Avi's Notes: Make sure to read this in tandem with the 1st lecture slides!

Ubuntu Linux – need to install on your computer and get it working

- Professor doesn't care if you do it via VM, dual boot, WSL, remote desktop into a computer with ubuntu etc.
- Just get it running

Intro:

- Main ideas of topic
- Doesn't go into specifics (we have other more advanced courses for that)

Cyber Security

- Everything relates to computers
- If you aren't protected = expect attacks to occur

CIA – will discuss later

General idea of cyber security:

- Protect from attacks
- Give a perspective on programming for security aspects

Security Mindset (Slide 4):

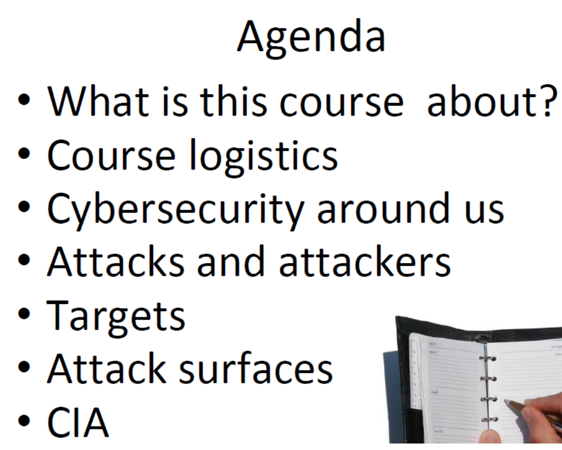
- Know our assets and enemies
- Cybersecurity concepts
- Vulnerabilities and defensive programming

Won't cover in course:

- Algorithms and implementations
- Hands on hacking
- Cryptography (other courses cover this in depth)
  - Will still have a few lectures on this subject
  - Course on its own
- System software security
  - Course on its own
- Network security
  - Course on its own

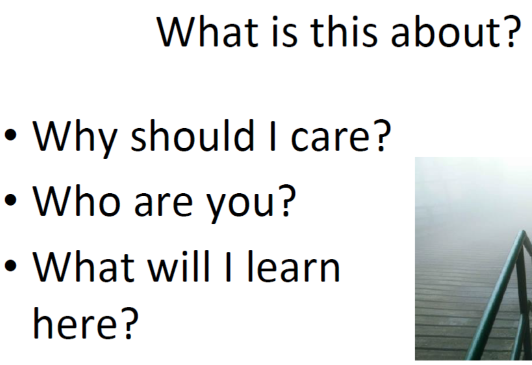
Cybersecurity today

- Hackers
- Stuxnet
  - Watch the 0-day movie (optional but informative)



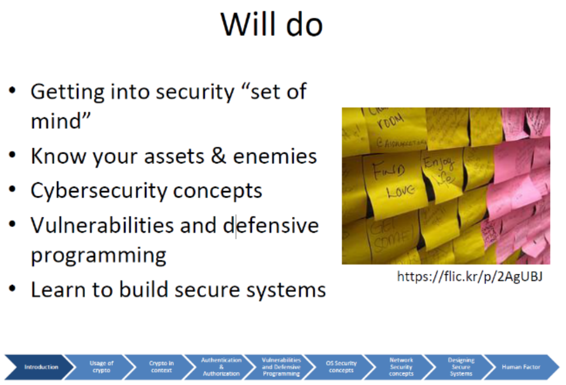
Agenda

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



What is this about?

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

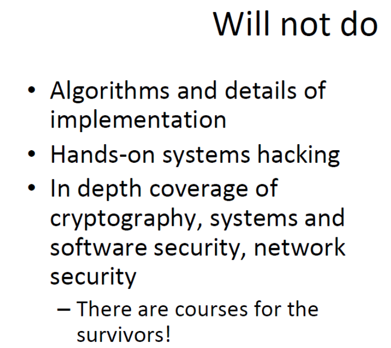


Will do

- 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

Introduction
Usage of crypto
Crypto in context
Authentication & Authorization
Vulnerabilities and Defensive Programming
OS Security concepts
Network Security concepts
Designing Secure Systems
Human Factor



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!

- NSO Group
  - 0 day vulnerabilities
    - Sold tool called Pegasus, to extract info from devices, to governments
- Targets
  - Cars, Internet of Things, Health Dept. Traffic Lights, infrastructures, SCADA (PLC – controllers)

Attacks and threats

- Physical
  - Unplugging server
  - Robbing a bank
- Cyber
  - Virtual
  - From home
  - Low risk
  - Anywhere
  - Easier to conceal (hide)
  - **Automation**
  - **Scale**
  - **Remote**
  - **Distribution**

Motives

- People wanting free software and games, Power, Theft, Revenge**, Fame, Money**, Fraud, Destruction
- **Identity (Fake brand), Ransom, politics**

Privacy

- Snowden: NSA -> too much surveillance (lack of privacy)
- Easy to gather info online

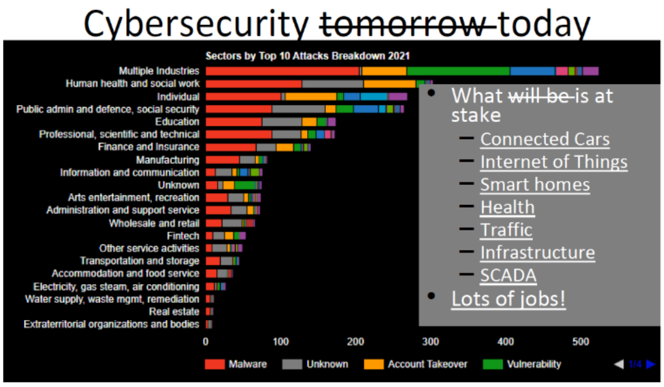
Politics

- Hacktivism
  - Using cyber tools to influence people
    - Send message, demands
  - Opisrael
    - Anonymous attack Israeli sites
  - Syrian Electronic Army
  - Russians influencing elections
  - Russians attacking Ukrainian infrastructure

Publicity

- Self promotion
- Fame
- Draw attention to security problems
- Potential to get a job

- **12 2021.** Hackers targeted multiple Southeast Asian governments over the past 9 months using custom malware linked to Chinese state-sponsored groups. Many of the nations targeted are currently engaged in disputes with China over territorial claims in the South China Sea.
- **10 2021.** Hackers leaked data and photos from the Israeli Defense Ministry after gaining access to 165 servers and 254 websites, overall compiling around 11 terabytes of data.
- **9 2021**. The EU formally blamed Russia for its involvement in the 'Ghostwriter' cybercampaign, which targeted the elections and political systems of several member states. Since 2017, Russian operators hacked the social media accounts of government officials and news websites, with the goal of creating distrust in U.S. and NATO forces.



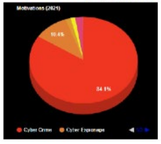
Cybersecurity ~~tomorrow~~ today

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

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

Attacks motives - Criminal

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



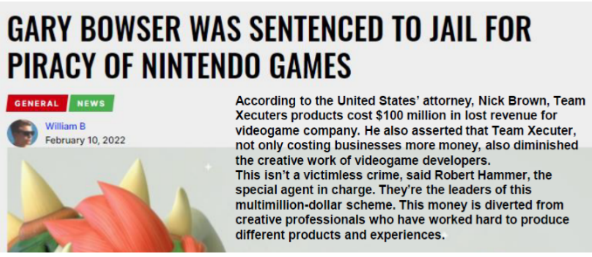
Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers

The payment clears the way for gas to begin flowing again, but it risks emboldening other criminal groups to take American companies hostage by seizing control of their computers.

Vehicles lining up on Thursday for gas at a Costco in Raleigh, N.C. President Biden urged Americans to avoid hoarding gasoline, and he warned stations not to engage in price gouging. Travis Long/T shorturl.at/kFNS1 ociated Press

Attacker profile

- Tech level
- Time and monetary investment
- Level of risk
- Build protections
- Big organizations can conduct these attacks



GARY BOWSER WAS SENTENCED TO JAIL FOR PIRACY OF NINTENDO GAMES

GENERAL NEWS

William B
February 10, 2022

According to the United States' attorney, Nick Brown, Team Xecuters products cost $100 million in lost revenue for videogame company. He also asserted that Team Xecuter, not only costing businesses more money, also diminished the creative work of videogame developers.
This isn't a victimless crime, said Robert Hammer, the special agent in charge. They're the leaders of this multimillion-dollar scheme. This money is diverted from creative professionals who have worked hard to produce different products and experiences.

Defcon

- Annual hacker conference
- Lots of lectures on youtube
- Stallman at MIT
  - Activist
  - Hacker
  - Open source
- **White hat**
  - Good
  - Legal
  - Ethical
  - Pentests (usually)
- **Black hat**
  - Illegal
  - Hacking for bad
- **Gray hat**
  - Mixed
  - Not destructive
  - Exploit and find vulnerabilities but keep them for themselves

Attacks motives - Privacy

- Targeted attacks
- Data Harvesting
- Surveillance
- Massive Electronic Surveillance - ECHELON, NSA, PRISM, …
- NSO scandals in Israel and worldwide

November 2021 . A Russian-speaking group targeted the personal information of around 3,500 individuals, including government officials, journalists, and human rights activists. The group obtained access to private email accounts and financial details, and operated malware on Android and Windows devices.

The whistleblower
I can't allow the US government to destroy privacy and basic liberties
theguardian
AADHAAR

https://goo.gl/B1JXgH

15

Test is mostly multiple choice

- Example question: what are white, black, and gray hat hackers?

Attacks motives - politics

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

https://goo.gl/EWziFv

This is an @IsraeliElite Force strike. BOW DOWN!
@IsraeliElite

Russian military stole information of 500,000 voters

למען אוקראינה: האקרים שיבשו את
מערכת הרכבות בבלארוס כדי
להקשות על התקדמות הצבא הרוסי

קבוצת ההאקרים האקטיביסטים שמכנה את עצמה "סייבר פרטיזנים" התנתה
את הפסקת השיבושים בהתחייבות נשיא המדינה אלכסנדר לוקשנקו להפסיק
לסייע לחיילים הרוסים, המתכננים פלישה לאוקראינה. "רכבת בלארוס
בפקודתו של הטרוריסט לוקשנקו מאפשרת לחיילי הכיבוש להיכנס לאדמה
שלנו"

חדשות חוץ 25.01.22 13:14

High skills, low money , low risk

Lone criminals or malicious insiders (employees hurting their own company)

Industrial espionage

Attacks motives - Publicity

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

Another group:

- Organized crime (darknet)
- Terrorists
  - Use cyber
- National security organizations
  - Such as the NSA in the US
- Cyber warriors
  - Attack other countries
  - Generally referring to soldiers or a military

cyber arms for sale (selling hacking tools and exploits)

- NSO group sold attack tools
- RCE – Remote code execution
- Jailbreak
  - Hole in system
    - Use it to gain access into system

Weak links

- Holes in system
- Leads to widened attack surfaces
- Always will be there
- Can be human/physical (social engineering)
- Open window, just lets someone craw inside
- Cannot always protect against weak links

Secure code = lots of time and money investment

End to end

Find weak link

Hardware attack

- NSA adding backdoor into routers
- EMP
- Cold boot Samsung

OS and Apps

- Valuable exploits
- Malware, viruses, trojan which lets us gain access to the system
- RAT = remote admin tools
  - Sudo, root, admin
  - Find vulnerability -> exploit it -> get remote admin access

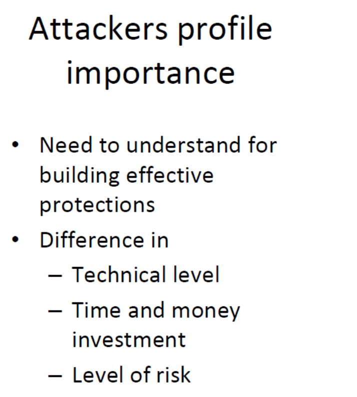
Data attacks

- Leaks
- Inference
  - Can find # of exploited user credentials

Network attacks

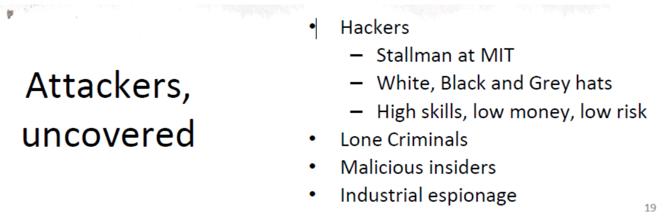
- Tamper or eavesdrop
- DDOS
- Remote code execute
  - Worst possible attack

Human factor



Attackers profile importance

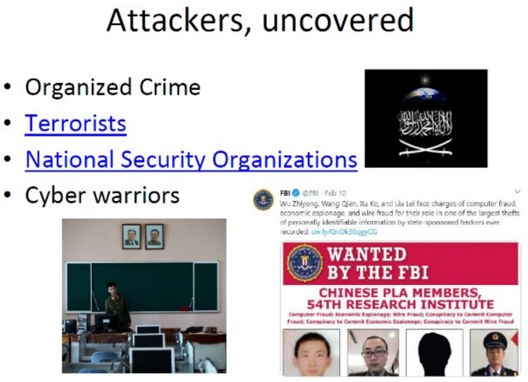
- Need to understand for building effective protections
- Difference in
  - Technical level
  - Time and money investment
  - Level of risk



Attackers, uncovered

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

19

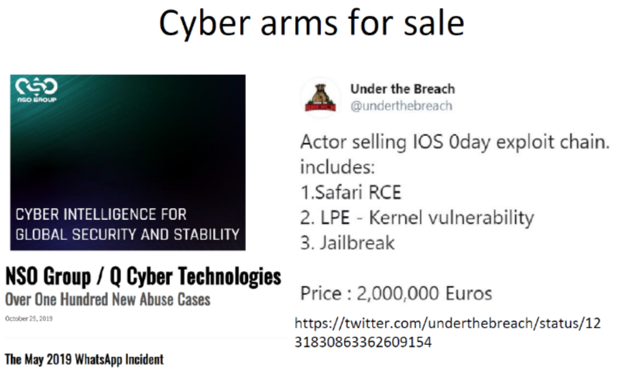


Attackers, uncovered

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

FBI @FBI · Feb 10
Wu Zhiyong, Wang Qian, Xu Ke, and Liu Lei face charges of computer fraud, economic espionage, and wire fraud for their role in one of the largest thefts of personally identifiable information by state-sponsored hackers ever recorded. ow.ly/QnOk30qgyCG

WANTED BY THE FBI
CHINESE PLA MEMBERS, 54TH RESEARCH INSTITUTE
Computer Fraud; Economic Espionage; Wire Fraud; Conspiracy to Commit Computer Fraud; Conspiracy to Commit Economic Espionage; Conspiracy to Commit Wire Fraud



Cyber arms for sale

NSO GROUP
CYBER INTELLIGENCE FOR GLOBAL SECURITY AND STABILITY

NSO Group / Q Cyber Technologies
Over One Hundred New Abuse Cases
October 29, 2019

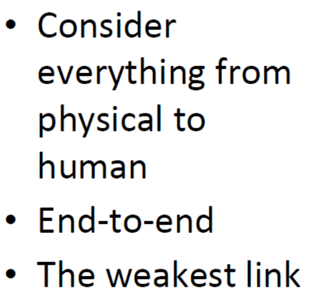
The May 2019 WhatsApp Incident

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



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

- Not aware of aspects of security (on programmer's head)
- Damage from programs
- Sec vs usability (passwords)
    - 2FA, etc.

Kevin Mitnick

- Famous for social engineering
    - Food people to thinking you are a technical changing password etc…
    - He runs a white hat company which social engineers people
    - Extract info from employees
    - Exploit peoples trust

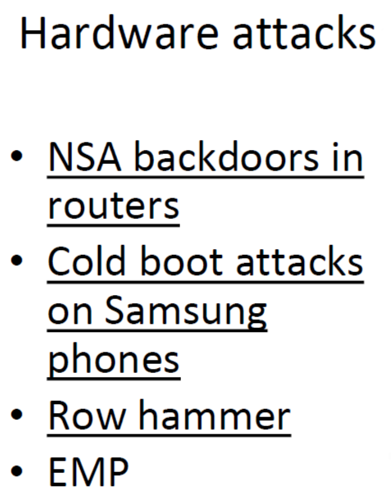
        Phishing emails

Israel

- Leading in cyber security
- Good banking regulations
- Army
- "the analyzer"
    - Young and famous hacker who got into nasa , pentagon, Knesset, air force,
    - Extract data and info
    - Banned from computers

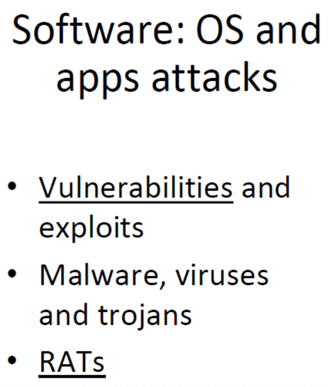
CIA

- Confidentiality
    - Prevent unauthorized reading of data
    - Privacy
    - Cryptography
        - Next 2 lectures
    - Access control
    - Bob sends message to alice but doesn't want eve hearing it
- Integrity
    - Stop people from changing data
    - Bank check, prevent user from adding a bunch of zeros in
    - Insert ingo into videos, change things
    - Non repudiation
        - Prove I actually sent this information
    - Cryptography
    - Confidentiality != integrity
        - See data but cant tamper
        - Or tamper data without seeing it
- Availability
    - Deny service to others (DOS)
        - Smart house (is a service)



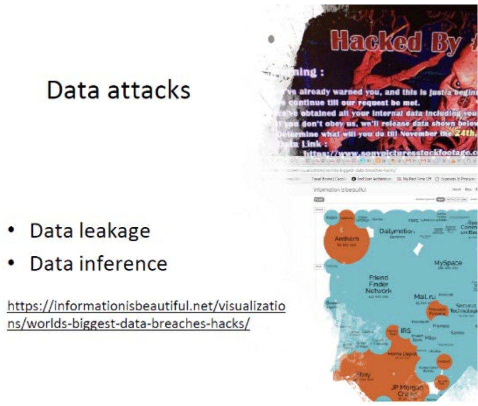
Hardware attacks

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



Software: OS and apps attacks

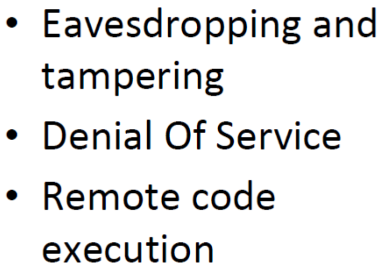
- Vulnerabilities and exploits
- Malware, viruses and trojans
- RATs



Data attacks

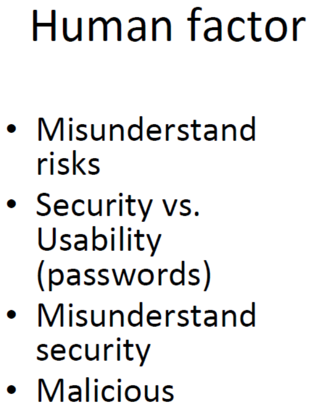
- Data leakage
- Data inference

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



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

  - Access controller and prevent access to others even without going into or hacking the system
  - Server, antivirus, cpu
    - Anti virus
      - Make it busy checking other programs, then slip by with your attack because its too busy
    - CPU
      - Can have it mine bitcoin or be full doing some arbitrary process
- AAA(add more)
  - Authentication
    - User verification
  - Authorization
    - Permissions
    - Is command given by authorized user
  - Accountability
  - Audit
  - Assure
  - Anonymize
    - TOR browser



Human factor

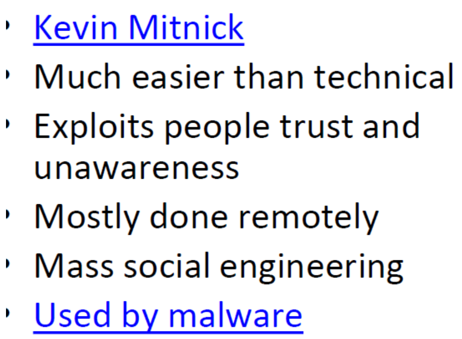
- Misunderstand risks
- Security vs. Usability (passwords)
- Misunderstand security
- Malicious

Cell hack

- Easier than hacking computers

Simulation is great

- Web attacks
  - A SQL injection for example
  - Read about it and get ideas
  - Then implement them too
  - If hard to simulation you can give a detailed description/account of the matter



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

Israel and cybersecurity

- One of the world leaders
- Startups, incubators and research centers
- תוכנית לוחמת סייבר
- של בנק ישראל תקנת357
- "האנלייזר"משפט
- המרכז הלאומי לסיוע בהתמודדות עם אירועי סייבר)CERT-IL)

cymotion
skyfence
mobile spaces
LetMobile
Shine
Dome
Skycure
HYBRID SECURITY
BIOCATCH
6scan
Sentropi
indeni
FORTSCALE
CYVERA
Sentinel
TheMarker
2020 Cybersecurity Ventu
United States
Israel
United Kingdom
Other countries
3%
8%
13%

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

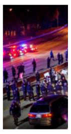
https://flic.kr/p/8xz/

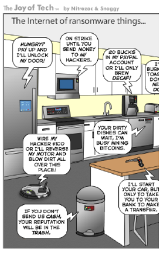
Integrity

- 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

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




The Joy of Tech by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.

AAA

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

Terms Learnt

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

- Confidentiality
- Integrity
- Availability

- 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!