Introduction

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

Books

- Textbook:
  - Network Security: Private Communication in a Public World, 2nd Edition. C. Kaufman, R. Perlman, and M. Speciner, Prentice-Hall
  - Security in Computing. C. P. Pfleeger and S. L. Pfleeger, Prentice Hall
- Supplementary books:
  - Applied Cryptography: Protocols, Algorithms, and Source Code in C, B. Schneier, John Wiley & Sons.
  - Handbook of Applied Cryptography. A. Menezes, P. van Oorschot and S. Vanstone. CRC Press
  - Security Engineering: A Guide to Building Dependable Distributed Systems, Ross J. Anderson, John Wiley & Sons

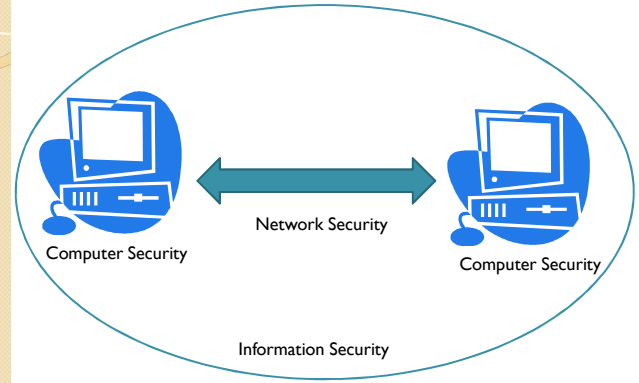
Outline of the Course

- 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
- Auhentication: 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?



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

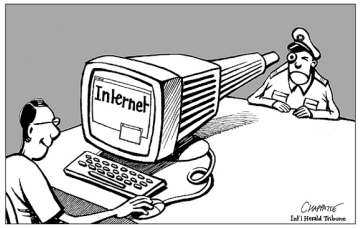
- Privacy (secrecy, confidentiality)
- Authenticity (integrity)
- Authorization
- Availability
- Non-repudiation
- Auditing

Privacy (secrecy, confidentiality)

- Only the intended recipient can see the contents of the communication
- SSL, https protocols can protect privacy of communication.
- Some applications has encrypted communication capabilites to protect privacy, such as Skype, Whatsup

Privacy (secrecy, confidentiality)

- However, encryption is not enough to protect privacy

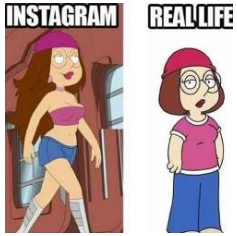


Big brother is watching

YOU!!!

Authenticity (integrity)

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



Authorization

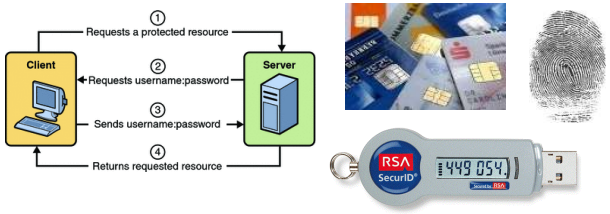
- Limit the resources that a user can access
- In the real world, we use lock, fences etc.

Authorization

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

Authorization

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



- Sometimes multiples of them ☺
  https://youtu.be/II6Ci-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):

Signatura

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

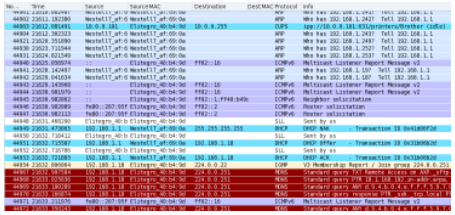
Non-repudiation

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

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

Auditing

- Take a log of everything done in the system



- Then use it for further analysis