Introduction

Ahmet Burak Can
Hacettepe University
abc@hacettepe.edu.tr
Books

• Textbook:

• Supplementary books:
  ◦ Handbook of Applied Cryptography. A. Menezes, P. van Oorschot and S. Vanstone. CRC Press
Outline of the Course

- Basic ciphers
- Block ciphers, Encryption modes and Stream ciphers
- Hash functions, message digests, HMAC
- Number Theory, Public Key Cryptography, RSA
- Digital certificates and signatures, X509
- Authentication: Two-Three factor authentication, Biometrics, Smart Cards
- Security Handshake
- Real-time Communication Security, SSL/TLS, IPSEC
- Kerberos
Outline of the Course

- Threshold cryptography
- Operating System Security
- Malicious Software: Trojans, logic bombs, viruses, worms, botnets, rootkits, trapdoors and cover channels
- Program Security
- Firewalls, VPNs, Intrusion detection systems
- HTTP and Web Application Security, XSS
- Wireless Security: WEP and WPA
Which Security Concept?

Computer Security

Network Security

Information Security

Computer Security
Information Security

- **Computer Security:**
  - Ensure security of data kept on the computer

- **Network Security:**
  - Ensure security of communication over insecure medium

- **Approaches to Secure Communication**
  - **Steganography**
    - hides the existence of a message
  - **Cryptography**
    - hide the meaning of a message
Steganography Sample

- Least significant bit values of pixels can be used to hide a secret message
  - Below images seem to be same but right picture store 5 Shakespeare games.

Hamlet, Macbeth, Julius Caesar
Merchant of Venice, King Lear
Basic Security Goals

- Privacy (secrecy, confidentiality)
- Authenticity (integrity)
- Authorization
- Availability
- Non-repudiation
- Auditing
Privacy (secrecy, confidentiality)

- Only the intended recipient can see the contents of the communication.
- SSL, https protocols can protect privacy of communication.
- Some applications have encrypted communication capabilities to protect privacy, such as Skype, Whatsapp.
Privacy (secrecy, confidentiality)

- However, encryption is not enough to protect privacy

Big brother is watching YOU!!!
Authenticity (integrity)

- The communication is generated by the alleged sender.
- Are you sure that you are communicating with the right person?
Authorization

- Limit the resources that a user can access
- In the real world, we use lock, fences etc.
Authorization

- If authorization mechanisms are not properly defined, resources cannot be protected.
Authorization

- In the digital world, we use password, smartcard, usb tokens, fingerprints, etc. for authentication.

- Sometimes multiples of them 😊

  https://youtu.be/lI6Ci-fkFtA
Availability

- Make the services available 99.999...% of time
Availability

- Internet worms can cause billions of dollar damage, such as Slammer, Nimda, Code Red worms.
- Availability is requirement for Internet companies!
Non-repudiation

- No party can refuse the validity of its actions.
- In the real world, we use wet signatures, authorization offices (noter):

\[ \text{Signature} \]

- In the digital world, similar signature techniques can be used:
Non-repudiation

- Digital signatures can provide cryptographic non-repudiation in the digital world, especially in remote services:

- Biometrics can also be used as a kind of non-repudiation mechanism:
Auditing

- Take a log of everything done in the system
- Then use it for further analysis

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>SourceMAC</th>
<th>Destination</th>
<th>DestMAC</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>44982</td>
<td>2102</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>ARP</td>
<td>Who has 10.0.0.1.12569 Tell 10.0.0.1.12569</td>
</tr>
<tr>
<td>44983</td>
<td>2102</td>
<td>0.0.0.0.0.0</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>CUPS</td>
<td>app://10.0.0.121/printer/Brother (udle)</td>
</tr>
<tr>
<td>44984</td>
<td>2102</td>
<td>0.0.0.0.0.0</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>ARP</td>
<td>Who has 192.168.0.1.247 Tell 192.168.0.1.247</td>
</tr>
<tr>
<td>44951</td>
<td>2102</td>
<td>0.0.0.0.0.0</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>CUPS</td>
<td>app://10.0.0.121/printer/Brother (udle)</td>
</tr>
<tr>
<td>44952</td>
<td>2102</td>
<td>0.0.0.0.0.0</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>ARP</td>
<td>Who has 192.168.0.1.247 Tell 192.168.0.1.247</td>
</tr>
<tr>
<td>44953</td>
<td>2102</td>
<td>0.0.0.0.0.0</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>CUPS</td>
<td>app://10.0.0.121/printer/Brother (udle)</td>
</tr>
<tr>
<td>44954</td>
<td>2102</td>
<td>0.0.0.0.0.0</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>ARP</td>
<td>Who has 192.168.0.1.247 Tell 192.168.0.1.247</td>
</tr>
<tr>
<td>44955</td>
<td>2102</td>
<td>0.0.0.0.0.0</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>CUPS</td>
<td>app://10.0.0.121/printer/Brother (udle)</td>
</tr>
<tr>
<td>44956</td>
<td>2102</td>
<td>0.0.0.0.0.0</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>ARP</td>
<td>Who has 192.168.0.1.247 Tell 192.168.0.1.247</td>
</tr>
<tr>
<td>44957</td>
<td>2102</td>
<td>0.0.0.0.0.0</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>CUPS</td>
<td>app://10.0.0.121/printer/Brother (udle)</td>
</tr>
<tr>
<td>44958</td>
<td>2102</td>
<td>0.0.0.0.0.0</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>ARP</td>
<td>Who has 192.168.0.1.247 Tell 192.168.0.1.247</td>
</tr>
<tr>
<td>44959</td>
<td>2102</td>
<td>0.0.0.0.0.0</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>CUPS</td>
<td>app://10.0.0.121/printer/Brother (udle)</td>
</tr>
<tr>
<td>44960</td>
<td>2102</td>
<td>0.0.0.0.0.0</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>ARP</td>
<td>Who has 192.168.0.1.247 Tell 192.168.0.1.247</td>
</tr>
<tr>
<td>44961</td>
<td>2102</td>
<td>0.0.0.0.0.0</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>CUPS</td>
<td>app://10.0.0.121/printer/Brother (udle)</td>
</tr>
<tr>
<td>44962</td>
<td>2102</td>
<td>0.0.0.0.0.0</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>ARP</td>
<td>Who has 192.168.0.1.247 Tell 192.168.0.1.247</td>
</tr>
<tr>
<td>44963</td>
<td>2102</td>
<td>0.0.0.0.0.0</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>CUPS</td>
<td>app://10.0.0.121/printer/Brother (udle)</td>
</tr>
<tr>
<td>44964</td>
<td>2102</td>
<td>0.0.0.0.0.0</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>ARP</td>
<td>Who has 192.168.0.1.247 Tell 192.168.0.1.247</td>
</tr>
<tr>
<td>44965</td>
<td>2102</td>
<td>0.0.0.0.0.0</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>CUPS</td>
<td>app://10.0.0.121/printer/Brother (udle)</td>
</tr>
<tr>
<td>44966</td>
<td>2102</td>
<td>0.0.0.0.0.0</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>ARP</td>
<td>Who has 192.168.0.1.247 Tell 192.168.0.1.247</td>
</tr>
<tr>
<td>44967</td>
<td>2102</td>
<td>0.0.0.0.0.0</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>CUPS</td>
<td>app://10.0.0.121/printer/Brother (udle)</td>
</tr>
<tr>
<td>44968</td>
<td>2102</td>
<td>0.0.0.0.0.0</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>ARP</td>
<td>Who has 192.168.0.1.247 Tell 192.168.0.1.247</td>
</tr>
<tr>
<td>44969</td>
<td>2102</td>
<td>0.0.0.0.0.0</td>
<td>00:00:0000:0000:0000</td>
<td>192.168.0.1</td>
<td>00:00:0000:0000:0000</td>
<td>CUPS</td>
<td>app://10.0.0.121/printer/Brother (udle)</td>
</tr>
</tbody>
</table>