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
- Firewalls,VPNs, Intrusion detection systems
Which Security Concept?

Computer Security <-> Network Security <-> Computer Security

Information Security

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

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

Authorization

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

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

- Sometimes multiples of them 😊

https://youtu.be/lI6Ci-fkFtA
Make the services available 99.999...% of time

Internet worms can cause billions of dollar damage, such as Slammer, Nimda, Code Red worms.

Availability is requirement for Internet companies!

No party can refuse the validity of its actions.

In the real world, we use wet signatures, authorization offices (noter):

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

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

Why security is hard to protect?

- You may trust SSL protocol, but the implementation might contain bugs:
  - Heartbleed bug: http://heartbleed.com
- You may trust your operating system, but it may contain hundreds of bugs:
  - National Vulnerability Database: https://nvd.nist.gov
- You may trust your CPU, but it might have problems:
  - Meltdown and spectre attacks: https://meltdownattack.com
- Even more, the vendor might install suspicious chips to your motherboard:

Law enforcement

- Learn about cyber crimes:
  - https://tr.wikipedia.org/wiki/Bilişim_suçları
  - http://www.atanerav.tr/bilsim-suclari/
- David Smith:
  - Melissa virus: 20 months in prison
- Ehud Tenenbaum (“The Analyzer”):
  - Broke into US DoD computers
  - sentenced to 18 months in prison, served 8 months
- Dmitri Sklyarov:
  - Broke Adobe ebooks
  - Arrested by the FBI, prosecuted under DMCA, stayed in jail for 20 days
- Onur Kılıçak: