

# Introduction

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

Information Securi

### 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

Information Security

### **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.
  - <u>Handbook of Applied Cryptography</u>. 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

Information Security

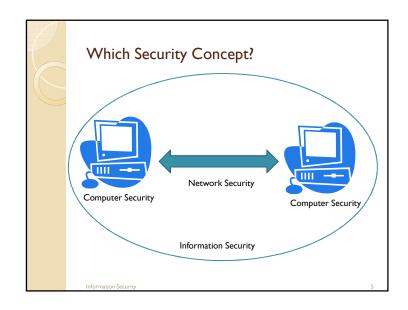
2

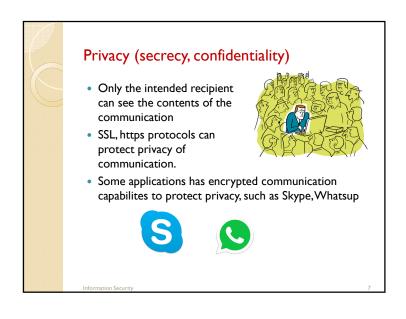
### Outline of the Course

- Threshold cryptography
- Operating System Security
- Malicious Software: Trojans, logic bombs, viruses, worms, botnets, rootkits, trapdoors and cover channels
- Firewalls, VPNs, Intrusion detection systems

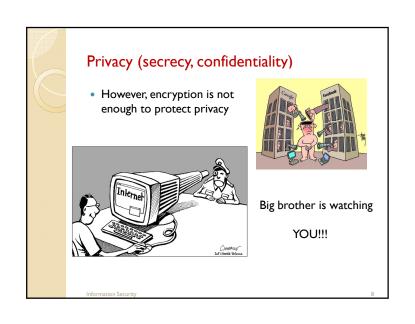
nformation Security

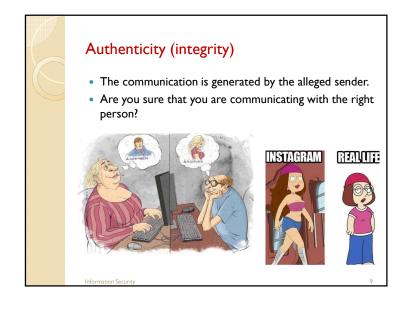
1





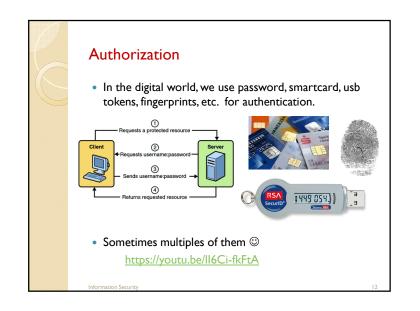
# Basic Security Goals Privacy (secrecy, confidentiality) Authenticity (integrity) Authorization Availability Non-repudiation Auditing













 Make the services available 99.999...% of time



SERVER DOWN

13

# **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:



Information Security

16

# Auditing

• Take a log of everything done in the system

	Time	Source	SourceMAC	Destination	DestMAC Protocol	info
	X1010.00140/	MEDIEFFI BITO	MEDIGCELTT. 03: 09		HEN.	WHO HAS \$32,\$00.1,241   IECC \$32,\$00.1,1
	21611.192399		WestellT_af:09:Da		HP	Who has 192.168.1.2427 Tell 192.168.1.1
	21612.081491	10.0.0.101	Elitegro_40:b4:9d	10.0.0.255	CUPS	ipp://10.0.0.101:631/printers/Brother (idle)
	21612.302323		WestellT_af:69:60		ARP	Who has 192.168.1.2437 Tell 192.168.1.1
	21620.351890		WestellT_af:69:0a		HP	Who has 192.168.1.2497 Tell 192.168.1.1
	21623.711944		WestellT_af:69:0a		APP	Who has 192.168.1.2527 Tell 192.168.1.1
	21624.821549		WestellT_af:69:8a		ARP	Who has 192.168.1.253? Tell 192.168.1.1
	21625.056974		Elitegro_40:b4:9d	ff82::16	IOPv6	Multicast Listener Report Message v2
	21028.142497		WestellT_af:09:Da		HP	Who has 192.168.1.197 Tell 192.168.1.1
44942	21629.041634	WestellT af:6	WestellT af:69:8a		ARP	Who has 192,168,1,187 Tell 192,168,1,1
	21629.143968		Elitegro_40:b4:9d	ff82::16	IOPV6	Multicast Listener Report Message v2
	21630.981979		Elitegro_40:b4:9d	ff02::16	IOF46	Multicast Listener Report Message v2
44945	21630.982062		Elitegro 49:b4:9d	ff82::1:ff48:b49		Neighbor solicitation
44946	21638.982889	fe88: :287:95f	Elitearo 48:b4:9d	ff82::2	IOPv6	Router solicitation
44947	21630.982113	fe00::207:95f	Eliteoro 40:b4:9d	ff02::2	ICPPv6	Router solicitation
44940	21631.468299	Eliteoro 40:b	Eliteoro 40:b4:9d		SLL	Sent by us
44949	21631.473955	192, 168, 1, 1	WestellT af:69:8a	255,255,255,255	DHCP	OHCP NAK - Transaction ID 0x41d06f2d
44950	21632.710412	Elitearo 40:b	Eliteoro 40:b4:9d		SLL	Sent by us
44951	21632.715587	192, 168, 1, 1	WestellT af:09:0a	192, 168, 1, 18	DHCP	DMCP Offer - Transaction ID 0x31b06b2d
64952	21632.716785	Fliteoro 48:b	Elitegro 40:b4:9d		SLL	Sent by us
44953	21632, 721885	192, 168, 1, 1	WestellT af:69:00	192, 168, 1, 18	DHCP	OHCP ACK - Transaction ID 0x31b06b2d
44954	21632.006064	192, 168, 1, 18	Eliteoro 40:b4:9d	224.0.0.22	IOPP	V3 Membership Report / Join group 224.0.0.25
44967	21632.997584	192, 168, 1, 18	Elitearo 49:54:9d	224.0.0.251	MONS	Standard query TXT Remote Access on ANP. sft
44468	21633.025035	192, 168, 1, 18	Elitearo 40:b4:5d	224.0.0.251	Mins	Standard query PTR 18.1.168.192.in-addr.arpa
44160	21633,100209	192 168 1 18	Elitearo 40:b4:5d	224.0.0.251	MONS	Standard query ANT d.9.4.b.0.4.e.f.f.f.5.5.7
	21633,166074		Elitegro 40:b4:9d		MONS	Standard query response PTR ssh. tcp.local
	21633.211976	fw90:::207:95f	Elitegro 40:b4:9d	ff82::16	IOPv6	Multicast Listener Report Message v2
	21633 356043		Elitearo 40:b4:50		Mins	Standard greny ANT d.9, 4, b. 0, 4, c. f. f. f. 5, 9, 7

• Then use it for further analysis



Information Security

17

### 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

# 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: <a href="https://nvd.nist.gov">https://nvd.nist.gov</a>
- 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-bighack-how-china-used-a-tiny-chip-to-infiltrate-america-s-topcompanies

Information Security

18