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

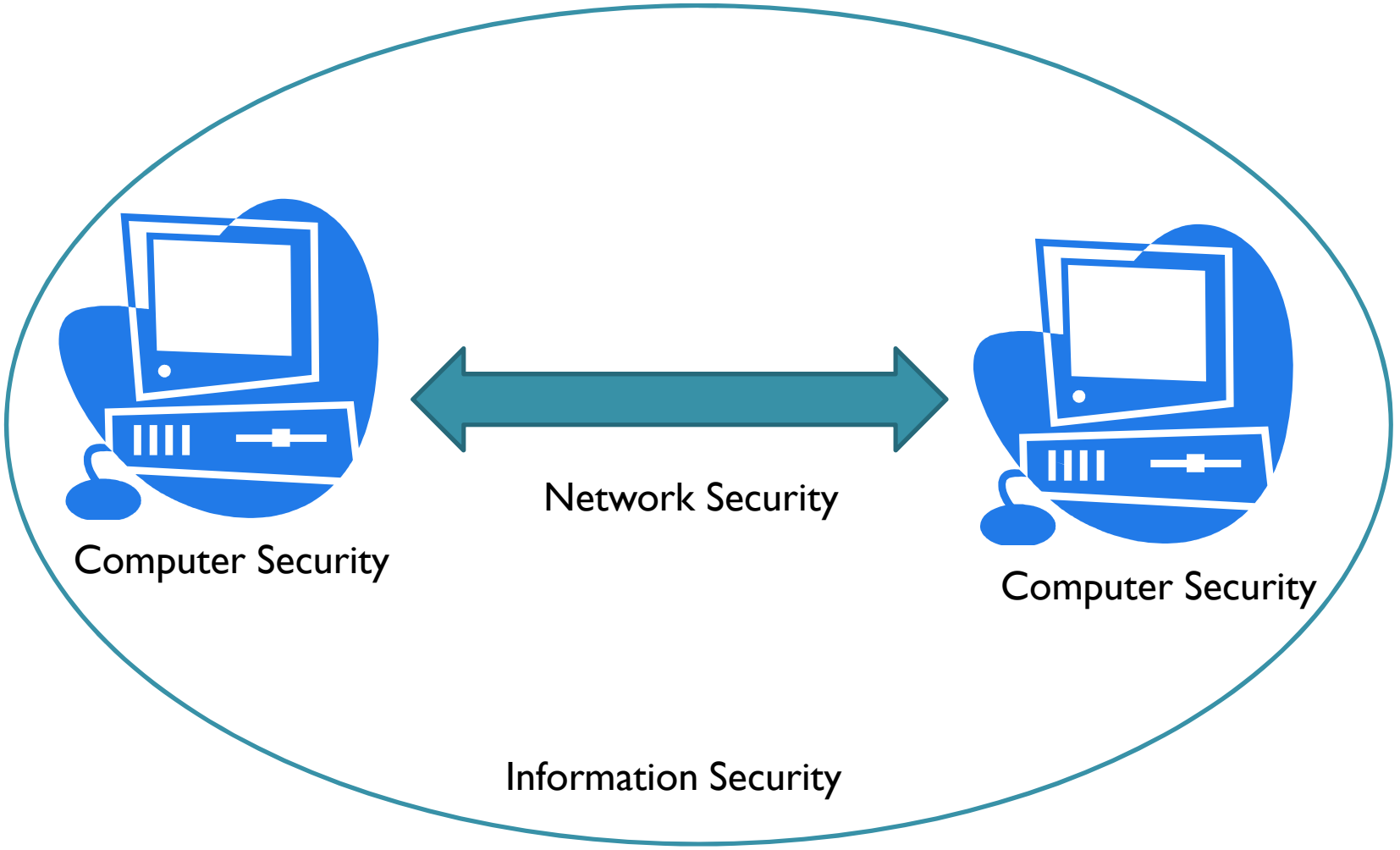
Outline of the Course

- 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
- 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
- Firewalls, VPNs, Intrusion detection systems

Which Security Concept?



Basic Security Goals

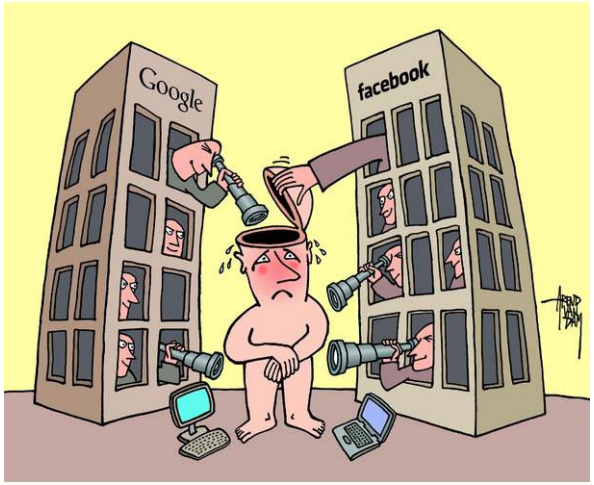
- Privacy (secrecy, confidentiality)
- Authenticity (integrity)
- Authorization
- Availability
- Non-repudiation
- Auditing

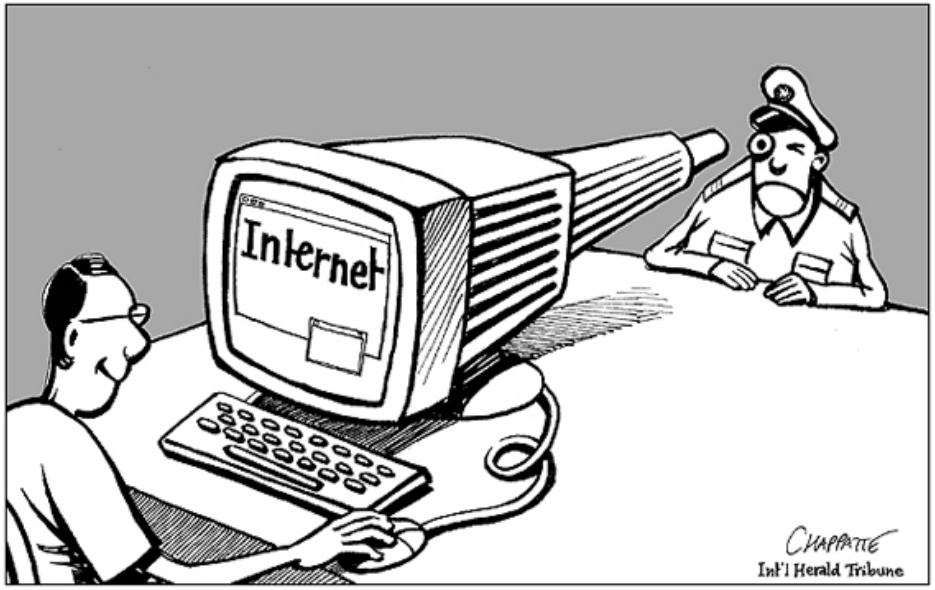
Privacy (secrecy, confidentiality)

- 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)

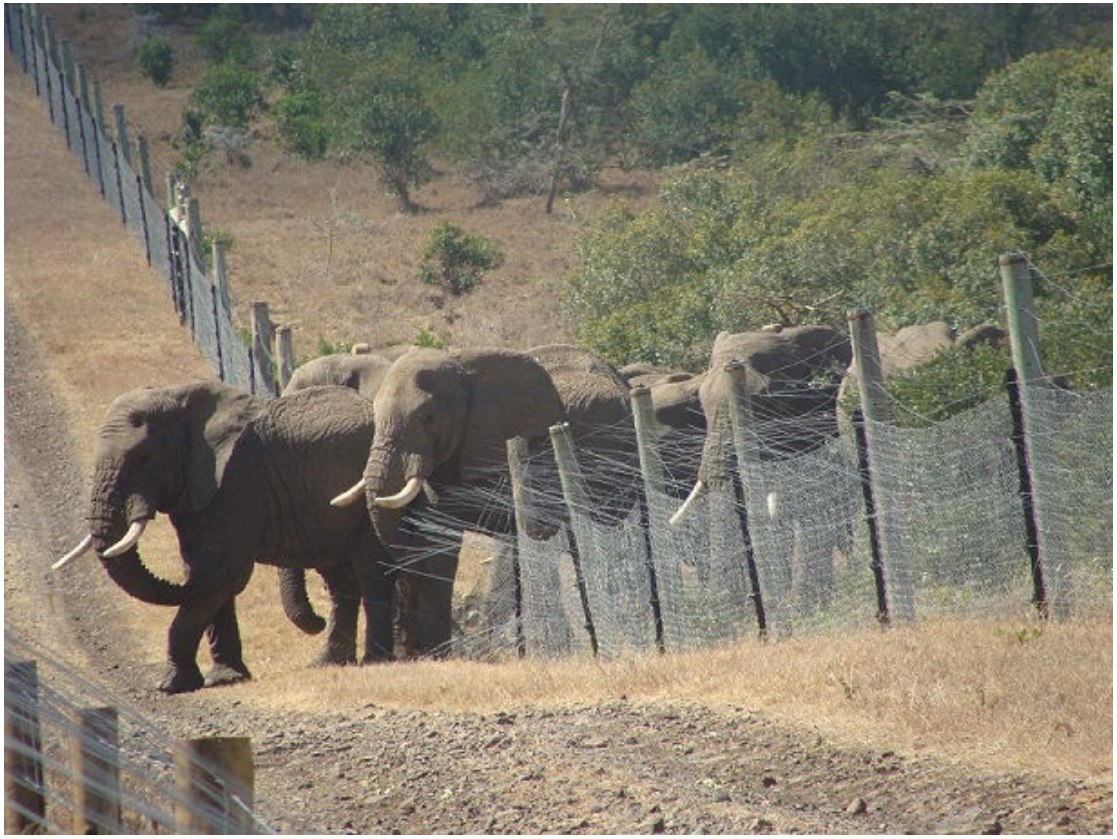
- The communication is generated by the alleged sender.
- Are you sure that you are communicating with the right person?

Authorization

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

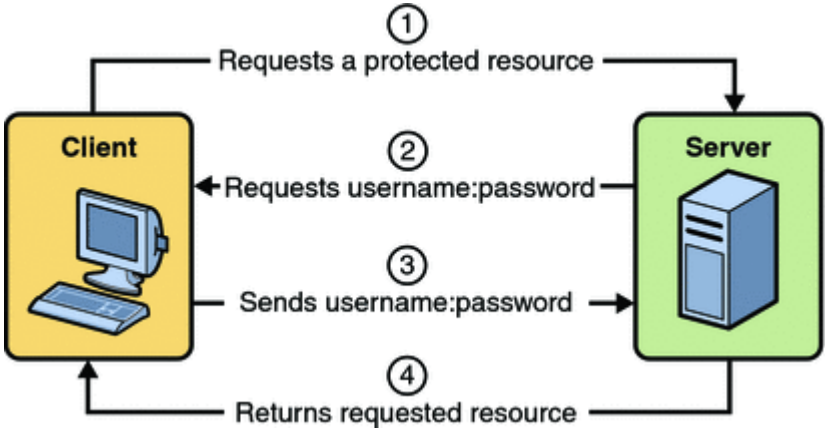
Authorization

- 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):

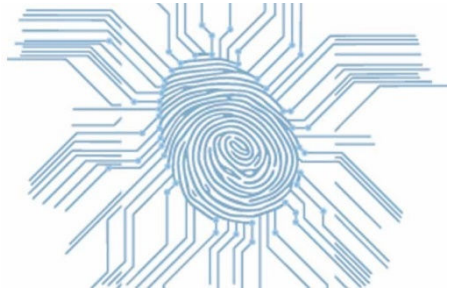
Signature

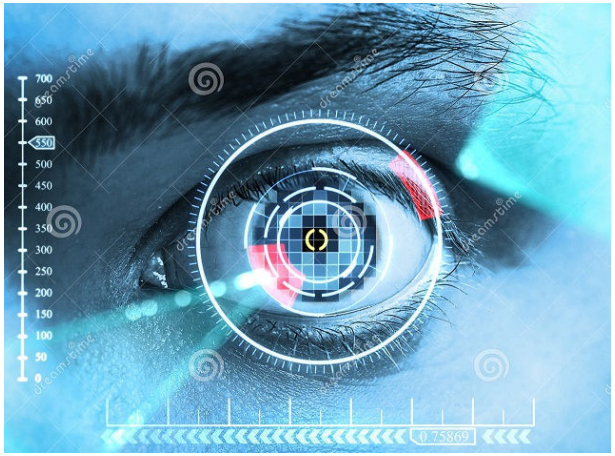
- In the digital world, similar signature techniques can be used:

Non-repudiation

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

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





Auditing

- Take a log of everything done in the system

No.	Time	Source	SourceMAC	Destination	DestMAC	Protocol	Info
44902	21611.192380	WestellT_af:6	WestellT_af:69:0a			ARP	Who has 192.168.1.242? Tell 192.168.1.1
44903	21612.081491	10.0.0.101	Elitegro_40:b4:9d	10.0.0.255		CUPS	ipp://10.0.0.101:631/printers/Brother (idle)
44904	21612.302323	WestellT_af:6	WestellT_af:69:0a			ARP	Who has 192.168.1.243? Tell 192.168.1.1
44921	21620.351890	WestellT_af:6	WestellT_af:69:0a			ARP	Who has 192.168.1.249? Tell 192.168.1.1
44930	21623.711944	WestellT_af:6	WestellT_af:69:0a			ARP	Who has 192.168.1.252? Tell 192.168.1.1
44931	21624.821549	WestellT_af:6	WestellT_af:69:0a			ARP	Who has 192.168.1.253? Tell 192.168.1.1
44940	21625.056974	::	Elitegro_40:b4:9d	ff02::16		ICMPv6	Multicast Listener Report Message v2
44941	21628.142497	WestellT_af:6	WestellT_af:69:0a			ARP	Who has 192.168.1.19? Tell 192.168.1.1
44942	21629.041634	WestellT_af:6	WestellT_af:69:0a			ARP	Who has 192.168.1.18? Tell 192.168.1.1
44943	21629.143968	::	Elitegro_40:b4:9d	ff02::16		ICMPv6	Multicast Listener Report Message v2
44944	21630.981979	::	Elitegro_40:b4:9d	ff02::16		ICMPv6	Multicast Listener Report Message v2
44945	21630.982062	::	Elitegro_40:b4:9d	ff02::1:ff40:b49c		ICMPv6	Neighbor solicitation
44946	21630.982089	fe80::207:95f	Elitegro_40:b4:9d	ff02::2		ICMPv6	Router solicitation
44947	21630.982113	fe80::207:95f	Elitegro_40:b4:9d	ff02::2		ICMPv6	Router solicitation
44948	21631.468290	Elitegro_40:b	Elitegro_40:b4:9d			SLL	Sent by us
44949	21631.473065	192.168.1.1	WestellT_af:69:0a	255.255.255.255		DHCP	DHCP NAK - Transaction ID 0x41d06f2d
44950	21632.710412	Elitegro_40:b	Elitegro_40:b4:9d			SLL	Sent by us
44951	21632.715587	192.168.1.1	WestellT_af:69:0a	192.168.1.18		DHCP	DHCP Offer - Transaction ID 0x31b06b2d
44952	21632.716786	Elitegro_40:b	Elitegro_40:b4:9d			SLL	Sent by us
44953	21632.721885	192.168.1.1	WestellT_af:69:0a	192.168.1.18		DHCP	DHCP ACK - Transaction ID 0x31b06b2d
44954	21632.806064	192.168.1.18	Elitegro_40:b4:9d	224.0.0.22		IGMP	V3 Membership Report / Join group 224.0.0.251
44967	21632.907584	192.168.1.18	Elitegro_40:b4:9d	224.0.0.251		MDNS	Standard query TXT Remote Access on AXP._sftp-
44968	21633.025036	192.168.1.18	Elitegro_40:b4:9d	224.0.0.251		MDNS	Standard query PTR 18.1.168.192.in-addr.arpa,
44969	21633.100289	192.168.1.18	Elitegro_40:b4:9d	224.0.0.251		MDNS	Standard query ANY d.9.4.b.0.4.e.f.f.f.5.9.7.0
44970	21633.166874	192.168.1.18	Elitegro_40:b4:9d	224.0.0.251		MDNS	Standard query response PTR _ssh._tcp.local PT
44971	21633.211976	fe80::207:95f	Elitegro_40:b4:9d	ff02::16		ICMPv6	Multicast Listener Report Message v2
44972	21633.350243	192.168.1.18	Elitegro_40:b4:9d	224.0.0.251		MDNS	Standard query ANY d.9.4.b.0.4.e.f.f.f.5.9.7.0

- Then use it for further analysis

Why security is hard to protect?

- You may trust SSL protocol, but the implementation might contain bugs :
  - Heatbleed 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:
  - https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Law enforcement

- Learn about cyber crimes:
  - https://tr.wikipedia.org/wiki/Bilişim_suçları
  - http://www.atamer.av.tr/bilisim-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
- Dmitry Sklyarov
  - Broke Adobe ebooks
  - Arrested by the FBI, prosecuted under DMCA, stayed in jail for 20 days
- Onur Kıpçak
  - http://www.hurriyet.com.tr/bilgisayar-korsanina-135-yil-hapis-cezasi-daha-40038386