- Vulnerability – weakness in hardware, software, personnel or procedures which may be exploit by threat
- Risk – is a combination of threat probability and the impact of a vulnerability
- Threat – any type of danger, can damage or steel data, create a disruption or cause a harm

Risk = Threat Probability*Vulnerability Impact

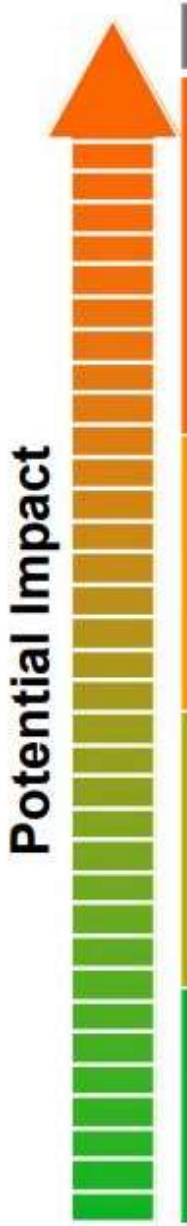
Threat

https://www.geeksforgeeks.org/threats-to-information-security/

Threat can be a advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest.

1. Software attacks
2. theft of intellectual property 3
3. identity theft, theft of equipment or information 4
4. sabotage 5
5. information extortion.

Today's threats (actors) are more sophisticated.



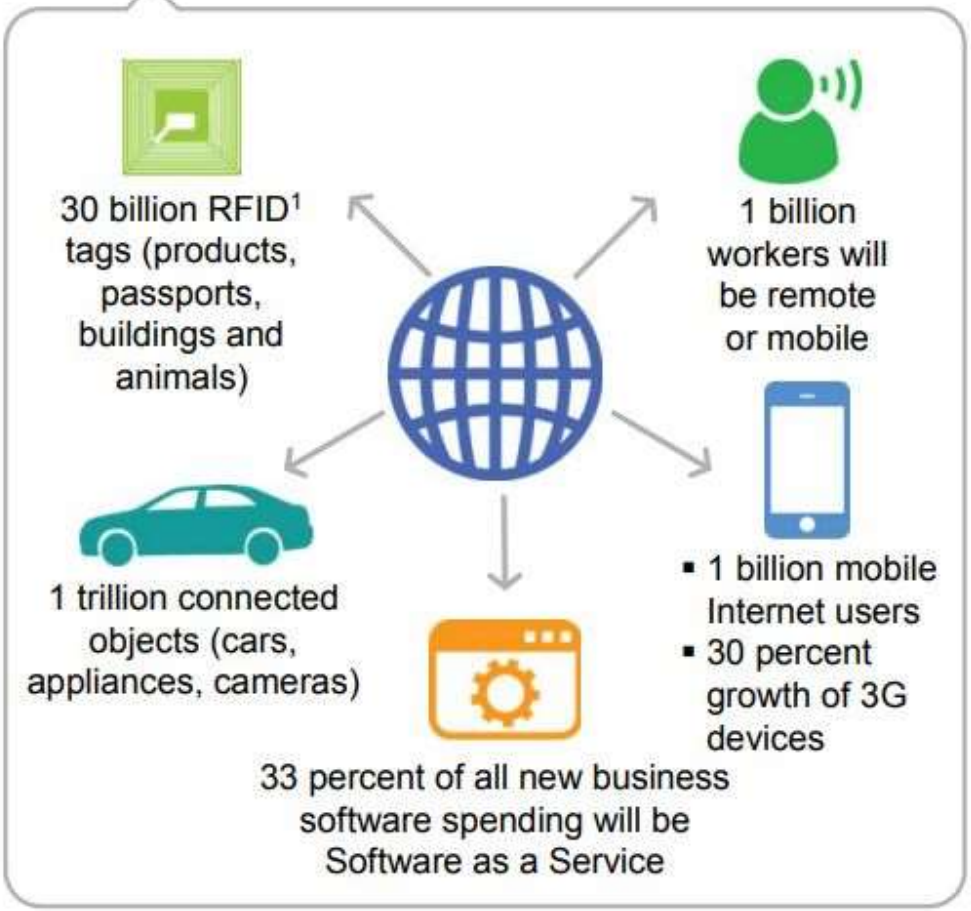
Threat	Type	% of Incidents	Threat Profile
Advanced, Persistent Threat / Mercenary	▪ National governments ▪ Organized crime ▪ Industrial spies ▪ Terrorist cells	Equals less than 10 percent	▪ Sophisticated tradecraft ▪ Foreign intelligence agencies, organized crime groups ▪ Well financed and often acting for profit ▪ Target technology as well as information ▪ Target and exploit valuable data ▪ Establish covert presence on sensitive networks ▪ Difficult to detect ▪ **Increasing in prevalence**
Hacktivist	▪ "White hat" and "black hat" hackers ▪ "Protectors of "Internet freedoms"	Equals less than 10 percent	▪ Inexperienced-to-higher-order skills ▪ Target known vulnerabilities ▪ Prefer denial of service attacks BUT use malware as means to introduce more sophisticated tools ▪ Detectable, but hard to attribute ▪ **Increasing in prevalence**
Opportunist	▪ Worm and virus writers ▪ Script Kiddie	20 percent	▪ Inexperienced or opportunistic behavior ▪ Acting for thrills, bragging rights ▪ Limited funding ▪ Target known vulnerabilities ▪ Use viruses, worms, rudimentary Trojans, bots ▪ Easily detected
Inadvertent Actor	▪ Insiders - employees, contractors, outsourcers	60 percent	▪ No funding ▪ Causes harm inadvertently by unwittingly carrying viruses, or posting, sending or losing sensitive data ▪ Increasing in prevalence with new forms of mobile access and social business

Source: Government Accountability Office (GAO), Department of Homeland Security's (DHS's) Role in Critical Infrastructure Protection (CIP) Cybersecurity, GAO-05-434

Number of vulnerabilities increase radically with emergence of new business models and technologies.

Adopting new business models and embracing new technologies

Exponentially growing and interconnected digital universe



Source: IBM X-Force® Trend Report, 2011

1. **Software attacks / malware /intrusive program code - (**Viruses, Worms, Trojan Horses etc. Many users believe that malware, virus, worms, bots) **same malicious + software** (combination of these two terms)**but act differently**

Malware – two categories

`A. Infection Method

B Malware Actions

A.1 – Viruses – replicate themselves by hooking, The Creeper Virus - ARPANET.

A.2 – Worm – replicate themselves

A.3 – Trojan - backdoor gateway for malicious programs enter system and steal data without your knowledge and permission. Examples include FTP Trojans, Proxy Trojans, Remote Access Trojans etc.

A.4 – Bots – advance worms – malicious bot infect one create connection to central system then command all infected host, this network called Bots.

B Malware Actions –

B.1- Adware

B.2 - Spyware - key logger is to record user keystrokes with timestamp- username, password, credit card

B.3 – Ransom ware - encrypt your files or will lock your computer making it inaccessible.

B.4 - Shareware – masquerades as a tool to help fix your system but when the software is executed it will infect your system or completely destroy it. The software will display a message to frighten you and force to take some action like pay them to fix your system.

B.5 - Rootkits – are designed to gain root access

B.6 – Zombies – wait for command

Theft of intellectual property – copy write, patent.

Identity theft - accessing other social media accounts

Theft of equipment and information – theft of memory storage.

Sabotage – destroy companies websites.

Information extortion – - theft of company's property or information to receive payment in exchange. E.g. Ransom ware

Technology with weak security –

a apply require advancement in technology, up to date of Securities news

Social media attacks - cyber criminals identify and infect a cluster of websites that persons of a particular organization visit, to steal information.

Mobile Malware –

Outdated Security Software –

Corporate data on personal devices – BYOD means Bring your own device like Laptops, Tablets to the workplace

Social Engineering – Manipulate the people and take their confidential information / credentials.

New Generation Threats

- **Emote**

The Cyber security and Infrastructure Security Agency (CISA) describes Emotet as “an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. Emotet continues to be among the most costly and destructive malware.”

- Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine. Phishing is an increasingly common cyber threat.

cyber attack

- **Man-in-the-middle (MitM)** attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.
- **Two common points of entry for MitM attacks:**
- 1. On unsecure public Wi-Fi, attackers can insert themselves between a visitor's device and the network. Without knowing, the visitor passes all information through the attacker.
- 2. Once malware has breached a device, an attacker can install software to process all of the victim's information.

- **A denial-of-service attack, floods systems, servers, or networks** with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests. Attackers can also use multiple compromised devices to launch this attack. This is known as a distributed-denial-of-service (DDoS) attack.

- **A Structured Query Language (SQL) –**

injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not.

An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box. Learn how to defend against SQL injection attacks.

zero-day exploit hits after a network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time.

- Zero-day vulnerability threat detection requires constant awareness.

- DNS tunneling utilizes the DNS protocol to communicate non-DNS traffic over port 53.

- It sends HTTP and other protocol traffic over DNS.
- There are various, legitimate reasons to utilize DNS tunneling.

However, there are also malicious reasons to use DNS Tunneling VPN services.

They can be used to disguise outbound traffic as DNS, concealing data that is typically shared through an internet connection.

For malicious use,

DNS requests are manipulated to exfiltration data from a compromised system to the attacker's infrastructure. It can also be used for command and control callbacks from the attacker's infrastructure to a compromised system.

- Password Attacks
- With the right password, a cyber attacker has access to a wealth of information.
- Social engineering is a type of password attack that Data Insider defines as “a strategy cyber attackers use that relies heavily on human interaction and often involves tricking people into breaking standard security practices.
- ” Other types of password attacks include accessing a password database or outright guessing.

- The Internet of Things
- Individual devices that connect to the internet or other networks offer an access point for hackers.
- Cytelligence reports that in 2019, hackers increasingly targeted smart home and internet of things (IoT) devices,
- such as smart TVs, voice assistants, connected baby monitors and cellphones.
- Hackers who successfully compromise a connected home not only gain access to users' Wi-Fi credentials, but may also gain access to their data,
- such as medical records, bank statements and website login information.

- The Explosion of Data
- Data storage on devices such as laptops and cellphones makes it easier for cyber attackers to find an entry point into a network through a personal device.
- For example, in the May 2019 book Exploding Data: Reclaiming Our Cyber Security in the Digital Age, former U.S. Secretary of Homeland Security Michael Chertoff warns of a pervasive exposure of individuals' personal information, which has become increasingly vulnerable to cyber attacks.
- Consequently, companies and government agencies need maximum cyber security to protect their data and operations. Understanding how to address the latest evolving cyber threats is essential for cyber security professionals.

- widespread use of online and digital communication systems, sensitive information is transmitted around the world every day.
- Cryptography has become essential for protecting information online.
- Cyber security professionals need a good understanding of cryptography
- cryptography tools to set up and run secure computer systems and networks.

Cryptography Tools for Cyber Security

Cryptography in the Modern Era

- In World War II, German submarines lurking below the surface of the North Atlantic preyed on Allied ships carrying supplies to England from the United States. The ships, not knowing the locations of submarines, could do little to avoid the attacks.
- Enter British mathematician Alan Turing and a team of code breakers. Using the cryptography tools available at the time, they cracked codes generated by Germany's sophisticated Enigma machine, revealing German communications with the submarines. This allowed the Allies to route their ships to avoid the submarines.
- Deciphering the German codes was one of the more significant achievements in cryptography, a field almost as old as human communication.
- Today, cryptography is a key tool in the battle to keep computer systems and networks secure and private.

- There’s a lot to protect. Individuals entrust personal, financial, medical and other information to companies, government agencies and other organizations that store it digitally. Hardly a month goes by without news of a data breach that exposes millions of accounts.
- Research firm Gartner estimates that more than 80% of companies encrypted their web traffic in 2019. That percentage is likely to grow as more companies seek to protect their data as well as meet stricter regulations governing security and privacy.

- Security Tokens
- Key-Based Authentication
- Dockers
- Java Cryptography Architecture
- Sign Tool

Five Cryptography Tools

SignTool

- Another security tool embedded in an operating system is Microsoft Sign Tool (SignTool.exe).
- A command-line tool, Sign Tool can digitally sign and time-stamp files and verify signatures in files. It's automatically installed with Microsoft Visual Studio, a software development environment.
- Sign Tool allows software developers to certify that the code they developed is theirs and that it hasn't been tampered with since it was published.

Java Cryptography Architecture

- The popular Java programming language has built-in cryptographic functions. The Java Cryptography Architecture (JCA) is integrated with the core Java application programming interface (API). The JCA contains APIs that handle security functions that include encryption, managing keys, generating random numbers securely and validating certificates. These APIs provide a way for developers to build security into application code.

- The Docker software platform builds applications based on containers: small self-contained environments that share an operating system kernel but otherwise run in isolation from one another.

- By their nature, Docker containers are secure. More security can be added by enabling one of several applications that fortify the system.

Docker

Key-based authentication

- Key-based authentication is a method that employs asymmetric algorithms to confirm a client's identity and can be an effective substitute for using passwords to verify a client. The key factors at play in key-based authentication are public and private keys that confirm identity.
- In public key authentication, each user is given a pair of asymmetric keys. Users store their public keys in each system they want access to, while the private keys are safely maintained on the device with which the user connects to the secured systems.
- When connecting, the server authenticates the user with the public key and asks the user to decrypt it using the corresponding private key.

Security Tokens

- A security token is a physical device that holds information that authenticates a person's identity. The owner plugs the security token into a system — via a computer's USB port, for example — to gain access to a network service. It's like swiping a security card to get into an office. A bank might issue security tokens to customers to use as an extra layer of security when they log in to their accounts.

Trends in Cryptography

- Cryptography tools constantly evolve as cryptographers and hackers leapfrog each other in building defenses and overcoming them. Several trends on the horizon point to new directions in cryptography.

1. Quantum Computers and Cryptography
2. Cloud Computing
3. Block chain

Quantum Computers and Cryptography

- The emerging technology of quantum computing promises great leaps in power and speed.
- Companies such as Google and IBM are racing to develop quantum computers, which could make some kinds of computing problems easier to solve than with today's conventional computers.
- One such problem area is the encryption protocols for today's computing systems. The computing power of a quantum computer, experts say, could shred current security defenses. Security experts are developing systems that could protect against quantum systems.

- When a company stores data on someone else's servers,
- such as in a public cloud, the company loses control over securing the data.
- To solve that problem,
- some companies encrypt the data before storing it on a cloud system,
- giving the company a measure of control over the encryption.
- Another approach is to use cloud services that encrypt information when it enters the cloud environment,
- which protects it as it is stored or transmitted.

Cloud Computing

Block chain

- Block chain is a distributed ledger that underlies digital currencies such as bit coin.
- A block chain is a series of data or transactions (the blocks) connected by cryptographic signatures stored in shared ledgers and supported by nodes, which form a network of processes. Nodes maintain a copy of the entire chain and are continually updated and kept in sync.
- Companies have deployed block chain technologies for secure transactions with customers as well as for storing data such as medical records.

https://onlinedegrees.und.edu/blog/types-of-cyber-attacks/

Common Types of Cyber Attacks and Prevention Tactics

- https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats

What is Social Engineering? Defining and Avoiding Common Social Engineering Threats

- https://www.upguard.com/blog/cyber-threat

What is a Cyber Threat?

- https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

Top 10 Most Common Types of Cyber Attacks

- https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html

What Is a VPN? - Virtual Private Network