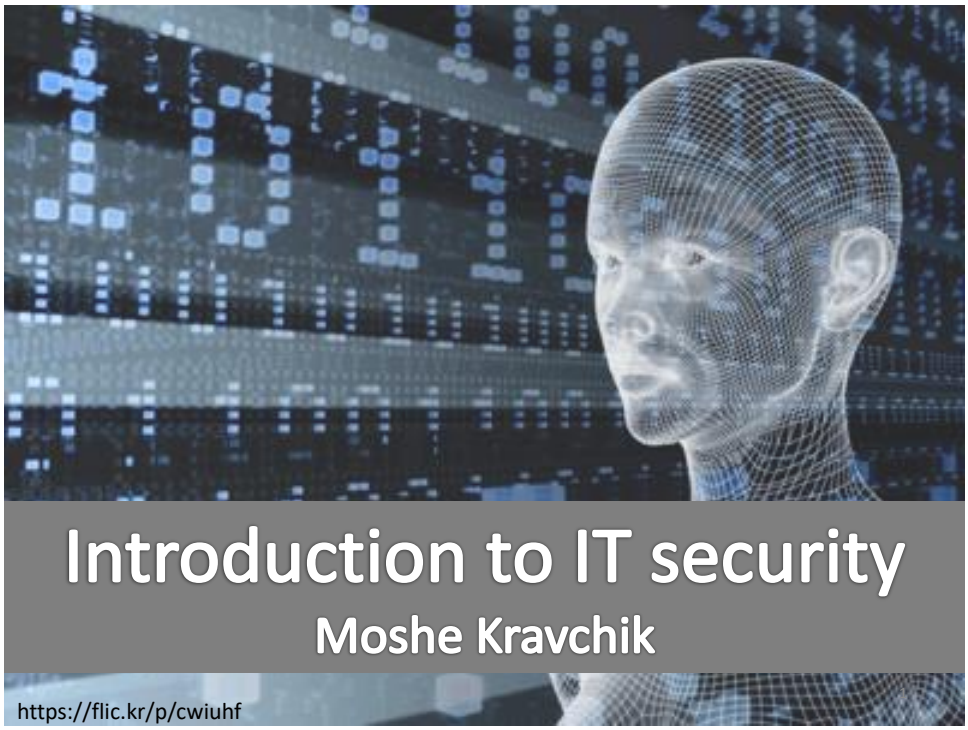


1

Agenda

- What is this course about?
- Course logistics
- Cybersecurity around us
- Attacks and attackers
- Targets
- Attack surfaces
- CIA

2

What is this about?

- Why should I care?
- Who are you?
- What will I learn here?

https://flic.kr/p/nMJNS

3

3

Will do

- Getting into security "set of mind"
- Know your assets & enemies
- Cybersecurity concepts
- Vulnerabilities and defensive programming
- Learn to build secure systems

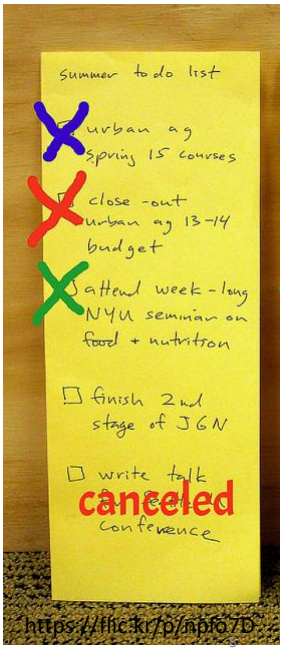
https://flic.kr/p/2AgUBJ

4

4

Will not do

- Algorithms and details of implementation
- Hands-on systems hacking
- In depth coverage of cryptography, systems and software security, network security
  - There are courses for the survivors!



https://flic.kr/p/npfo7D

5

Course logistics

- 13 lectures
- Exercises, class and home
- Final grade: 70% exam, 30% exercises
- Homework will require external reading and some programming
- … and creative mind!
- Book: Stallings & Brown

https://flic.kr/p/bfeZ8

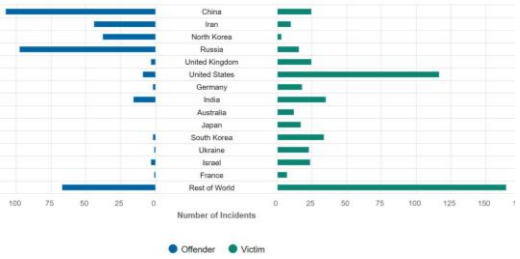
6

6

Cybersecurity today: 2019-today

- **12 2019.** Chinese hackers used custom malware to target a Cambodian government organization
- Unknown hackers stole login credentials from government agencies in 22 nations across North America, Europe, and Asia
- Russian government hackers targeted Ukrainian diplomats, government officials, military officers, law enforcement, journalists, and nongovernmental organizations in a spear phishing campaign
- **10 2019** India announced that North Korean malware designed for data extraction had been identified in the networks of a nuclear power plant

https://goo.gl/u8ZGGE



An Israeli cybersecurity firm was found to have sold spyware used to target senior government and military officials in at least 20 countries by exploiting a vulnerability in WhatsApp.
Iranian hackers targeted more than 170 universities around the world between 2013 and 2017, stealing $3.4 billion worth of intellectual property and selling stolen data to Iranian customers.

9

9

Cybersecurity ~~tomorrow~~ today

- What ~~will be~~ is on stake
  - Connected Cars
  - Internet of Things
  - Smart homes
  - Health
  - Traffic
  - Infrastructure
  - SCADA
- Lots of jobs!

10

10

Attacks and Threats

- Cyber threats same as physical
- … and very different
  - Automation
  - Scale
  - Remote
  - Distribution

11

11

Attacks motives - Criminal

- Criminal attacks – gain from abusing the system
- Fraud
- Destruction
- Theft
  - Money
  - IP (Software, games, Videos, Music)
  - Identity
  - Brand
- Ransom

12

12

Attacks motives - Privacy

- Targeted attacks
- Data Harvesting
- Surveillance
- SIGnal INTelligence
- Massive Electronic Surveillance - ECHELON, NSA, PRIZM, …

January 2018. The Unique Identification Authority of India and its Aadhaar system are hacked by unknown actors, resulting in the personal data of more than 1 billion people being available for purchase.

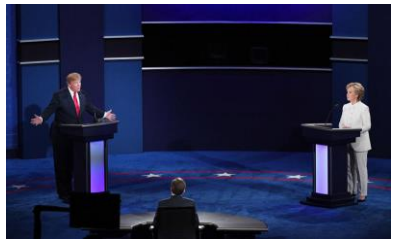
https://goo.gl/B1JXgH

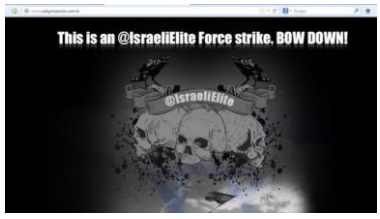
13

13

Attacks motives - politics

- Hacktivism
- Anonymous
- Syrian Electronic Army
- OpIsrael
- Elections influence





Russian military stole information of 500,000 voters

Eleven of the Russians are charged with identity theft, conspiracy to launder money and conspiracy to commit computer crimes. Two defendants are charged with a conspiracy to commit computer crimes.

https://goo.gl/EWziFv

14

14

Attacks motives - Publicity

- Temple of Artemis
- Fame (Geohot: jailbreak, PlayStation, Android)
- Attention to security problems

15

15

Attackers profile importance

- Need to understand for building effective protections
- Difference in
  - Technical level
  - Time and money investment
  - Level of risk

16

16

Attackers, uncovered

- Hackers
  - Stallman at MIT
  - White, Black and Grey hats
  - High skills, low money, low risk
- Lone Criminals
- Malicious insiders
- Industrial espionage

17

17

Attackers, uncovered

- Organized Crime
- Terrorists
- National Security Organizations
- Cyber warriors

https://goo.gl/pNQV58 https://twitter.com/FBI/status/1226896376971300865

18

Cyber arms for sell

NSO Group / Q Cyber Technologies

Over One Hundred New Abuse Cases

October 29, 2019

The May 2019 WhatsApp Incident

Under the Breach
@underthebreach

Actor selling IOS 0day exploit chain.
includes:
1.Safari RCE
2. LPE - Kernel vulnerability
3. Jailbreak

Price : 2,000,000 Euros

https://twitter.com/underthebreach/status/1231830863362609154

19

19

Attack surfaces

- Consider everything from physical to human
- End-to-end
- The weakest link

https://goo.gl/PqSo74

20

20

Hardware attacks

- NSA backdoors in routers
- Cold boot attacks on Samsung phones
- Row hammer
- EMP

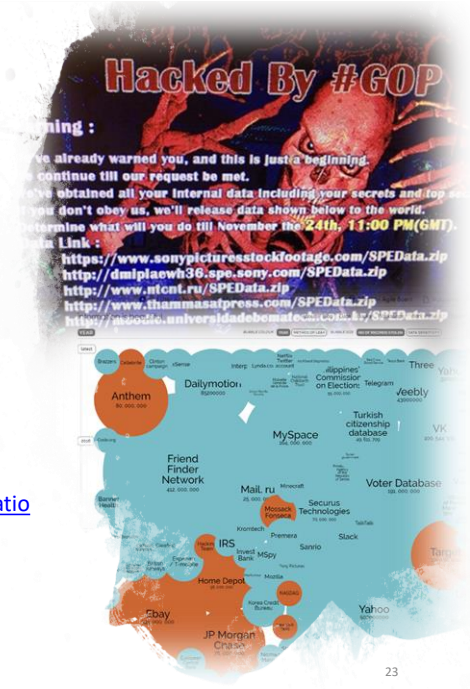
21

Software: OS and apps attacks

- Vulnerabilities and exploits
- Malware, viruses and trojans
- RATs

22

Data attacks



- Data leakage
- Data inference

https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

23

23

Network attacks

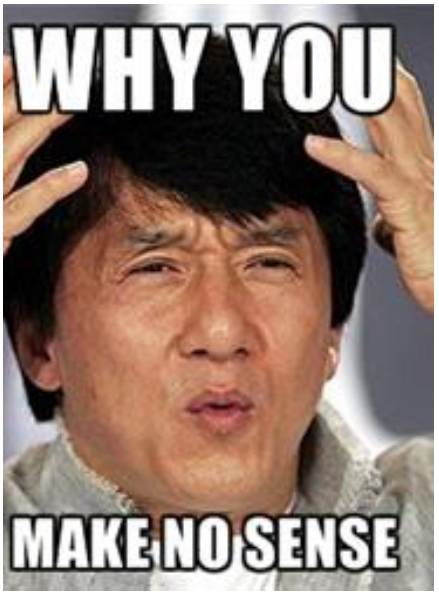
- Eavesdropping and tampering
- Denial Of Service
- Remote code execution

24

24

Human factor

- Misunderstand risks
- Security vs. Usability (passwords)
- Misunderstand security
- Malicious



25

25

Social Engineering

- Kevin Mitnick
- Much easier than technical
- Exploits people trust and unawareness
- Mostly done remotely
- Mass social engineering
- Used by malware

North Korean hackers infiltrate Chile's ATM network after Skype job interview

Redbanc employee applied for a LinkedIn job and got a call from the world's most active hacker crews.

https://goo.gl/BsLWHP

26

Israel and cybersecurity

- One of the world leaders
- Startups, incubators and research centers
- תוכנית לוחמת סייבר
- תקנת 357 של בנק ישראל
- משפט "האנלייזר"
- המרכז הלאומי לסיוע בהתמודדות עם אירועי סייבר (CERT-IL)

CIA - Confidentiality

- Confidentiality – preventing unauthorized reading of data
  - Prevent Eve from reading Bob's letters to Alice
  - Some also extend it to all kinds of access, including knowing that the data exists
  - Privacy
  - Cryptography is widely used for that

https://flic.kr/p/8xzAnc

Integrity

https://goo.gl/34vEKm

- Integrity – preventing unauthorized change of data
- Sum of the check, medical prescriptions, Nuclear commands – how to verify them?
- Photos, videos – digital data is so easy to change…
  - Russian IRA spreading fake news about French Yellow Vests
- Non-repudiation
- Cryptography is widely used for that

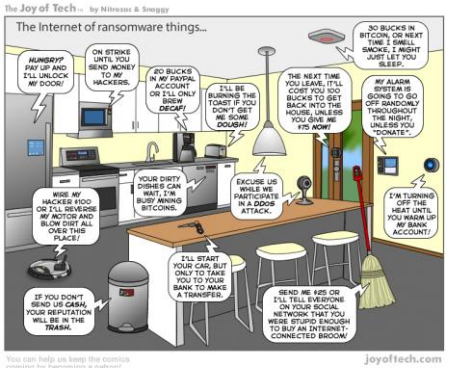
https://goo.gl/5vYRcv

29

29

Availability

- Data or service is available in a timely manner when needed
- Denial Of Service attacks
  - Demonstration and strikes are real life examples
- Servers, antiviruses, CPU



30

30

AAA

- (Did we forget something?)
- CIA extensions for operations over data
- Authentication, Authorization, Accountability
- Audit, Assurance, Anonymity, …

31

31

Terms Learnt

- Asset
- Threat
- Attacker
- Attack surface
- Vulnerability
- Exploit

- Confidentiality
- Integrity
- Availability

32

32

33

Summary

- Cybersecurity is vital for our society's today and tomorrow
- Who might attack you and why
- How can they do it?
- Confidentiality, Integrity, Availability
- Now go and study!

34