Security Recap

- Encryption - uses 'keys'
  - Symmetric keys
    - AES; ‘session key’ through key distribution center
  - Public keys
    - RSA algorithm; Certificate authority to get key
- Message integrity
  - MAC - with hash function and authentication key
- Digital signature
  - MAC + public key
- Nonce - to discuss now!

### Security Mechanisms

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Access &amp; Integrity</th>
<th>Confidentiality</th>
<th>Data Integrity</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symmetric key cryptography</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public key cryptography</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message Authentication Code, MAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital signature</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nonce</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key distribution center</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate authority</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Which mechanisms address which principles?

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Access &amp; Integrity</th>
<th>Confidentiality</th>
<th>Data Integrity</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symmetric key cryptography</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public key cryptography</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message Authentication Code, MAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital signature</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nonce</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key distribution center</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate authority</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
*End point authentication*

1) State “I am Alice”
   - Anyone can do this
2) Provide IP address along with statement
   - Easy to get and use someone else’s IP address: “IP spoofing”
3) Provide password, IP address and name
   - Playback attack
   - Provide encrypted password, IP address and name: Playback attack still works
4) Use ‘nonce’ (think about Apple Pay)
   - A ‘number’ used only ‘once’
   - Allows for “woman-in-the-middle” attacks

**Authentication with nonce**

This approach requires a shared symmetric key

- can we authenticate using public key techniques?
- Use nonce + public key cryptography?

Authentication: yet another try

**Goal:** avoid playback attack

**Nonce:** Select a number (R) used only once—in-a-lifetime

To prove Alice is “live”, Bob sends Alice nonce, R. Alice must return R, encrypted with shared secret key

'R nonce' Security Hole

Woman in the middle attack: Trudy poses as Alice (to Bob) and as Bob (to Alice)
'nonce' Security Hole

Woman in the middle attack: Trudy poses as Alice (to Bob) and as Bob (to Alice)

Difficult to detect:
- Bob receives everything that Alice sends, and vice versa.
- Bob, Alice can meet one week later and recall conversation
- Problem is that Trudy receives all messages as well

Review: Network Security

- The field of network security is about:
  - how computer networks can be attacked
  - how to defend networks against these attacks
  - how to design protocols and hardware that are immune to attacks
- But, the design of the Internet...
  - Original vision: a group of mutually trusting users attached to a transparent network
  - Security considerations are in all layers
  - Internet protocol designers are trying to catch up

Recap so far...

Security mechanisms

- Cryptography
  - Keys - symmetric and public/private
  - Key distribution
- Hash function + Authentication key
- Nonce

To provide
- Secure access to resources
- Confidentiality
- Message integrity
- Authentication

Types of Attacks

- Eavesdrop:
  - Intercept messages; sniff packets
- Actively insert, reorder, corrupt messages into connection
- Impersonation:
  - Fake (spoof) source address in packet
  - Record and playback
- Hijacking: "take over" ongoing connection by removing sender or receiver, inserting self in place
- Denial of service: prevent service from being used by others (e.g., by overloading resources), attack on the infrastructure
Malware

- **Virus, worm, trojan horse**
  - An attack in their own right
  - Used to distribute software to be used in security breach
- **Spyware**: to record keystrokes
- **Botnet**: to take control of a host
- ... Often is self-replicating

Chapter 8 roadmap

- 8.1 What is network security?
- 8.2 Principles of cryptography
- 8.3 Message integrity
- 8.4 Securing e-mail
- 8.5 Securing TCP connections: SSL
- 8.6 Network layer security: IPsec
- 8.7 Securing wireless LANs
- 8.8 Operational security: firewalls and IDS

**email: Confidential step 1**

- Alice wants to send confidential e-mail, m, to Bob.

Alice:
1) Generate random symmetric private key, $K_S$
2) Encrypt message with $K_S$
3) Encrypt $K_S$ with Bob’s public key
4) Send both $K_S(m)$ and $K_B(K_S)$ to Bob

**email: Confidential step 2**

- Alice wants to send confidential e-mail, m, to Bob.

Bob:
- Uses his private key to decrypt and recover $K_S$
- Uses $K_S$ to decrypt $K_S(m)$ to recover m
email: Message integrity & authentication

- Alice wants to provide sender authentication message integrity. …How?
- Alice digitally signs message
- sends both message (in the clear) and digital signature

Pretty good privacy (PGP)

- To Activity (to act out PGP)...
- Internet e-mail encryption scheme, de facto standard.
- Uses
  - Symmetric key cryptography
  - Public key cryptography
  - Hash function
  - Digital signature
- Provides
  - Secrecy
  - Sender authentication
  - Integrity

email: fully secure

- Alice wants to provide secrecy, sender authentication & message integrity. …How?
- Alice uses three keys: her private key, Bob’s public key, the newly created symmetric key
- What does Bob do to retrieve the msg & be sure it came from Alice?

Chapter 8 roadmap

8.1 What is network security?
8.2 Principles of cryptography
8.3 Message integrity
8.4 Securing e-mail
8.5 Securing TCP connections: SSL
8.6 Network layer security: IPsec
8.7 Securing wireless LANs
8.8 Operational security: firewalls and IDS