Week 11

Lecture 1

User Authentication
Additional Material on Kereberos

Lecture 2

Secure Socket Layer

Workshop 11: Workshop based on Lectures in Week 9

Quiz 11

User Authentication

COMP90043

Lecture 2

Udaya Parampalli

Public Key Cryptography: Diffie-Hellman and RSA

Lecture 1

1.1 User Authentication

- Remote User-Authentication principles
- Means of Authentication
- Mutual Authentication Protocols
- Replay Attacks.
- Protocols Remote User Authentication
  - Needham-Schroeder (NS) Protocol
  - Denning's modification
  - Neuman's modifications

Remote User-Authentication principles

- Authentication is a fundamental building block of a network-based computer systems.
- What is User Authentication?

- "The process of verifying an identity claimed by or for a system entity", RFC 4949 (Internet Security Glossary)

- How do you assure accountability to the actions of users?
- User Authentication is the basis for Access Control.
- What are the important steps?
- According to Stallings: there are two important steps.

Remote User-Authentication

- The process of authentication has the following two important steps: [**William Stallings**]
- **Identification step:** Presenting an identifier to the security system. (Identifiers should be assigned carefully, because authenticated identities are the basis for other security services, such as access control service.)

- **Verification step:** Presenting or generating authentication information that corroborates the binding between the entity and the identifier.
- Note that user authentication is different from message authentication.
- Example: user ID and password;

The NIST Model

Please read NIST 800-63-2 for more details;
Stallings 15.1 gives a brief summary

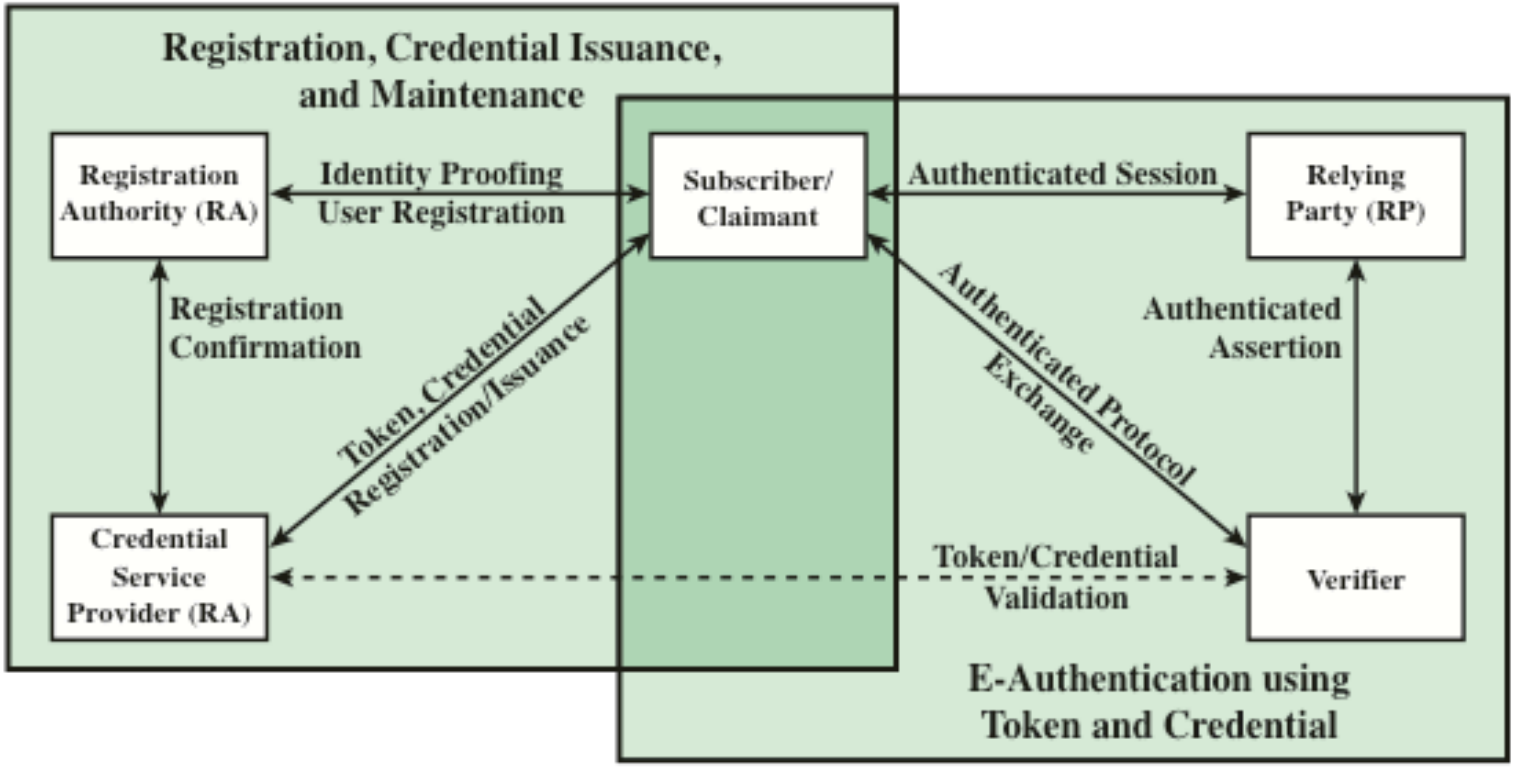

Figure 15.1 The NIST SP 800-63-2 E-Authentication Architectural Model

From William Stallings

Means of Authentication

- Stallings describes four general means of authenticating a user's identity.
- **Something the individual knows**: Examples:a password, a personal identification number (PIN), or answers to a prearranged set of questions.

- **Something the individual possesses**: Examples: cryptographic keys, electronic keycards, smart cards, and physical keys. This type of authenticator is referred to as a token .

- **Something the individual is** (static biometrics): Examples: Recognition by fingerprint, retina, and face.

- **Something the individual does** (dynamic biometrics): Examples: recognition by voice pattern, handwriting characteristics, and typing rhythm.

Mutual Authentication Protocols

- Goals of such protocols is to provide proof for the communicating parties each other's identity and to exchange session keys for subsequent interactions.

- Sometimes protocols can be one-way or mutual.

- Main problem that these protocols solve is to address the two important issues:

- 1. **Confidentiality**: the exchanged session keys are protected,
- 2. **Timeliness**: Ensure that the exchange is current and prevent replay attacks.

Mutual Authentication

- These protocols discussed during key management discussions where the exchange of session keys are the issue. Here the scope of such protocols extended mutual user authentication.
- Stalling's define mutual authentication as "Protocols which enable communicating parties to satisfy themselves mutually about each other's identity and to exchange session keys".

Mutual Authentication

Central to the problem of authenticated key exchange are two issues:

Timeliness

- Important because of the threat of message replays
- Such replays could allow an opponent to:
  - compromise a session key
  - successfully impersonate another party
  - disrupt operations by presenting parties with messages that appear genuine but are not

Confidentiality

- Essential identification and session-key information must be communicated in encrypted form
- This requires the prior existence of secret or public keys that can be used for this purpose

From Stallings

Replay Attacks

- Stallings discusses the following replay attacks from [GONG93]:

1. The simplest replay attack is one in which the opponent simply copies a message and replays it later
2. An opponent can replay a timestamped message within the valid time window
3. An opponent can replay a timestamped message within the valid time window, but in addition, the opponent suppresses the original message; thus, the repetition cannot be detected
4. Another attack involves a backward replay without modification and is possible if symmetric encryption is used and the sender cannot easily recognize the difference between messages sent and messages received on the basis of content

Approaches to Coping With Replay Attacks

- Attach a sequence number to each message used in an authentication exchange
  - A new message is accepted only if its sequence number is in the proper order
  - Difficulty with this approach is that it requires each party to keep track of the last sequence number for each claimant it has dealt with
  - Generally not used for authentication and key exchange because of overhead

- Timestamps
  - Requires that clocks among the various participants be synchronized
  - Party A accepts a message as fresh only if the message contains a timestamp that, in A's judgment, is close enough to A's knowledge of current time

- Challenge/response
  - Party A, expecting a fresh message from B, first sends B a nonce (challenge) and requires that the subsequent message (response) received from B contain the correct nonce value

One-Way Authentication

- Email application also uses encryption.
- Email: Sender and Receiver need not be online at the same time.
  - The envelope or header must be in clear for the protocol to work over public networks.
  - Uses SMTP or X.400. Encryption should ensure that main handling systems cannot obtain decryption keys.
  - Recipient requires an authentication of the message source.

Remote User Authentication

- Let us look at the protocol using symmetric key systems for use over distributed environments.
- The protocol is similar to the Needham-Schroeder protocol we considered earlier.
- A two-level hierarchy of symmetric encryption keys are employed.
- We need a trusted key distribution centre (KDC) and each user shares a master key with the KDC. The KDC generates session keys required for the authenticated sessions.

Applications

- Kerberos: Part of Project Athena-Authentication service over open distributed environment-variants are used everyday- See additional notes for study.
  - This is similar to windows login, when you login to your system-you will login once which will help you to get access to various other services in the system, file system, print system etc.

- Federated Identity Management: Relatively new concept: a common identity management scheme across multiple enterprises works in a large scale with millions of uses –See additional notes.
- We will discuss some protocol issues in the workshop.

Needham-Schroeder (NS) Protocol

- Let us look at the protocol as discussed in the textbook.
- The protocol:

1. A->KDC: $ID_A \| ID_B \| N_1$

2. KDC -> A: $E(K_a,[K_s \| ID_B \| N_1 \| E(K_b,[K_s \| ID_A])])$

3. A -> B: $E(K_b, [K_s \| ID_A])$

4. B -> A: $E(K_s, [N_2])$

5. A -> B: $E(K_s, [f(N_2)])$

Issues with NS protocol

- Main goal: secure distribution of session keys between communicating parties.
- It is vulnerable to a replay attack if an old session key is compromised.

- How do you address this situation?
- Dennings modification using timestamps.
- Neuman approach of using nonces.

NS Dennings Modification.

- Stallings discusses the following modification by Denning, 1981.

1. $A \rightarrow KDC: \quad ID_A \| ID_B$
2. $KDC \rightarrow A: \quad E(K_a, [K_s \| ID_B \| T \| E(K_b, [K_s \| ID_A \| T])])$
3. $A \rightarrow B: \quad E(K_b, [K_s \| ID_A \| T])$
4. $B \rightarrow A: \quad E(K_s, N_1)$
5. $A \rightarrow B: \quad E(K_s, f(N_1))$

- T: Time stamp, assures fresh keys for A and B;
- Verification: that | Clock – *T* | < *delta t*1 + delta *t*2
- delta t1: mean discrepancy between KDC's and local clocks
- delta t2: mean network delay time

Suppress-Replay Attacks

- The NS –Dennings uses global synchronized clocks-expensive to maintain.
- What is a Suppress-Replay attack?

- An adversary stores a past message and he replays later when the timestamp in the message becomes current at the recipient's machine.

- How to avoid?

- Parties regularly synchronize their clocks with that of KDC.
- Use handshaking protocols using nonces

NS Protocol

- Denning 81 Modification

1. $A \rightarrow KDC: \quad ID_A \| ID_B$
2. $KDC \rightarrow A: \quad E(K_a, [K_s \| ID_B \| T \| E(K_b, [K_s \| ID_A \| T])])$
3. $A \rightarrow B: \quad E(K_b, [K_s \| ID_A \| T])$
4. $B \rightarrow A: \quad E(K_s, N_1)$
5. $A \rightarrow B: \quad E(K_s, f(N_1))$

- Neuman 93 Modification

1. $A \rightarrow B: \quad ID_A \| N_a$
2. $B \rightarrow KDC: \quad ID_B \| N_b \| E(K_b, [ID_A \| N_a \| T_b])$
3. $KDC \rightarrow A: \quad E(K_a, [ID_B \| N_a \| K_s \| T_b]) \| E(K_b, [ID_A \| K_s \| T_b]) \| N_b$
4. $A \rightarrow B: \quad E(K_b, [ID_A \| K_s \| T_b]) \| E(K_s, N_b)$

Think why the later is an interesting solution to resist SR attacks?

Authentication using Public Key Approach

- Many varieties of protocols exist.
- We saw before a scheme based on public key encryption.
- Important issue is each party should have correct public key of the other
- A method using Authentication Server is a possibility.
- Various protocols exist making use of time stamps and nonces.

Week 11

Lecture 1

User Authentication
Additional Material on Kereberos

Lecture 2

Secure Socket Layer

Workshop 11: Workshop based on Lectures in Week 9

Quiz 11