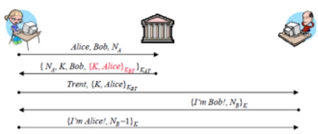
- If two users that have never met before wish to communicate securely, they can do so through an authentication server (AS)
  - An AS is like a name registration authority, who maintains a database with the principals it serves
  - Can deliver information computed from a key shared with each principal
  - Trusted by principals to always behave honestly (Trusted Third Party – call it Trent)



- Simple protocol for authenticated key establishment
  - Possible attacks? (check 1st and 2nd message)
  - Nothing guarantees the freshness of messages

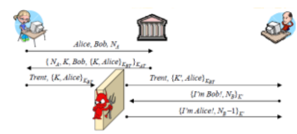
Challenge-Response Authentication

- There are many methods to ensure that a message is not a replay of an old message. One well known is called challenge-response authentication (or handshake)
  - One party sends a challenge message
  - Second party sends a response in a pre-agreed manner that indicates freshness
    - Use of time constraint; if the response doesn't arrive on time, authentication fails
  - Nonces (Random "numbers used once"), Timestamps, Sequence numbers
- Needham-Schroeder[1978]
- Possible attacks?
  - Denning and Sacco (1981)
  - Focus on messages 3, 4 and 5



Needham-Schroeder

- There are many methods to ensure that a message is not a replay of an old message. One well known is called challenge-response authentication (or handshake)
  - Eve blocks Alice's 3rd message and injects her own which is a replay of an old run
  - Had all the time to break the old session key, she manages to fool Bob
  - Failed to provide liveness of Trent…



- Fix with timestamps
  - Tight synchronization is required

1. Alice → Trent : Alice, Bob
2. Trent → Alice : $\{ T, K, Bob, \{ T, K, Alice \}_{KBT} \}_{KAT}$
3. Alice → Bob : $\{ T, K, Alice \}_{KBT}$
4. } Same as in the Needham-Schroeder protocol
5. }

Otway-Rees

- Otway-Rees avoided the synchronization limitation by not using timestamps but a session identifier
  - Attack?

1. $A \rightarrow B : M, A, B, \{N_A, M, A, B\}_{K_{AS}}$
2. $B \rightarrow T : M, A, B, \{N_A, M, A, B\}_{K_{AS}}, \{N_B, M, A, B\}_{K_{BS}}$
3. $T \rightarrow B : M, \{N_A, K_{AB}\}_{K_{AS}}, \{N_B, K_{AB}\}_{K_{BS}}$
4. $B \rightarrow A : M, \{N_A, K_{AB}\}_{K_{AS}}$

- Kerberos solution
- In general
  - Message freshness and principal's liveness
    - Instead of nonces, better to use MACs or a signature scheme – Data Integrity
  - Mutual authentication

Public key Cryptographic Key Exchange and Authentication

- Recap certificates
  - Every user submits their public key to the CA. The CA concatenates
    - User name, User public key (encryption or verification), Name of the CA, Expiration date, Serial Number of Certificate,…
    - And generates a signature (of the CA) on this data string
- The combination of the data and signature is the public key certificate. This is sent back to the user
  - Anyone with the CA's public key can verify the users public key certificate, and so obtain a trusted copy of the users public key
  - Certificates can be stored in repositories and retrieved as needed
  - Since they are digitally signed, there's no need to be secured
- Diffie-Helman, RSA, El Gamal

Jamming

Security in Wireless Systems

Inherent openness in wireless communications channel: Common attacks at the physical layer

- Eavesdropping
  - Needs more powerful solutions compared to wire-line
  - But at least, there are some **conventional techniques**

- Jamming attacks (Denial-of-service)
  - Error correcting codes (at a higher layer)
  - Physical layer solutions
    - Coding theory and information theory based approaches
    - Beam-forming (signal processing based approaches)
    - Spread spectrum techniques

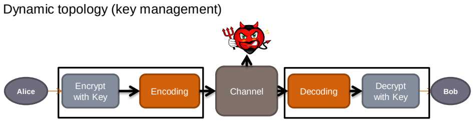
Eavesdropping (confidentiality) Wireless networks

Cryptography

- At higher layers of the protocol stack
- Based on the assumption of <u>limited computational power</u> at Eve
- Vulnerable to large-scale implementation of quantum computers

Wireless networks

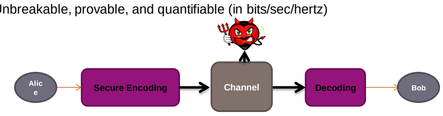
- Open nature → intercept the transmission of secret keys
- Lack of infrastructure (key distribution)
- Dynamic topology (key management)



Physical layer solutions Confidentiality

Information-theoretic security

- Idea: use the inherent randomness of medium (the difference between the channels)
- Eliminate the key management issues: lower complexity and resources
- No assumption on Eve's computational power
- No assumption on Eve's available information
- Unbreakable, provable, and quantifiable (in bits/sec/hertz)



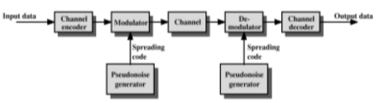
Anti-jamming solutions
Physical layer approaches

Coding theory and information theory based approaches

Beam-forming (signal processing based approaches) or cooperative jamming

Spread spectrum techniques

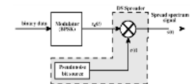
- At the physical layer
- Based on the assumption of limited knowledge at Eve
- Code Division Multiple Access (CDMA)



Spread spectrum techniques

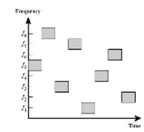
Direct Sequence (DS)

- The modulated signal is multiplied by a spreading code

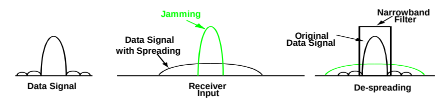


Frequency Hopping (FH)

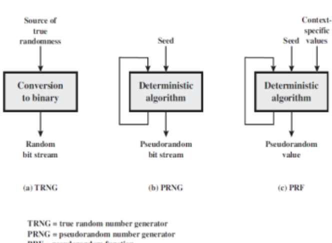
- Signal hops from frequency to frequency at fixed intervals
- The frequency sequence is dictated by the spreading code



Time Hopping (TH)



Random number generation

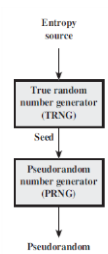


Must be sent to receiver: securely

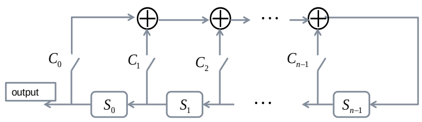
Pseudorandom Number (PN) sequences

Deterministic (non-random) sequence

- Looks random: in some well-defined statistical sense
  - Uniform distribution of bits
  - Independence: No one subsequence in the sequence can be inferred from the others
  - Some statistical tests



Linear Feedback Shift Registers (LFSRs)



Characteristic polynomial $f(x)=1+C_1x+\ldots+C_{n-1}x^{n-1}+x^n=\sum_{i=0}^{n}C_ix^i$

- $C_i \in \{0,1\}$

M-sequence (Maximal length sequence)

- Period= $2^n - 1$ (cycle)

An exercise

Jamming in Frequency Hopping Spread Spectrum

A transmitter-receiver pair wishes to communicate *k* messages (pieces of data)

- Number of successful transmission = *k*
- Transmission time for each message = *T*
- Number of available channels = *C*
- Use one channel to transmit each message and then (after *T* ms) hop uniformly to another one
- Jammer can prevent communication across C_{jam} channels
- Number of transmitted messages (maybe jammed) = *n*

Notes

- Recall Binomial distribution