Authentication in Distributed Systems

CS60002: Distributed Systems

Bhaskar Pal

Dept. of Computer Sc. & Engg.,
Indian Institute of Technology Kharagpur
Outline

- Background
- Conventional Cryptography
- Modern Cryptography
  - Private Key
  - Public Key
- Authentication Protocols
• An Intruder is an entity which is not authorized to access information
Role of Cryptography

• Study of mathematical techniques to secure information

• Goals
  – Confidentiality of Information
  – Authentication
  – Data integrity
A Simple Model of Cryptographic System

- **P** is plaintext
- **C** is ciphertext
- **K_C** and **K_D** are encryption and decryption keys
- **E** and **D** are encryption and decryption algorithms
- **C = E_{K_C}(P) = D_{K_D}(C) = D_{K_D}(E_{K_C}(P))**
Intruder

- Has knowledge of E, D and other information
- Does not know the Key
- The objective of intruder is to interpret the ciphertext
- Also it can perform some malicious communication
A Classification of Cryptographic System

- **Conventional Systems**
  - Plain-text a text written in some language. Use a secret mapping procedure to map a letter (or a set of letters) to some other letter (s) in the same alphabet
  - Example: “adr” → “pgk”
Conventional Cryptography

• The Caeser Cipher
  – C=E(P)=(P+3)mod 26
  – P=D(C)=(C-3)mod26
  – 3 can be replaced by any k, (0<k<26) k is the key

• Simple Substitution
  – Eliminate positional correlation of caeser cipher
  – Cipher line can be any permutation of the alphabets
  – frequency distribution of letters are not changed- !attack

• Polyalphabetic Ciphers
  – periodic sequence of n substitution alphabet ciphers
  – 11, 3, 4, 5, 6
Modern Cryptography

• The plain-text is in binary

• Private key Cryptosystem
  – Same key is used for encryption and decryption
  – Keys are kept secret
  – e.g. DES, AES

• Public key Cryptosystem
  – Encryption and decryption keys are different
  – Decryption keys is kept secret i.e. private and the Encryption key is public
  – e.g. RSA
Private Key Cryptography

- Alice and Bob share a secret key
- If Alice wants to send Bob a message $M$, she encrypts $M$ with the secret key shared between them
- Bob decrypts the message with the same key
- No other person can decrypt the message as only Alice and Bob know the secret key
Data Encryption Standard (DES)

• Encrypts 64 bit blocks with 56 bit key to 64 bit blocks of ciphertext
• Major operations used are permutation and substitution
• Three main stages
  – Initial Permutation
  – 16 rounds of substitution are performed
  – Final Permutation
• Each round uses a round-key generated from the initial key
• Decryption uses the same algorithm but the steps and keys are applied in reverse order
• The crux of the system is the length of the key (56 bits), the intruder has to search $2^{56}$ values
Public Key Cryptography

- Each user generates a pair of keys
- If Alice wants to send Bob a message $M$, she encrypts $M$ with Bob’s public key
- Bob decrypts the message with its private key
- No other person can decrypt the message as only Bob knows his private key

Encryption Algorithm

$$C = E_{\text{pub}}(P)$$

Decryption Algorithm

$$P = D_{\text{prv}}(C)$$
The Rivest-Shamir-Adleman Method

- Select 2 large primes \( p \), \( q \) and compute \( n=p \times q \)
- \( \Phi(n) = (p-1) \times (q-1) \)
- select \( e \), relatively prime to \( \Phi(n) \) i.e. \( \gcd(e, \Phi(n)) = 1 \)
- Find \( d = e^{-1} \mod \Phi(n) \)
- Encryption key known to sender is a pair \( (e, n) \)
- Decryption key known to receiver is a pair \( (d, n) \)
- Encryption is performed as follows
  \( C=M^e \mod n \)
- Decryption is performed as
  \( M = C^d \mod n = M^{ed} \mod n \)
Authentication in Distributed Systems

• **Goal** - The application of cryptographic methods in performing authenticated communication between two entities

• **Authentication in DS** - To verify the identity of the communicating entities to each other

• **System Model**
  – A set of computers connected by a network
  – No shared memory
  – Communication solely by passing messages to each other
Authentication Services

• Authenticated Interactive Communication
  – Both the parties should involve in the communication
  – Synchronous in nature

• Authenticated One Way Communication
  – Sender and Receiver need not to synchronize
  – Asynchronous in nature
  – Example: Electronic Mailing System

• Signed Communication
  – Message is signed by the sender
  – Sender’s identity and content of the message can be authenticated to a third party
Potential Threats

• An intruder
  – Can gain access to any point in the network
  – Can copy or alter parts of the message
  – Can replay back an old message
  – Can transmit erroneous messages

• Intruder can have knowledge about
  – The authentication protocol
  – Message types
  – Message sequences and purposes

• An Intruder
  – May involved in an on-going transaction
  – Can try to prevent a secure authenticated communication
Authentication Servers

- A secret conversation key is required in setting up authenticated communication
- AS is responsible for distributing this secret key
- Each user X registers its secret key $K_X$ with AS
- $K_X$ is only known to X and AS
- AS uses this $K_X$ to securely communicate the secret conversation key to X
Establishing Interactive Connections

• If A wants to set up a secure authenticated interactive communication with B
  – It has to send a message M to B
  – M must have the following properties
    • Only B should understand M
    • B should to able to verify that M is a legitimate message from A and it is not a replay from an intruder
A Protocol for Private Key Systems

• Symmetric in nature - A single secret key is used for both encryption and decryption

• A & B both share a secret conversation key with AS

• Issues Involved
  – How A can get the conversation key from AS?
  – How A can send the received conversation key to B?
Obtaining a Conversation Key

- A → AS : A, B, I_A  
- AS → A : E_{KA}(I_A, B, CK, E_{KB}(CK, A))  

\[ \text{A, B, I}_A \]

\[ \text{E}_{KA}(\text{I}_A, B, \text{CK}, E_{KB}(\text{CK}, A)) \]
Communicating the Conversation Key

- $A \rightarrow B : E_{KB} (CK, A)$ \hspace{1cm} (3)

- To prevent foul play by the intruder

- $B \rightarrow A : E_{CK} (I_B)$ \hspace{1cm} (4)
- $A \rightarrow B : E_{CK} (I_B - 1)$ \hspace{1cm} (5)
Compromising the Conversation Key

- Intruder C has recorded all the messages 3 - 5
- $C \rightarrow B : E_{KB} (CK, A)$  
  (3)
- $B \rightarrow A : E_{CK} (I_B)$  
  (4)
- $A \rightarrow B : E_{CK} (I_B - 1)$  
  (5)
Compromise of a Conversation Key

- Denning - Sacco’s Remedy
  - Incorporate Time-stamp in the messages
  - The new protocol

A → AS : A, B
AS → A : $E_{KA}(B, CK, T, E_{KB}(CK, T, A))$
A → B : $E_{KB}(CK, T, A)$

Check at B: $|CLOCK_B - T| < \Delta t_1 + \Delta t_2$

$\Delta t_1$ : Max discrepancy with the server’s clock
$\Delta t_1$ : Expected Network Delay
A Protocol for Public Key Systems

- For X, The encryption key PKX is known publicly
- The decryption key SKX is secret
- Main Issue:
  - No explicit conversation key is required for communication
  - Public encryption keys are used
  - Handshake protocol
    - A knows the public encryption key of B
    - A doesn’t know the public encryption key of B. However it is known to AS
Handshake Protocol: Public Key is known

- \( \text{A} \rightarrow \text{B} : E_{PKB}(I_A, A) \)
- The intruder can replay such a message
- To verify B sends the following
  - \( \text{B} \rightarrow \text{A} : E_{PKA}(I_A, I_B) \)
  - \( \text{A} \rightarrow \text{B} : E_{PKB}(I_B) \)
Handshake Protocol: Public Key is not known

- $A \rightarrow AS : A, B$
- $AS \rightarrow A : E_{SKAS}(PKB, B)$

- The second message is a signed message and only $AS$ can create it
- $D_{PKAS}(E_{SKAS}(m)) = m$
Performing One-Way Communication

- Asynchronous
- Main Issue is to ensure that the receiver is able to verify the authenticity of the sender and the message
A Protocol for Private Key Systems

- $A \rightarrow AS : A, B, I_A$  \hspace{1cm} (1)
- $AS \rightarrow A : E_{KA}(I_A, B, CK, E_{KB}(CK, A))$ \hspace{1cm} (2)

\[\text{A, B, I}_A\]

\[\text{A, AS}\]

$E_{KA}(I_A, B, CK, E_{KB}(CK, A))$


A Protocol for Private Key Systems

- \( E_{KB}(CK, A) \) is used to authenticate the identity of the sender
- This template is put at the header of the message (mail)
- The mail has the following format -

\[
A \rightarrow B : E_{KB}(CK, A); E_{CK}(M)
\]
A Protocol for Public Key Systems

• A and B know their public encryption keys
  – Otherwise A can take it from AS and send to B

• The mail has the following format -

\[ A \rightarrow B : E_{PKB} (A, I, E_{SKA} (B)); E_{PKB} (I, M) \]

• \( E_{SKA} (B) \) helps B to authenticate the identity of the sender
• Only A can create \( E_{SKA} (B) \)
• Nonce identifier ‘I’ is used to verify the integrity i.e. to connect the header with that of the mail message