Security Sensor Network

Biswajit panja
Topics

- Security Issues in Wired Network
- Security Issues in Wireless Network
- Security Issues in Sensor Network
Security Issues in Wired Network
Security Attacks

(a) Normal flow

(b) Interruption

(c) Interception

(d) Modification

(e) Fabrication

Figure 1.1 Security Threats
An encryption scheme has five ingredients:

- Plaintext
- Encryption algorithm
- Secret Key
- Ciphertext
- Decryption algorithm

Security depends on the secrecy of the key, not the secrecy of the algorithm.
Conventional Encryption Principles

Figure 2.1 Simplified Model of Conventional Encryption

Source: Network Security Essentials, William Stallings
### Average time required for exhaustive key search

<table>
<thead>
<tr>
<th>Key Size (bits)</th>
<th>Number of Alternative Keys</th>
<th>Time required at $10^6$ Decryption/µs</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>$2^{32} = 4.3 \times 10^9$</td>
<td>2.15 milliseconds</td>
</tr>
<tr>
<td>56</td>
<td>$2^{56} = 7.2 \times 10^{16}$</td>
<td>10 hours</td>
</tr>
<tr>
<td>128</td>
<td>$2^{128} = 3.4 \times 10^{38}$</td>
<td>$5.4 \times 10^{18}$ years</td>
</tr>
<tr>
<td>168</td>
<td>$2^{168} = 3.7 \times 10^{50}$</td>
<td>$5.9 \times 10^{30}$ years</td>
</tr>
</tbody>
</table>
Symmetric Block Ciphers

- DEA
- TDEA
- International Data Encryption
- Blowfish
Figure 2.9  Encryption Across a Packet-Switching Network

- = end-to-end encryption device
- = link encryption device
PSN = packet switching node
Key Distribution

1. A key could be selected by A and physically delivered to B.
2. A third party could select the key and physically deliver it to A and B.
3. If A and B have previously used a key, one party could transmit the new key to the other, encrypted using the old key.
4. If A and B each have an encrypted connection to a third party C, C could deliver a key on the encrypted links to A and B.

- **Session key:**
  - Data encrypted with a one-time session key. At the conclusion of the session the key is destroyed

- **Permanent key:**
  - Used between entities for the purpose of distributing session keys

Source: Network Security Essentials, William Stallings
1. Host sends packet requesting connection
2. Front end buffers packet; asks KDC for session key
3. KDC distributes session key to both front ends
4. Buffered packet transmitted

FEP = front end processor
KDC = key distribution center

Figure 2.10 Automatic Key Distribution for Connection-Oriented Protocol
Encryption using Public-Key system

Source: Network Security Essentials, William Stallings
Authentication using Public-Key System

Source: Network Security Essentials, William Stallings
Applications for Public-Key Cryptosystems

- Three categories:
  - **Encryption/decryption**: The sender encrypts a message with the recipient’s public key.
  - **Digital signature**: The sender ”signs” a message with its private key.
  - **Key exchange**: Two sides cooperate to exchange a session key.
The RSA Algorithm – Key Generation

1. Select \( p, q \) \( p \) and \( q \) both prime
2. Calculate \( n = p \times q \)
3. Calculate \( \Phi(n) = (p - 1)(q - 1) \)
4. Select integer \( e \) \( \gcd(\Phi(n), e) = 1; 1 < e < \Phi(n) \)
5. Calculate \( d \) \( d = e^{-1} \mod \Phi(n) \)
6. Public Key \( K_U = \{e, n\} \)
7. Private key \( K_R = \{d, n\} \)
Diffie-Hellman Key Exchange

**User A**

- Generate random $X_A < q$;
- Calculate $Y_A = \alpha^{X_A} \mod q$
- Calculate $K = (Y_B)^{X_A} \mod q$

**User B**

- Generate random $X_B < q$;
- Calculate $Y_B = \alpha^{X_B} \mod q$;
- Calculate $K = (Y_A)^{X_B} \mod q$
Key Management

Public-Key Certificate Use

Unsigned certificate:
contains user ID,
user's public key

Generate hash code of unsigned certificate

H

Encrypt hash code with CA's private key to form signature

E

Signed certificate:
Recipient can verify signature using CA's public key.

Source: Network Security Essentials, William Stallings
Authentication Applications: Kerberos

1. User logs on to workstation and requests service on host.

2. AS verifies user’s access right in database, creates ticket-granting ticket and session key. Results are encrypted using key derived from user’s password.

3. Workstation prompts user for password and uses password to decrypt incoming message, then sends ticket and authenticator that contains user’s name, network address, and time to TGS.

4. TGS decrypts ticket and authenticator, verifies request, then creates ticket for requested server.

5. Workstation sends ticket and authenticator to server.

6. Server verifies that ticket and authenticator match, then grants access to service. If mutual authentication is required, server returns an authenticator.

Source: Network Security Essentials, William Stallings
IP Security Scenario

Source: Network Security Essentials, William Stallings
End-to-end versus End-to-Intermediate Authentication

Source: Network Security Essentials, William Stallings
Figure 8.3  Example Distributed Network Management Configuration
Distributed Intrusion Detection

Source: Network Security Essentials, William Stallings
Distributed Intrusion Detection

Figure 9.6 Agent Architecture
Security Issues in Wireless Network
Attacks

- Attacks could range from deleting messages, injecting erroneous messages, impersonate a node.
- Poor physical protection
- Attacks not only from outside but also from within the network from compromised nodes
Key Management and Routing

- A single key management service for an Ad-hoc network is not a good idea
  - CA may be down/unavailable
  - CA compromises
- Secure routing is an issue with dynamically changing network.
- False routing information generated by compromised nodes
Used key agreement

- Certificate based key agreement
- Public key certificates can allow participants to verify the binding between the IP address and keys of other participants.
- Disadvantage
  - Difficult to determine if the certificate presented by the participant has been revoked
Password based Authenticated Key Exchange

- Password is chosen and shared among the nodes
- Desirable properties: - Secrecy, Perfect Forward Secrecy, Contributory key agreement, Tolerance to disruption attempts
- Protocol: - Diffie-Hellman
Problems associated with Ad-hoc Routing

- Frequent changes in network topology
- Problems associated with wireless communication
- Trust relationship between neighbors
- Throughput
- Attacks using modification of protocol fields of messages
Some Approaches

- Using pre-deployed security infrastructure
- Using independent Security Agents (SA)
- Installing extra facilities in the network to mitigate routing misbehavior
Security Issues in Sensor Network
Requirements

- Confidentiality
- Authenticity
- Integrity
- Freshness
- Scalability
- Availability
- Accessibility
- Self-Organization
- Flexibility

Source: Constraints and approaches for distributed network security, NAI Lab
Sensor Node Constraints

- Battery Power/Energy
  - Computational Energy Consumption
  - Communications Energy Consumption
- Rechargeability
- Sleep Patterns
- Transmission Range
- Memory
  - Program Storage and Working Memory
  - Programmable Storage for Security Information
- Location Sensing
- Tamper Protection
- Time
- Unattended Operations

Source: Constraints and approaches for distributed network security, NAI Lab
Networking Constraints

- Ad hoc Networking
- Limited Pre-Configuration
- Data Rate/Packet Size
- Channel error rate
- Intermittent connectivity
- Unreliable communications
- Latency
- Unicast vs. multicast
- Unidirectional Communications
- Isolated subgroups
- Frequent Routing Changes
- Population Density
- Unknown Recipients

Source: Constraints and approaches for distributed network security, NAI Lab
Sensor Network Encryption Protocol (SNEP)

- $E = \{D\}_{(k_{\text{encr}}, c)}$, $M = \text{MAC}(k_{\text{mac}}, c|\{D\}_{(k_{\text{encr}}, c)})$
- $A \rightarrow B: \{D\}_{(k_{\text{encr}}, c)}$, $M = \text{MAC}(k_{\text{mac}}, c|\{D\}_{(k_{\text{encr}}, c)})$
- **Advantages:**
  - Semantic security: Same message get encrypted differently because of counter
  - Data authentication: MAC verifies
  - Low communication overhead

Source: SPINS: Security protocol for sensor network
Micro TESLA

- Delayed disclosure of symmetric keys.
- Sender computes a MAC with message and a secret key.
- Receiver node stores the msg with MAC in buffer, not the key yet.
- \( K_i = F(K_{i+1}) \)

Source: SPINS: Security protocol for sensor network
Micro TESLA

- Each key corresponds to a time interval, and packets sent in that interval use that key.

\[ K_0 = F(F(k_2)) \]

If key lost, it can be calculated using the function. So, the packets can be authenticated using the key.

Source: SPINS: Security protocol for sensor network
Flat Architecture

Cluster head

Relay nodes

M1
M2
M3
Mn
Mn-1
Mn-2
Removes dup data

Report to cluster head

Reports to higher level
Cluster head

Higher level cluster head makes a decision after
Collecting group data

Higher level cluster head (1,0)

Cluster head (1,1)

Group (1,0)

Group (2,0)

Group (2,1)

Group (2,2)

Group (2,3)

Group (2,4)
Multi party Diffie-Hellman

Cluster head

Broadcast Session Key
Another approach

[Diagram showing distribution of private key to clusters and nodes within two groups, Group A and Group B, with a trusted third party (Certification Authority) at the top.]
Questions?