Network Security Concepts

Bheemarjuna Reddy Tamma
IIT HYDERABAD

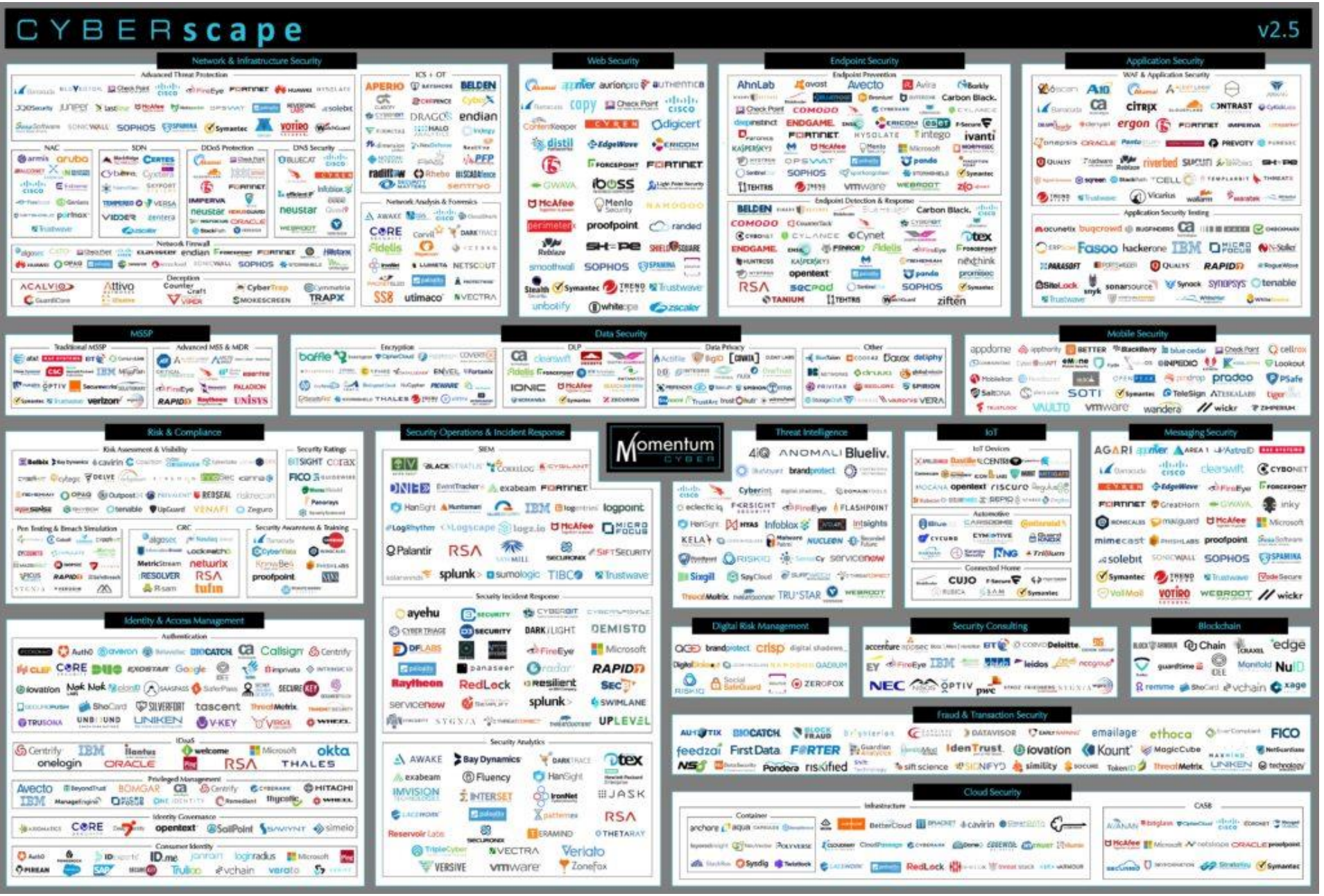
Credits: *Adapted from William Stallings textbook on Wireless Security, Kurose and Ross textbook on Computer Networking and based on slides/notes from Stefan Savage, Dan Boneh, Kirill Levchenko, Alex Gantman, Deian Stefan, Nadia Heninger, Alex Dent, Vitaly Shamtikov, Robert Turner, and a host of others and Internet sources*

The security problem

- **Lots of buggy software**
- **Social engineering is very effective**
  - Art of manipulating people so they give up confidential information
- **Money can be made from finding and exploiting vulnerabilities**

1. Marketplace for vulnerabilities
2. Marketplace for owned machines (Pay-Per-Install)
3. Many methods to profit from owned machines

current state of computer security



Source: Momentum Cyber

Definitions

Security

- The state of being free from danger or threat
  - The safety of a state or organization against criminal activity such as terrorism, theft, or espionage
  - Procedures followed or measures taken to ensure the security of a state or organization
  - The state of feeling safe, stable, and free from fear or anxiety

Cybersecurity

- The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this

https://en.oxforddictionaries.com/definition/security

Security (I) by RFC4949 (Internet Security Glossary)

- A system condition that results from the establishment and maintenance of measures to protect the system.
- A system condition in which system resources are free from unauthorized access and from unauthorized or accidental change, destruction, or loss.
- Measures taken to protect a system.
  - [Parker] System security involves 6 basic functions
    - Deterrence, Avoidance, Prevention, Detection, Recovery and Correction

"I" identifies a RECOMMENDED Definition of Internet Origin

https://tools.ietf.org/html/rfc4949

Cybersecurity by ITU-T X.1205

- Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.
  - Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.
  - Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.
  - The general security objectives are (CIA trinity)
    - Confidentiality
    - Integrity, which may include authenticity and non-repudiation
    - Availability

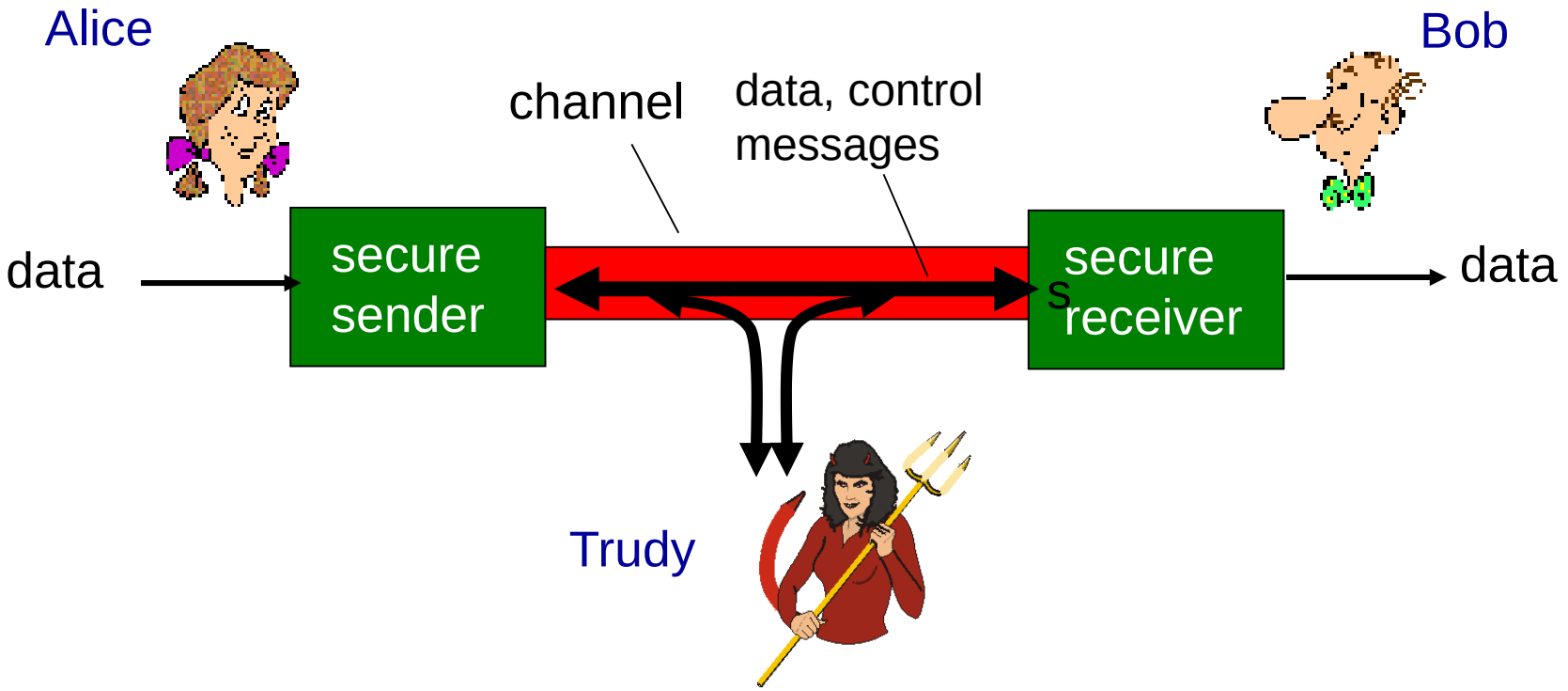
https://www.itu.int/rec/T-REC-X.1205-200804-I

Key elements of Cybersecurity

- Application security
  - Keeps software and devices free of threats
- Information Security
  - Protects integrity and privacy of data, both in transit and at rest (stored)
- **Network Security**
  - **Secures networks from intruders by controlling network connections**
- Disaster Recovery / Business Continuity Plan (BCP)
  - DR policy dictates how an organization recovers from a cyber attack that causes data loss or affects operations
  - BCP: Plan an organization falls back while trying to operate w/o certain resources
- Operational Security
  - Includes procedures for handling and protecting data assets
- End User Education
  - Addresses the most unpredictable cybersecurity factor: people!

Friends and enemies: Alice, Bob, Trudy

- Well-known in network security world
- Bob, Alice (lovers!) want to communicate "securely"
- Trudy (intruder) may intercept, delete, add/modify messages



Who might Bob, Alice be?

Real-life Bobs and Alices!

- Web browser/server for electronic transactions (e.g., on-line purchases) & web browsing
- On-line banking client/server
- DNS servers
- Routers exchanging routing table updates
- Remote access
- File transfers, video streaming, Emails, online chats, Skype, WhatsApp, Apps, etc.

There are bad guys (and girls) out there!

Q: What can a "bad person" do?

A: A lot!

- *eavesdrop:* intercept messages
- actively *insert* messages into connection
- *impersonation:* can fake (spoof) source address in packet (or any field in packet)
- *hijacking:* "take over" ongoing connection by removing sender or receiver, inserting himself in place
- *denial of service:* prevent service from being used by others (e.g., by overloading resources)

Security Trinity: *Confidentiality*

- The property that data is not disclosed to system entities unless they have been authorized to know the data.
- A breach of confidentiality means that someone gains access to information who should not have access to it
- In the context of network security, only sender and intended receiver should "understand" message contents
  - sender encrypts message & receiver decrypts message
  - concealing the quantity or destination of communication is called *traffic confidentiality*
- Not the same as privacy!
  - Privacy assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed
    - Some info we share voluntarily when filling online forms
    - We can be monitored throughout our lives easily by companies, governments and unknown entities in this digital age☹

Security Trinity: Integrity

- Data integrity: "The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner"
- In the context of network security, sender and receiver want to ensure message is not altered in transit without detection
- System integrity: "The quality that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation"
- Integrity also means ensuring information non-repudiation and authenticity
- Authentication ensures that you are really talking to whom you think you are talking.
  - It involves verification of sender/receiver using passwords/certificates
- Non-repudiation: someone can't repudiate (deny) something.
  - It ensures that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

Security Trinity: Availability

- The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system
  - i.e., a system is available if it provides services according to the system design whenever users request them
- Turning off a computer provides confidentiality and integrity, but hurts availability!
- Denial of Service (DoS) attacks are direct assaults on availability

More Definitions: Vulnerability

- A flaw in a software, firmware, hardware, or service component resulting from a weakness that can be exploited, causing a negative impact to the confidentiality, integrity, or availability of an impacted component or components
  - Vulnerabilities can allow attackers to run unauthorized code, access system information and steal, modify and destroy data
- Vulnerabilities in
  - Design or specification, Implementation , Operation & management
- Not every vulnerability results in an attack, and not every attack succeeds
  - Success depends on the degree of vulnerability, the strength of attacks, and the effectiveness of any countermeasures in use.
- **Exposure:** An error in code or a config issue that gives an attacker indirect access to a system/network for info gathering or hiding their activities

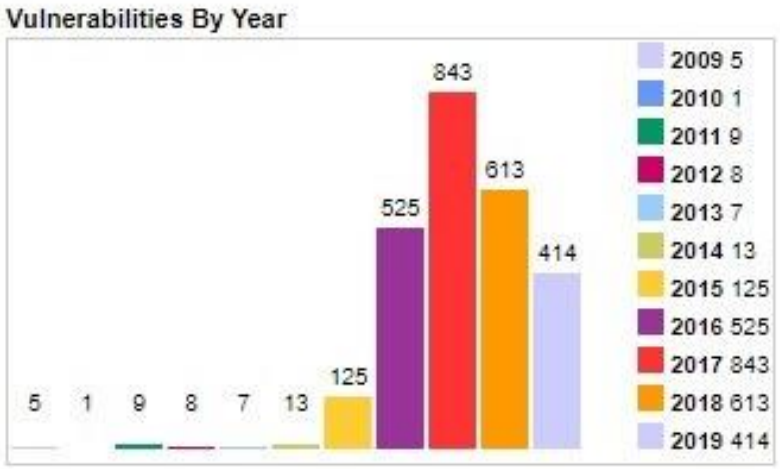
https://cve.mitre.org/about/faqs.html

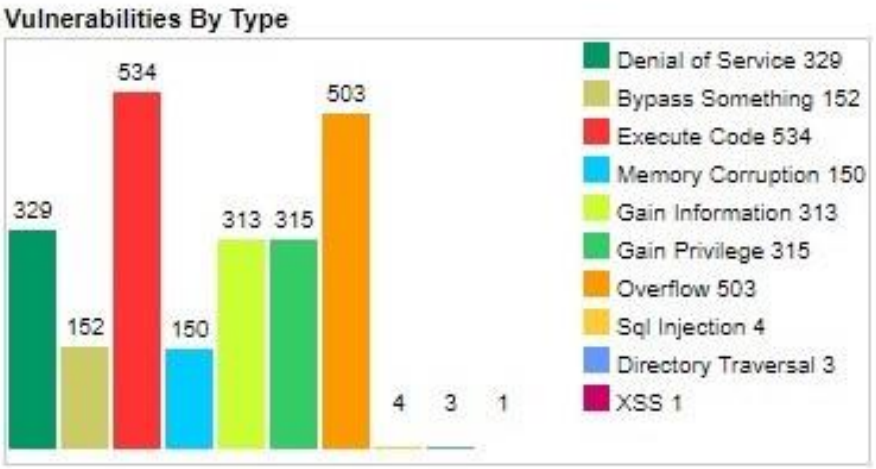
Lots of vulnerability disclosures (2021)

S.No	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Debian Linux	Debian	OS	3067
2	Android	Google	OS	2563
3	Linux Kernel	Linux	OS	2357
4	Mac Os X	Apple	OS	2212
5	Ubuntu Linux	Canonical	OS	2007
6	Firefox	Mozilla	Application	1873
7	Chrome	Google	Application	1858
8	Iphone Os	Apple	OS	1655
9	Windows Server 2008	Microsoft	OS	1421
10	Windows 7	Microsoft	OS	1283
11	Acrobat Reader Dc	Adobe	Application	1182
12	Acrobat Dc	Adobe	Application	1182
13	Windows 10	Microsoft	OS	1111
14	Flash Player	Adobe	Application	1078
15	Windows Server 2012	Microsoft	OS	1050

https://www.cvedetails.com/top-50-products.php?year=2021

Android: Vulnerability Stats (2021)





https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224

More Definitions: Threat and Attack

- Threat: An adversary that is motivated and capable of exploiting a vulnerability in the system by launching attacks
  - Different enemies have different abilities
  - You can't design a secure system unless you know who the enemy is
- Attack: An intentional act by which an entity attempts to evade security services and violate the security policy of a system
- Passive vs Active Attacks
  - Passive attack attempts to learn or make use of information from a system but does not affect system resources of that system
    - Monitoring of network traffic
    - Very difficult to detect, but feasible to prevent them /w encryption
  - Active attack attempts to alter system resources or affect its operation
    - Man-in-the-middle (MITM) & DoS attacks
    - Very difficult to prevent them due to wide variety of vulnerabilities
    - Main goal is to detect attacks and recover the system to normal operation

Attackers

- **Types**
  - Individual
    - Outsider
    - Insider
    - Trusted/Privileged Insider
  - Group
    - Ad hoc
    - Established
  - Organization
    - Competitor
    - Supplier
    - Partner
    - Customer
  - State or State-sponsored actor
- **Capabilities**
  - Time
  - Money
  - Training
  - Access
- **Motivation/Intent**
  - Curiosity
  - Fame
  - Money
  - National interest

Threat Model

- Your very first question in any security discussion should be

  What's the threat model?

- Do not argue about attacks or defenses without understanding the threat model
- The threat model defines the problem to be solved
  - If there is no consensus on the problem, there will be no consensus on solutions

Threat Model: An example

- Asset
  - TV, Smartphone, Jewelry
- Trust Boundary
  - Spouse, roommate
- Attacker
  - Roommate, thief

Risk Assessment

- Now that we know what we want to protect and from whom, we can reason about what risks attackers can pose to our assets
- Risk Assessment/analysis involves
  a) Start by understanding system requirements
  b) Identify assets and attackers
  c) Establish security requirements
  d) Evaluate system design
  e) Identify threats and classify risks
  f) Address identified risks

Types of Network Attacks

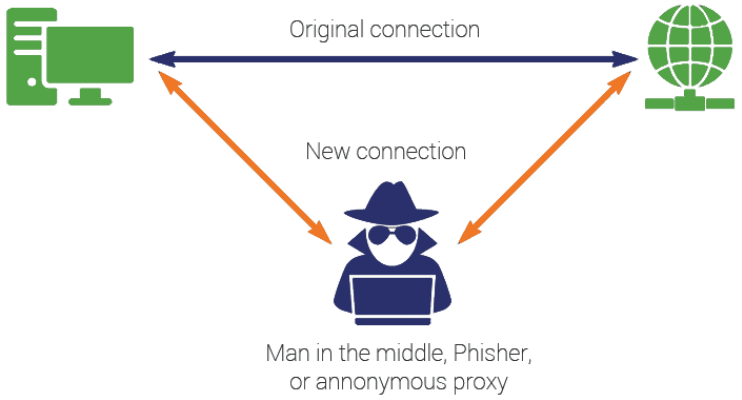
- Eavesdropping attacks
- Man-in-the-middle (MITM) attacks
- Denial of Service (DoS) attacks

Eavesdropping Attacks

- Easy to intercept traffic, almost impossible to detect
- By default, everything is transmitted in clear text
  - Usernames, passwords, content ...
  - No security offered by the transmission medium
- Different tools available on Internet
  - Wireshark/Kismet/Tcpdump/airdump-ng/...
- With the right equipment, it's possible to eavesdrop from few kilometers away in wireless networks
- Affects Confidentiality of data exchanged
- Countermeasures
  - Encryption and signal-hiding techniques

MITM Attacks

- Attacker intercepts or modifies communication between sender and receiver
- Affects Integrity



https://www.thesslstore.com/blog/man-in-the-middle-attack-2/

Denial of Service (DoS) Attacks

- Attacks on higher levels
  - SYN Flooding
  - Ping of death, Ping flood
  - ...
- IP spoofing
- Spoofed MAC control packets in Wi-Fi
- ARP spoofing
- Spoofed deauthentication / disassociation messages
  - can target one specific user
- Frequency jamming
  - Not very technical, but works very well

Homework

- Reflections on Trusting Trust, Turing award lecture, Ken Thompson, Creator of UNIX, B and Go languages
- Designing an Internet, Talk at Google, David D. Clark, MIT Computer Scientist

References

- IETF RFC 4949: https://tools.ietf.org/html/rfc4949
- Overview of Cybersecurity, ITU-T X.1205:

https://www.itu.int/rec/T-REC-X.1205-200804-I

- CVE: https://cve.mitre.org/
- CVE Stats and Visualization: https://www.cvedetails.com/top-50-products.php?year=2021