CS310: Lecture 16

Device Security

Ravi Mittal

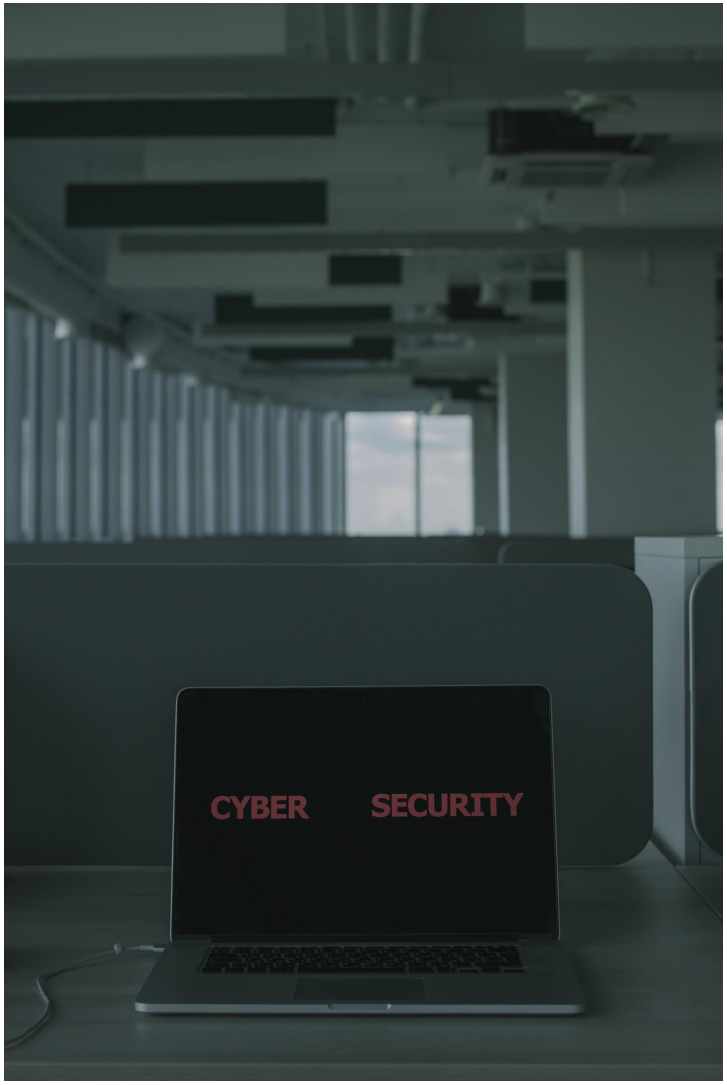


Photo by **cottonbro** from **Pexels**

Contents

- The Threat Attack Surface
- If you don’t see something does not mean it’s not there!
- Do you know that your devices are participating in DDOS attacks?
- Do you know your wifi router can steal and send your confidential information?
- Do you know malware in your mobile can clean up your bank account?
- Are Cyber threats limited to Money-Bank-Wealth?
- Every Device is becoming Smart
- Lots of Attack Scenario
- Why are devices not designed to be secure?
- Why is the Internet not designed to be secure?
- Device Security: What? How?

The Threat

Attack Surface

Unwanted resident Robber @ your home?

- Do you invite a thief to live in your home?
- Do you share your secrets to him/her?
- What do you do when you know that ..
  - The thief is looking at all your activities …
    - Your secrets..
      - Your bank account details..
      - Your emails
      - Your messages
      - Your transactions..
      - Your activities

- What action would you take…

  to get rid of the unwanted robber…?

Security – Traditional Way

- Valuables at home - Gold, Silver, cash
- Protection Mechanism
  - Lock
  - Locker
  - Window Grills
  - Neighbor hood watch
  - Dogs

- What is the Threat Attack Surface that is exposed to thieves?
  - Door, Windows, Locks, Backdoors etc
- Who are traditional thieves?
  - People from your village, City, Town..

Why should a thief work so hard to steal valuables from your home?

- Stealing from home is very risky affair for thieves..
- Why not use easy way?
- Why not rob you fully …
  - empty your bank account and credit card?
  - Steal your credentials?
- Why not record your personal conversations?
  - And ask you to pay money in lieu of recordings..
- Why not collect your credentials (user id, password, email address, home address, Aadhar Card number, Passport Number, PAN Number, Credit Card number, Debit Card number, Bank transaction password, ATM card number, ATM pin etc)?
  - And steal money and sell credentials in **Dark Web**

Oh.. My God… Who can rob me?

- Surely, you are not the target of local thief..
- You are targeted by Cyber Criminals from all over the world..
  - This is a business …
  - It's corporatized
  - It is happening at a grand scale
  - Many Governments are helping Cyber Criminals…
    - North Korea
    - And your friendly (or not so friendly) neighboring countries..
- Why should they not rob you.. If you allow them to… and your local police can't do anything..

Bots in your devices ?

- Did you check if there are (malicious) bots in your devices that are
  - Collecting your valuable information
  - Sending them to their masters – Cyber Criminals
- What are the chances that your devices have bots?
  - 0% ? Ok.. Are you sure?
- Which country has honor of having the largest number of bots (working for cyber criminals)?
  - Russia
  - USA
  - China
  - Brazil
  - India

Bots in your devices ?

- Did you check if there are (malicious) bots in your devices that are
  - Collecting your valuable information
  - Sending them to their masters – Cyber Criminals
- What are the chances that your devices have bots?
  - 0% ? Ok.. Are you sure?
- Which country has honor of having the largest number of bots (working for cyber criminals)?
  - Russia
  - USA
  - China
  - Brazil
  - **India (730755 bots)**

- Look at the link

https://www.spamhaus.org/statistics/botnet-cc/

The World's Worst Botnet Countries

Countries in this chart have the highest number of detected spam-bots as listed in the Spamhaus XBL zone. Most bots can be used for spam, phishing, click-fraud, DDoS and other malicious activities.

Many issues may relate to a country's bot density including technical, policy and socioeconomic factors.

Additional and more detailed statistics can be found at the Spamhaus CBL website:

CBL breakdown by Country

CBL breakdown by Country Traffic

CBL breakdown by Country Infections

CBL breakdown by Country Per Capita

Source: Spamhaus (XBL) database. Data is compiled automatically every 24 hours from the XBL database using the number of currently listed bots for each network (ISP/NSP).

India: Number of bot infected machines > number of Covid-19 infected people today)

The 10 Worst Botnet Countries

As of 21 September 2021 the world's worst botnet infected countries are:

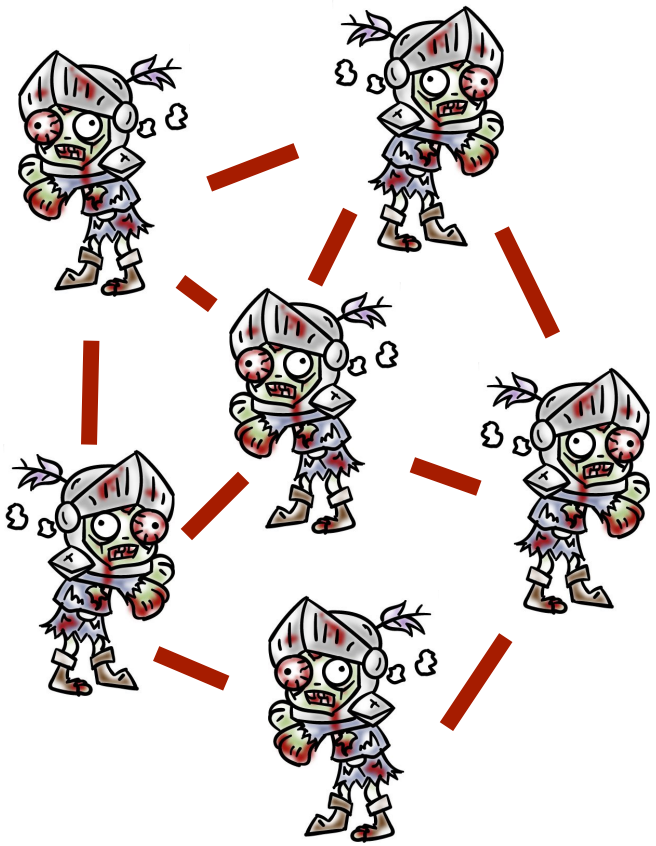
1	**India**	Number of Bots: 730755
2	**China**	Number of Bots: 701287
3	**United States of America**	Number of Bots: 479789
4	**Thailand**	Number of Bots: 354722
5	**Indonesia**	Number of Bots: 284472
6	**Viet Nam**	Number of Bots: 269487
7	**Brazil**	Number of Bots: 148079
8	**Algeria**	Number of Bots: 147398
9	**Pakistan**	Number of Bots: 123702
10	**Iran (Islamic Republic of)**	Number of Bots: 107285

If you don’t see anything doesn’t mean it’s not there

Botnet

- A network of (malware) bots controlled by an attacker to perform coordinated malicious activities

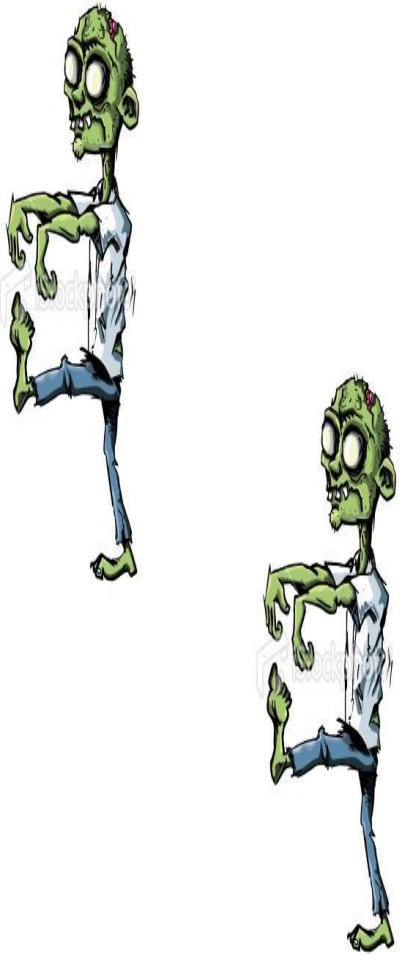
- A popular platform for most Internet-based attacks and frauds



Ref: Mustaque Ahmad and Wenke Lee, GTech

Places (in your home) where bots can live and work!

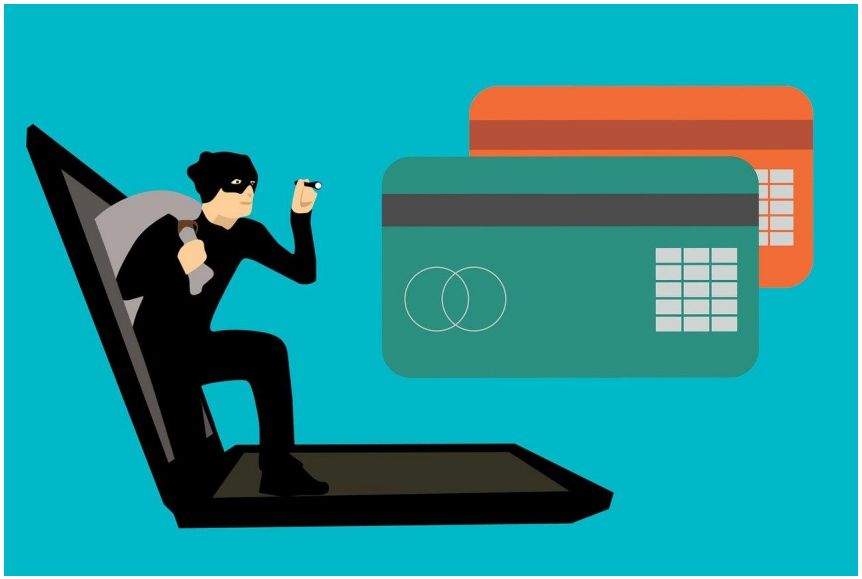
- Mobile phone
- Laptop, Desktop, iPad, Tablets
- Routers, Wifi routers
- Webcams, Digital Video Recorders
- Home security Systems
- Home Appliances: Refrigerator, Washing Machines, Ovens, Cameras, Heaters etc
- Cars
- Medical Devices for personal use
- Any device that is connected to Internet



So what ??

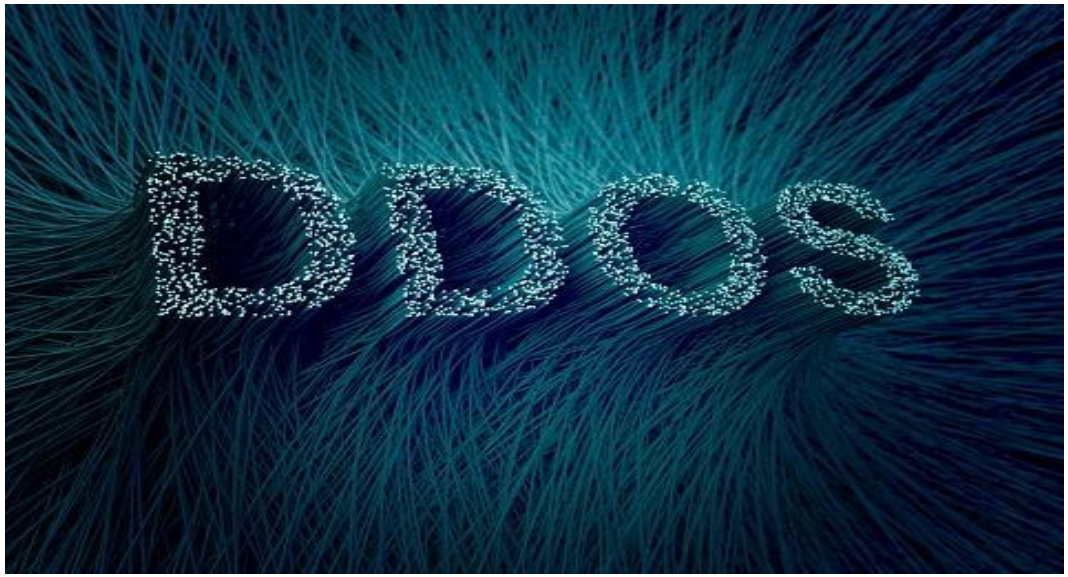
- Let malware or bot be there in my devices.. It doesn't matter to me..
- Oh.. No. It matters to all of us..

- Why?



From Pixabay

Do you know that your devices are participating in DDOS attacks



From Pixabay

Distributed Denial Of Service (DDOS) Attacks

Objective: Overwhelm target site with traffic.

Do you know that your wifi router can steal (and send) all your confidential information?

From Pixabay

Malware residing in your Router

- A malware bot sitting in WiFi router can see all of our transactions
  - Collects and sends your personal email address, passwords, bank details, our communication history and other information to the bot master
  - Modify router's DNS entries and so that your internet traffic is diverted to a phishing site
    - If you try to connect to your bank for a transaction, the malware can direct the request to fake phishing site which looks exactly like banking site..
    - When you try to do transaction, it can steal your credentials (passwords etc).. Now it can take out money from your bank.
- It can display inappropriate ads (eg porn ads)

Did you set password of your WiFi Router?

- Every smart device has a device (user) id and a password
- Routers come with default user id and password. Example:
  - User name : admin
  - Password: password
- Also, a WiFi router has WiFi channel id and passwords
  - For example I have created channel id (SSID): myrouter and set it's password (mypassword1234), so that my neighbors can't access my router
- Note that most of us have never set device's user id and password ..it remains default user id and password
  - Like leaving your home unlocked..
- So, there is a treat for cyber criminals

Do you know a malware in your mobile can

clean up your bank account?

From Pixabay

How ?

- Well check what all you do to transfer money from your bank using mobile phone !
- Which of the following your mobile phone doesn’t know?
  - Your name and credentials
  - Your account number
  - Money in the bank account
  - Account password
  - OTP sent

Your credit /debit card details may be in the Dark Net

70 Lakh Indian Credit and Debit Card Holders' Private Data Has Been Leaked Online

The data dump was reportedly posted in the Dark Web by unknown sources, and appears to be aggregated data that may have belonged to a third party banking partner operator.

- NEWS18.COM
- LAST UPDATED: DECEMBER 10, 2020, 17:55 IST
- FOLLOW US ON: Facebook Twitter Instagram Telegram Google News

Cyber Crime as a Service !

- You must have heard of
  - Platform as a service (PaaS)
  - Infrastructure as a service (IaaS)
  - Software as a Service (SaaS)
- Now, Cyber Crime as a Service in Dark Net
  - Sophisticated exploits and other malware for rent
  - Design and delivery of customized solutions
  - Rapid adaptation to defeat cybersecurity defences
  - Development of malware for niche market
  - Outsourcing of a complete cyber-enabled attack
  - Technical support for cybercrime activities
  - Robust and dynamic integration of stolen data
  - Minimal technical expertise required by customer

Cybercrimes are growing day-by-day ..

Ref: Standard Chartered Report on Cybercrime as a Service

Are threats limited to

Money – Bank – Wealth ?

Life is more important than money!

- A cyber criminal can invade
  - Personal medical devices eg. pacemaker, insulin pump, etc
  - Medical devices used for patient monitoring, Surgery ..

Medical Devices Hit By Ransomware For The First Time In US Hospitals

Medical device hijack

From Wikipedia, the free encyclopedia

There's A Virus Infecting Our Medical Devices With Identity Stealing Malware

How about Nuclear Power Plants?

Cyberattack Hits Indian Nuclear Plant

ARMS CONTROL TODAY

December 2019
By Melissa Robbins

The Nuclear Power Corporation of India Ltd. (NPCIL) confirmed on Oct. 30 that a cyberattack against the Kudankulam Nuclear Power Plant in Tamil Nadu had occurred in early September.

Monkey Cage • Analysis

An Indian nuclear power plant suffered a cyberattack. Here's wh you need to know.

Authorities don't seem to understand the real threat from cyber-operations.

REPORT

HACKING NUCLEAR SYSTEMS IS THE ULTIMATE CYBER THREAT. ARE WE PREPARED?

Nightmare scenario

By Sean Lyngaas | Jan 23, 2018, 10:48am EST
Illustrations by Alex Castro and William Joel

Power Sector facing 30 cyber attacks a day

How about Cyber Attacks on Aircraft?

MOTORS / AVIATION JANUARY 28, 2020

Cyber Pirates Are Hacking Business Jets to Steal Valuable Data and Money. Here's What You Should Know.

The danger of hacking doesn't end just because the wheels go up.

MOTORS / AVIATION JANUARY 28, 2020

Cyber Pirates Are Hacking Business Jets to Steal Valuable Data and Money. Here's What You Should Know.

The danger of hacking doesn't end just because the wheels go up.

Attack Surface for Aircraft is too big !

Ref: https://oatao.univ-toulouse.fr/19627

Every Device is Becoming Smart

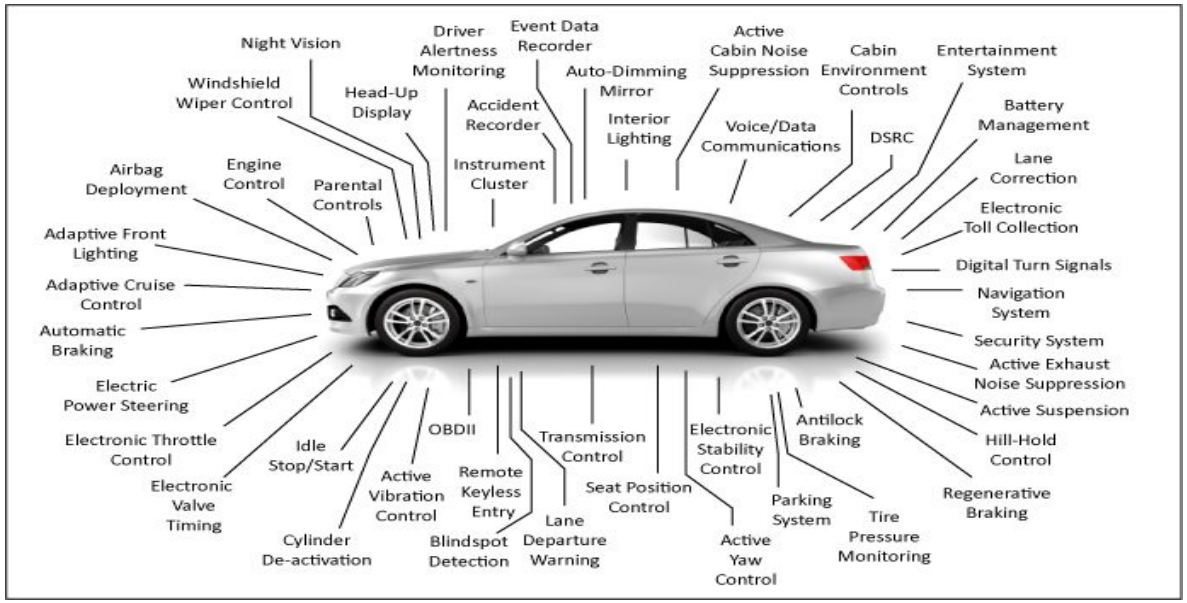
Thing □ Computer Thing

Every thing is becoming "Computer on the Internet"

- **Cars** □ Fully connected distributed system with 20 processors running 100 Million+ lines of code □ Local area network □ connected to Internet
  - **Cars** □ Computers that can move

Cars are coming with modern computers that are connected to cloud

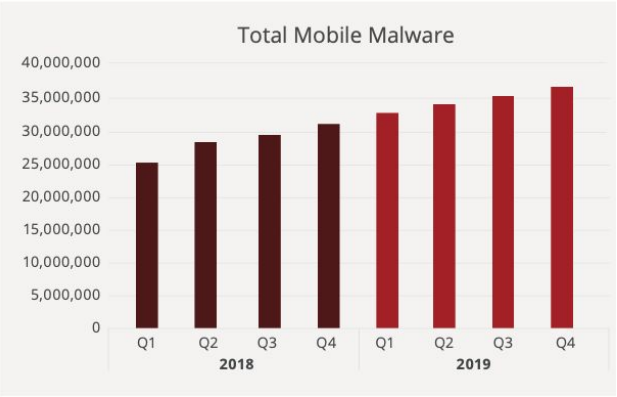
Can hackers disable your car's breaks?



Ack: chipsetc.com

Mobile Phone

- Mobile phone Computer that allows phone calls, shoot video, make transactions, make video calls, play music, read newspapers, exchange emails and instant messages, Internet device
  - It's really big computer – bigger than Supercomputer of 80's
  - Over 15 million lines of code
  - Easy to hack ; A large number of malware Apps



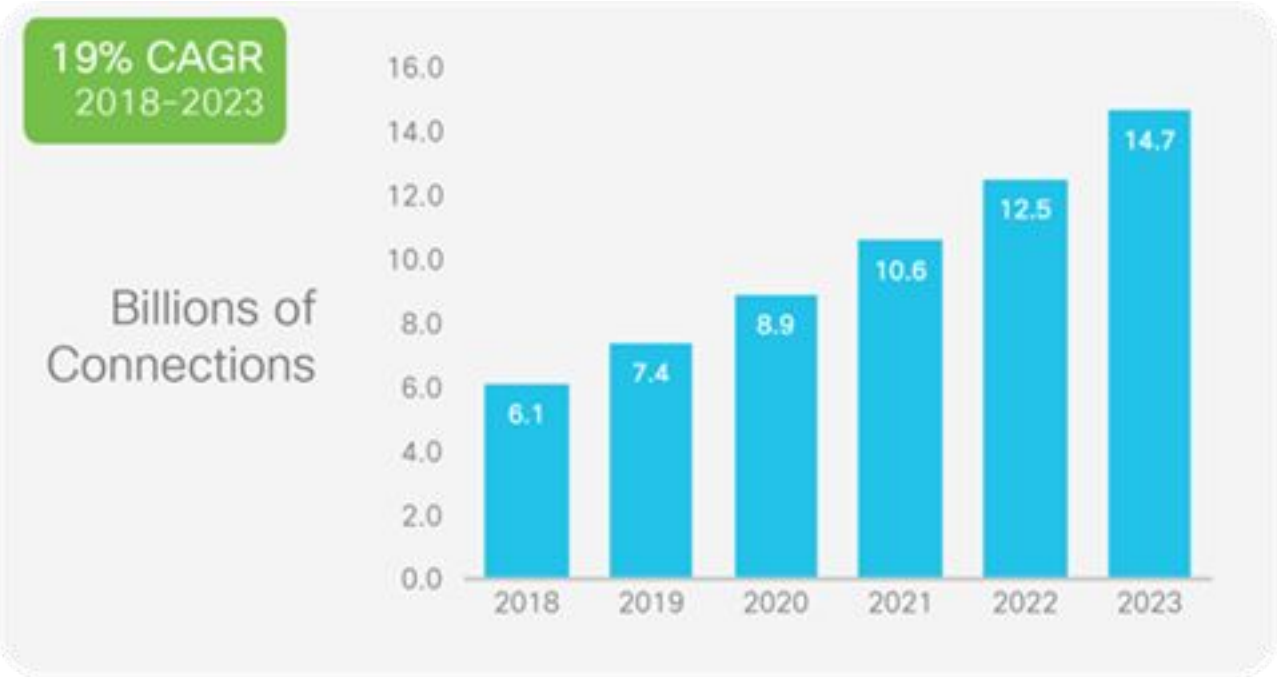
Ref: McAfee Mobile Threat Report

And Many more…

- Airplane Computer that fly - carry people and goods
- Refrigerator Computer that cools things down
- Microwave Oven computer that heats up
- House Lock Computer that locks doors
- Camera Computer with lens
- ATM Computer with money inside
- Modern light bulb Computer that gives bright light
- TV Computer that shows video program
- Washing machine Computer that washes clothes
- Voting Machines Computer that enables voting

Did you realize that your TV has power to participate in cyber crime?

Machine to Machine Connection



- IoT lets people, processes, data, and things to connect to each other
- There will be 1.8 M2M connections for each person by 2023

Source: Cisco Annual Internet Report, 2018–2023

New world of IoT

- Very soon, most of the devices in the world will have Internet connectivity
- Internet of Things (IoT) has four parts
  - Sensors: To collect data about environment
    - Smart thermostats, Street and highway sensors, Smartphones with their motion sensors and GPS location receivers, Industrial sensors
  - Processors and Memory: to store data and to figure out what to do with the data coming from sensors and users
    - Within individual devices and on Cloud
  - Actuators
  - The connecting network: The Internet
- IoT devices are often small, power constrained, memory constrained – easy to hack

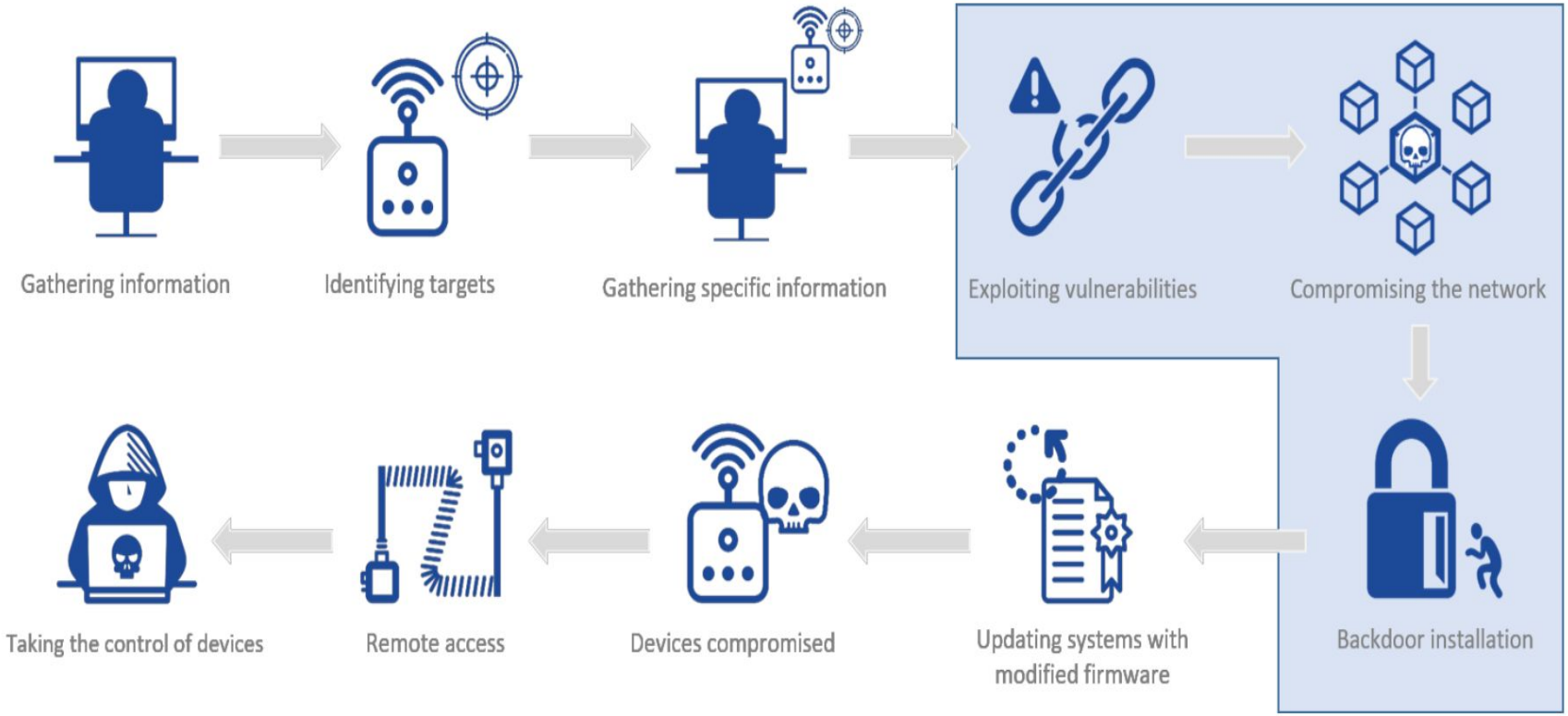
What is the impact of Hyper connectivity?

- Huge Attack Surface
  - the sum total of resources exposed to exploit
- Cyber criminals have choice where to attack
  - Asymmetric Advantage

Lots of

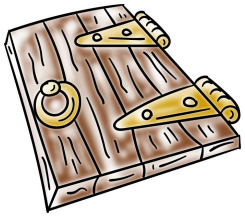
Attack Scenario

Steps in Cyber Attack



Ref: Enisa IoT Security Presentation

Threat Landscape – Malware, Exploit Kit, APT

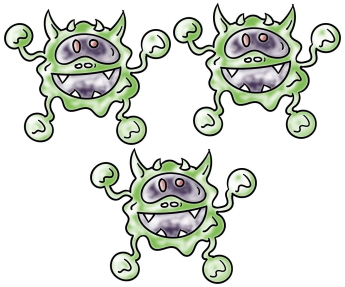


Trap doors or back doors

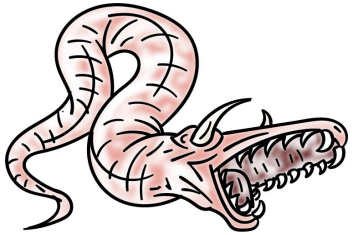
Logic bombs

Trojan horses

Botnet



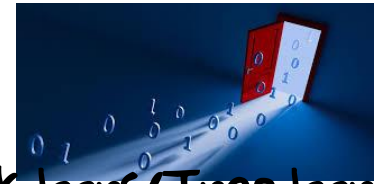
Viruses



Worms

APTs

Rootkit



Backdoors/Trapdoors

Spyware

Threat Landscape - Others

Ultrasonic Sensor Jamming

Ultrasonic Sensor Spoofing

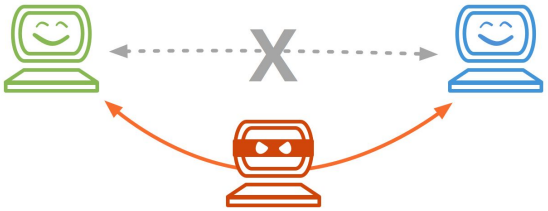
Software Security

Loss in Cloud

Unauthorized Access and Use

Phishing

IoT Protocol Hijacking



Man in the Middle

Protocol Vulnerabilities

Why are Devices not designed to be secure?

Designing Device to be secure !

- When we say Device Security – We mean security of the embedded computer
  - Secure Hardware and Secure Software
- Let's first ask: What is the incentive of designing secure hardware and software?
  - Do we ever ask these question when purchasing a device?
    - Is my mobile secure enough? Does it support hardware level encryption? Does it have enough feature for Internet security?
    - Do we try to find out if WiFi Router supports VPN or other security features?
  - Even if we know about security feature requirements, are we ready to pay extra money for security?
- Almost all users want inexpensive devices with full of features and high performance

Companies don't design secure devices..

- Designing and Developing Secure Devices is expensive
  - More effort is required in development, coding, and testing
- It's cheaper to develop poor quality software
- Software (code) size is continuously increasing
  - Common to find a few million lines of code in many devices
  - Modern car has over 100 million lines of code
- Reuse of code written by developers over decades
- Most of the code used in systems is, generally, of very low quality
  - Not tested fully – as it is very difficult to achieve 100% code coverage
- Companies have incentives to release product early (with thousands of known and unknown bugs)

Companies don’t design secure devices..

- Early release of a product is very important for commercial success
- It is impossible to test existing millions of lines of code + newly added code fully
- New addition to existing code (called extensibility) may cause quality and security issues in the device
- Low cost embedded (IoT) devices are, often, developed by small companies that don’t have capacity and capability to develop secure software
- Most of these devices don’t have any way to be patched
  - These devices are never patched with security bug fixes

Complexity is enemy of security

- More complexity Less security
- IoT Devices are becoming highly complex
- Complexity Not many people are able to understand more mistakes in design, development, maintenance, enhancements, and updates large “attack surface”
- Large attack surface huge advantage to attacker
- This makes Attacker’s job simple

Why is the Internet not designed to be secure?

The Internet

- The Internet ties different networks together
  - The ***Inter***net
- Different networking technologies may carry Internet data
  - Ethernet
  - GSM/GPRS data-channel may carry Internet Packets, 3G, 4G, 5G
  - TV cable may have one or more data-channels carrying Internet packets, in addition to regular TV channels
  - Telephone cable may carry Internet packets using ADSL technology
- Internet Networks carry different types of data contents
  - Data: File, Images
  - Voice
  - Video
  - Movies

Enormous diversity and dynamic range

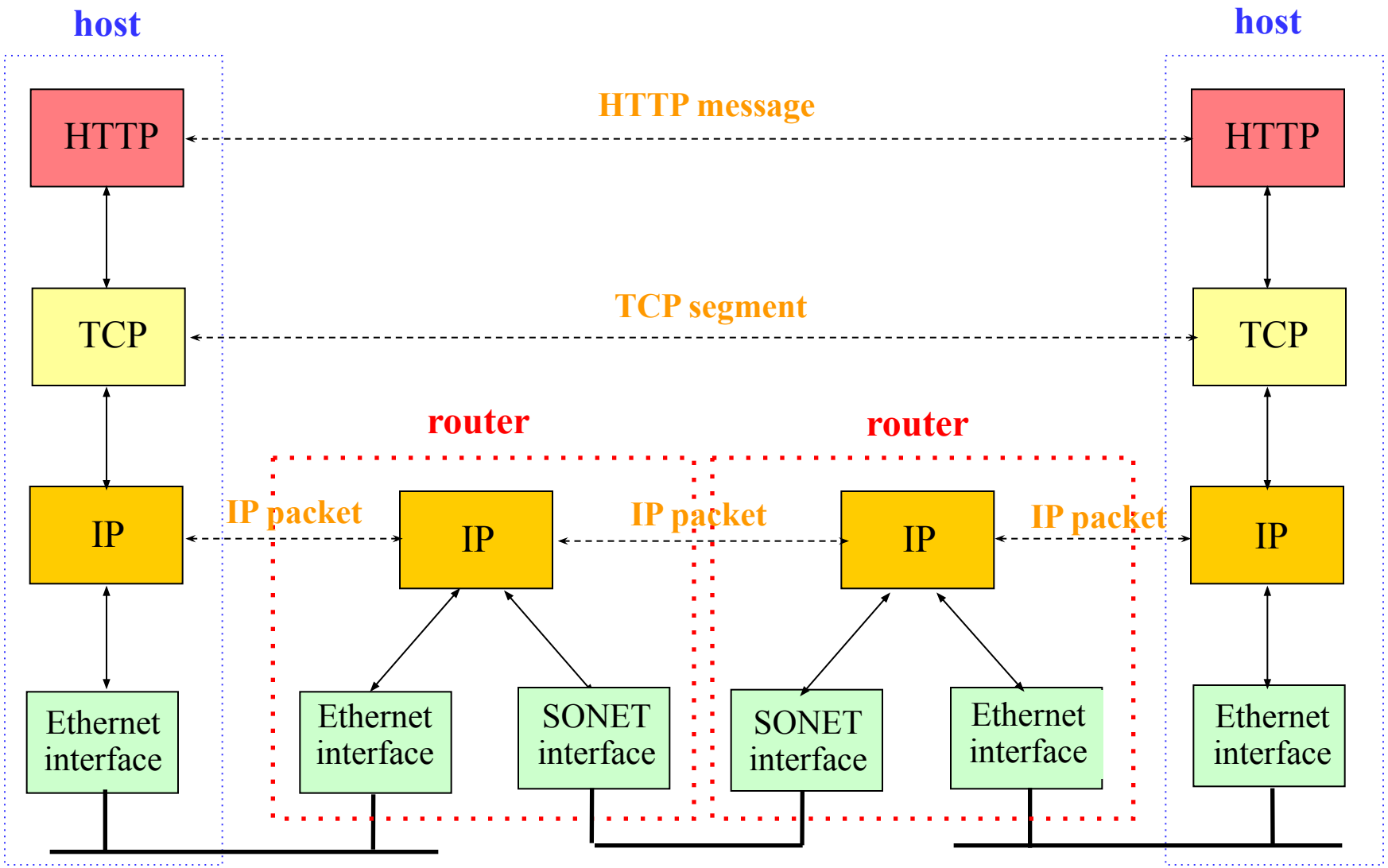
- Communication latency: microseconds to seconds (10^6)
- Bandwidth: 1Kbits/second to 100 Gigabits/second (10^7)
- Packet loss: 0 – 90%
- Technology: optical, wireless, satellite, copper,…
- Endpoint devices: sensors, cell phones, datacenters,…
- Applications: skype, live video, gaming, remote medicine,…
- Users: Everyone: a child (3-4 years) – Grandfathers (90 years), students, housewives, teachers, Government, Military, Operators, Thieves, Priests

Goals for the Internet

- Ability to connect many different networks
  - Ethernet, Optical and Wifi and ….
- Ability to scale to entire world
- Ability to tolerate and recover from failures
  - Which are inevitable…
- Able to support wide variety of applications

There is no goal for secure communication!!

The Internet Layering Model

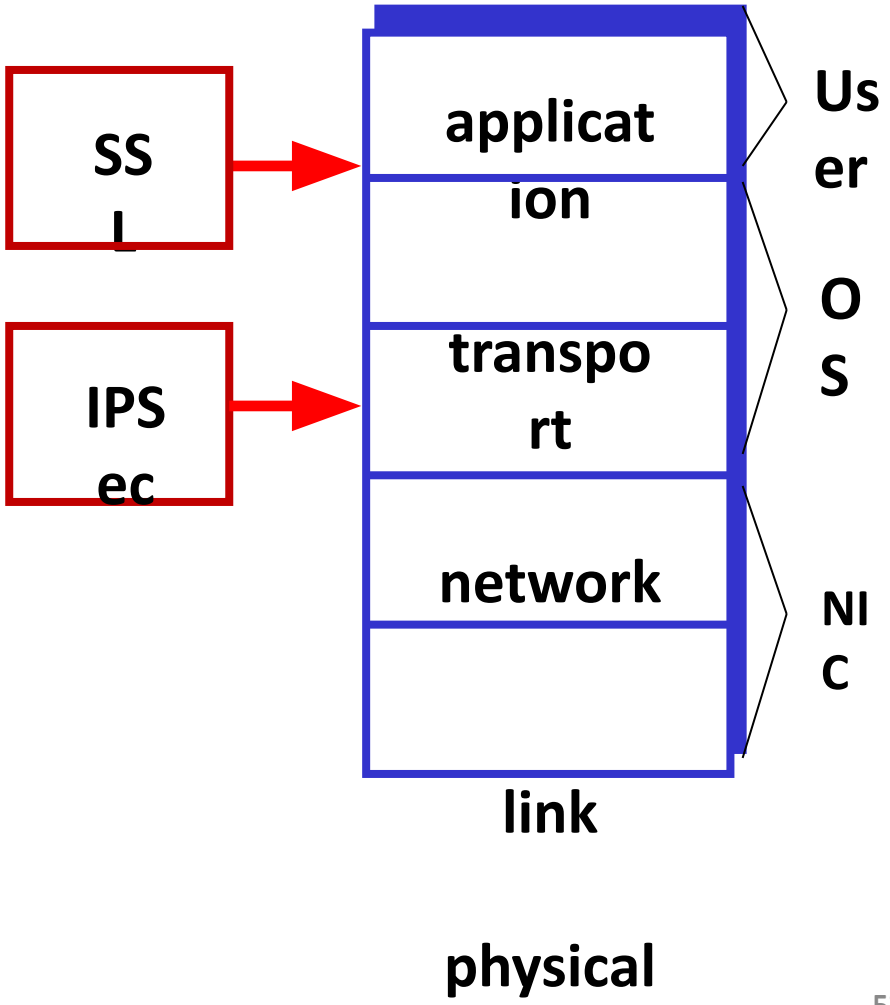


How about Security ?

- Is there any layer corresponding to security?
- Does network layer bother about not transmitting evil person's packets?
- Where will security functions fit into?
- How about physical and DL layer security?
- Can someone change routing protocol thus forcing traffic to pass through own's router?
- Can you encrypt header information?
- It's distributed system with no centralized control
- The Internet by itself provides raw data communication mechanism – without any built-in security
- **The Internet is NOT designed for security**

The Internet Security

- Internet security then leads to
  - Security of end applications
  - Security of some of it's components eg BGP router
- Internet Security Protocols
  - IPSec
  - NAT and Firewalls
  - SSL and TLS



Device Security

What? How?

IoT Security Techniques

- End-point Security
  - Use tools/solutions: Antivirus, anti-malware, firewalls, and intrusion prevention and detection systems
- Use of Security Protocols: IPSec/SSL, TLS, WPA, HTTPS, VPN, Tunneling and Encryption algorithms
- Authenticate Devices
  - Digital Certificates, Biometrics, Two-factor authentication etc.
- Use Data Encryption
  - Symmetric Encryption
  - Asymmetric Encryption: Public Key Cryptographic solution for IoT
    - Public key and Private key generation
- Development of Secure Applications
- Awareness of latest threats
- Regular maintenance (eg patching) of devices and software

How to protect oneself from Cyber Threats? (1/3)

- Set strong passwords
  - At least 8 characters long with combination of digits, capital letters, small case letters and special symbols
- Don’t use the same password in multiple accounts
- Change password frequently (at least once in 3 months)
- Set two step verification in Google and other accounts
- Set device passwords in every device on the Internet
  - WiFi Router
  - Security Camera, etc
- Update device software frequently
  - Make sure the device is running the latest software release
- Use Internet Security Suite in Laptop, Desktop, Mobile, and Routers

How to protect oneself from Cyber Threats? (2/3)

- Use VPN
  - It doesn't cost much
- Use https (instead of http)
  - As this enables end-to-end encryption
  - Use https (or tls) specially when downloading firmware updates
- Don't visit malicious websites
  - Websites that attempts to install malware (often look like legitimate websites). These websites may ask you to install a software (obviously containing malware)
- Don't install codecs unless you are sure about their origin
- Don't open emails from unknown sources that looks suspicious
- Don't open email attachments unless the email comes from known sources

How to protect oneself from Cyber Threats? (3/3)

- Disable ancient protocols from your machine: ftp, telnet
- Secure sensitive information
  - Don’t hardcore secrets such as user name, password, etc
  - Don’t keep user ids/passwords in google drive or google photo
- Don’t keep your personal information (name, birthday, address, photo, Id card number, mobile number etc) on social media websites (eg Facebook)
- Replace credit/debit cards once in a year

References

- Introduction to IoT Security, Christina Skouloudi, Apostolos Malatras | ENISA IoT Security team ENISA-FORTH NIS Summer School, enisa, 2018
- Bruce Schneier Blogs on Security, https://www.schneier.com/
- Presentation ppt slides from Udacity course ”Introduction to Information Security” by Mustaque Ahmad and Wenke Lee
- Ppt from Malware: Information Security, Principles and Practice, Book, Mark Stamp