

## Introduction

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

## Books

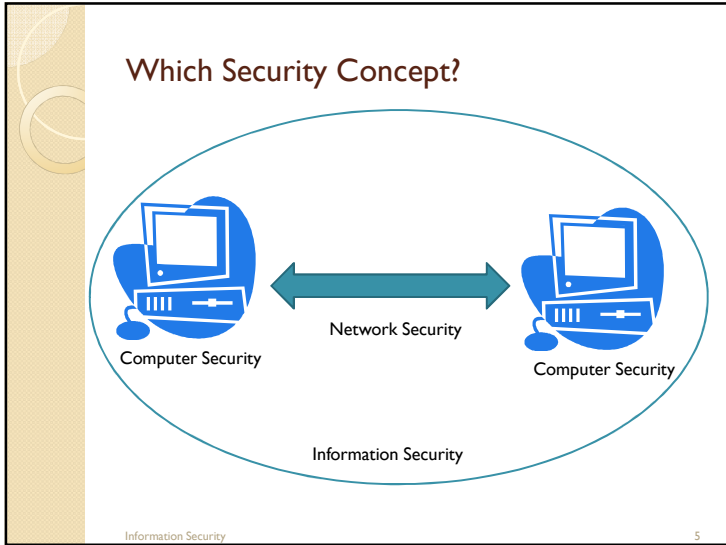
- Textbook:
  - Network Security: Private Communication in a Public World, 2nd Edition. C. Kaufman, R. Perlman, and M. Speciner, Prentice-Hall
  - [Computer Security and the Internet: Tools and Jewels](#) by Paul C. van Oorschot. 2019, Springer.
- Supplementary books:
  - Security in Computing. C. P. Pfleeger and S. L. Pfleeger, Prentice Hall
  - 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
- 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
- Firewalls, VPNs, Intrusion detection systems



- ### Basic Security Goals
- Privacy (secrecy, confidentiality)
  - Authenticity (integrity)
  - Authorization
  - Availability
  - Non-repudiation
  - Auditing
- Information Security
- 6

- ### 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 capabilities to protect privacy, such as Skype, Whatsup
- 
- 
- 
- Information Security
- 7

### Privacy (secrecy, confidentiality)

- However, encryption is not enough to protect privacy

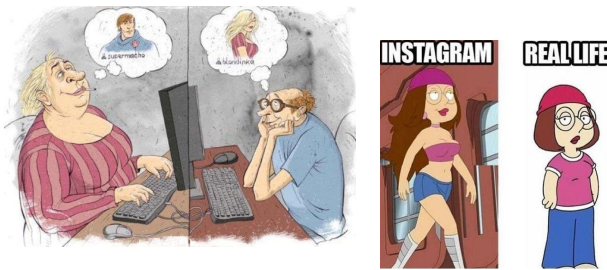
Big brother is watching YOU!!!

Information Security

8

### Authenticity (integrity)

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



Information Security

9

### Authorization

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

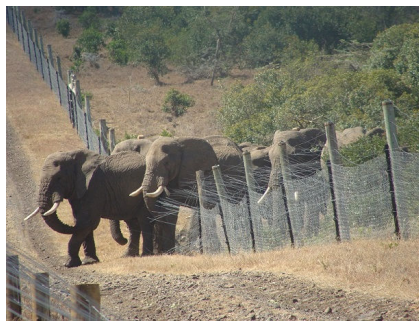


Information Security

10

### Authorization

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

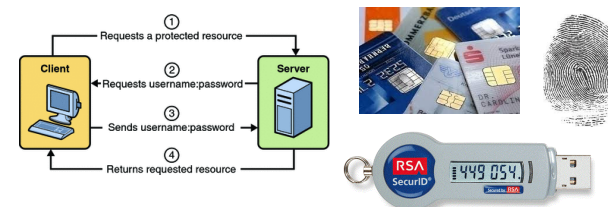


Information Security

11

### Authorization

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



- Sometimes multiples of them ☺



<https://youtu.be/1l6Ci-fkFtA>

Information Security

12

### Availability


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

Information Security 13

### Availability

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



Information Security 14

### Non-repudiation

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

*Signature*


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



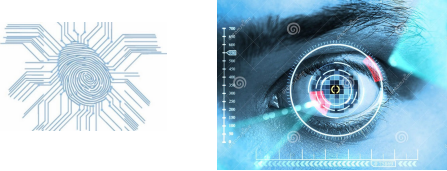
Information Security 15

### 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:



Information Security 16



