INFORMATION SYSTEMS SECURITY AND CRYPTOGRAPHY

Lesson 01

By: Michael Maigwa M. Kangethe

DISCLAIMER

This document does not claim any originality and cannot be used as a substitute for prescribed textbooks. The information presented here is merely a collection by the Lecturer for his respective teaching assignments. Various sources as mentioned at the end of the document as well as freely available material from internet were consulted for preparing this document. The ownership of the information lies with the respective author(s) or institutions.

What is information systems security?

The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats

Why information Security

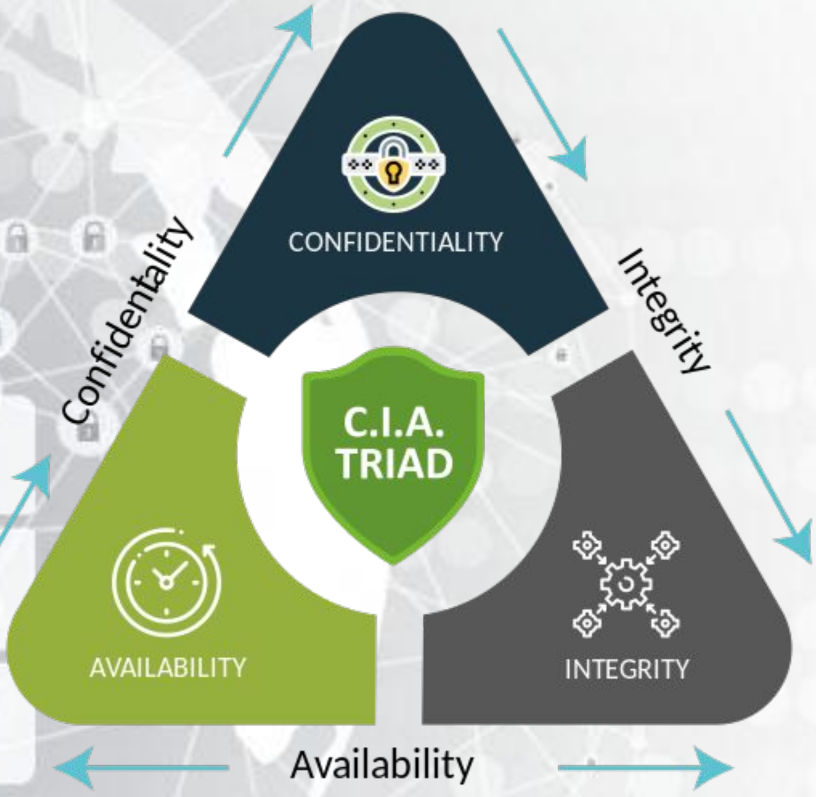
Sun Tzu stated that the best tacticians are those who can control situations through intelligence and leverage information to dictate the choices of their adversaries.

Once an organization establishes a complete understanding of its attack surface, it can deploy security controls that protect critical assets

What are the 3 main pillars of information security?

- **Confidentiality** — You need to know your data is protected from unauthorized access.
  - Only those with proper access rights and privileges should be able to access the data
- **Integrity** — You have to be able to trust your data.
  - means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. The property that data or information have not been altered or destroyed in an unauthorized manner. The ability to detect even minute changes in the data.
- **Availability** — You need to be able to access your data.
  - The Data and systems are available on demand at all times

The C.I.A Triad



Some Important Terms and Jargons

Vulnerability

A vulnerability is a weakness, flaw or other shortcoming in a system (infrastructure, database or software), but it can also exist in a process, a set of controls, or simply just the way that something has been implemented or deployed.

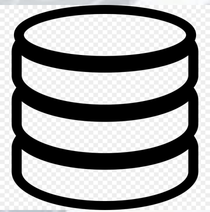
These weaknesses can include:

Technical vulnerabilities, like bugs in code or an error in some hardware or software.

Human vulnerabilities, such as employees falling for phishing, smishing or other common attacks.

Some Important Terms and Jargons

Money



Data

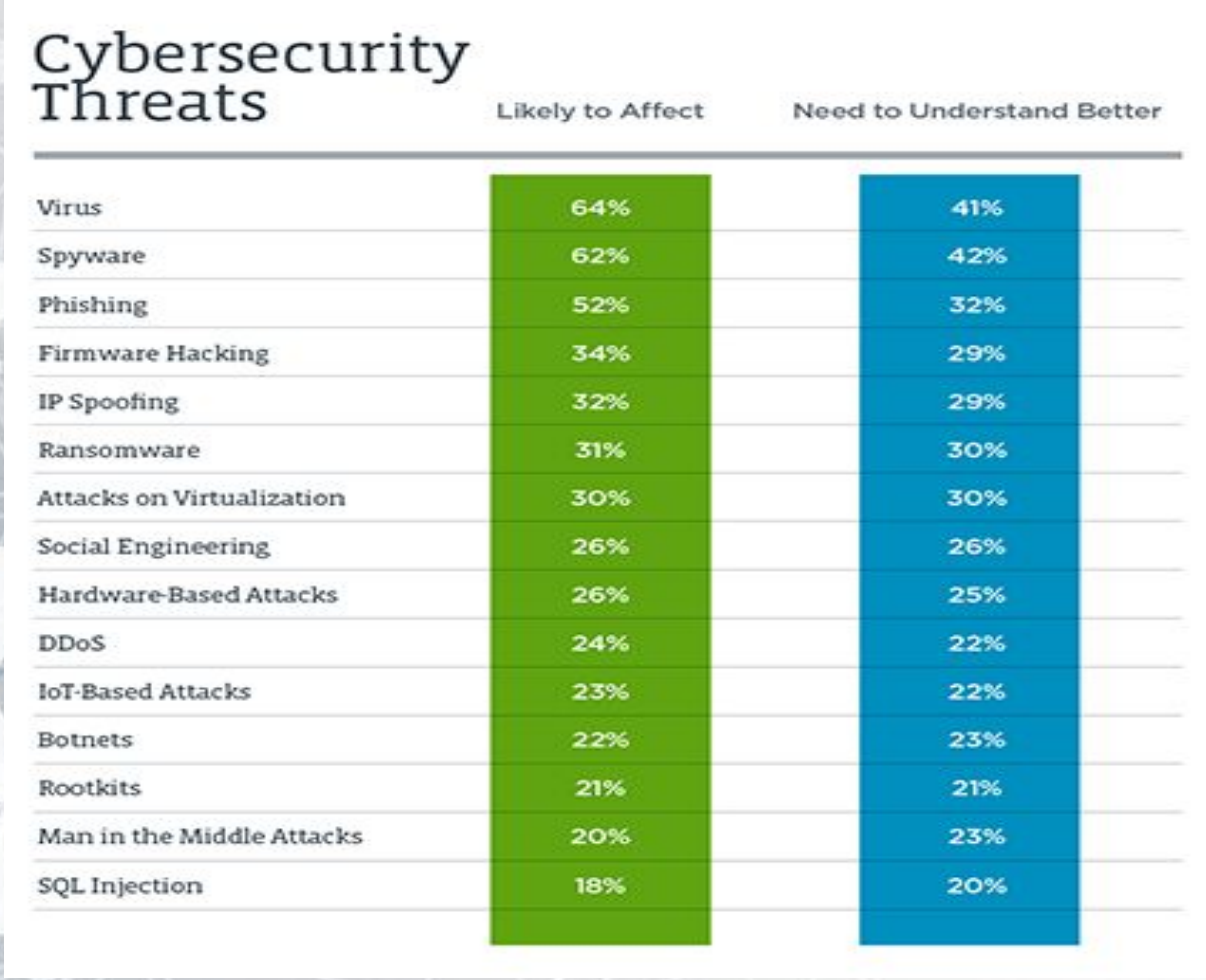
Computing Resources

Chaos and Anarchy

Threat

A threat is anything that could exploit a vulnerability, which could affect the confidentiality, integrity or availability of your systems, data, people and more. (Confidentiality, integrity and availability, sometimes known as the CIA triad, is another fundamental concept of cybersecurity.)

A more advanced definition of threat is when an adversary or attacker has the opportunity, capability and intent to bring a negative impact upon your operations, assets, workforce and/or customers. Examples of this can include malware, ransomware, phishing attacks and more — and the types of threats out there will continue to evolve.



Cybersecurity Threats

	Likely to Affect	Need to Understand Better
Virus	64%	41%
Spyware	62%	42%
Phishing	52%	32%
Firmware Hacking	34%	29%
IP Spoofing	32%	29%
Ransomware	31%	30%
Attacks on Virtualization	30%	30%
Social Engineering	26%	26%
Hardware-Based Attacks	26%	25%
DDoS	24%	22%
IoT-Based Attacks	23%	22%
Botnets	22%	23%
Rootkits	21%	21%
Man in the Middle Attacks	20%	23%
SQL Injection	18%	20%

Some Important Terms and Jargons

Risk

Risk is the probability of a negative (harmful) event occurring as well as the potential of scale of that harm. Your organizational risk fluctuates over time, sometimes even on a daily basis, due to both internal and external factors.

A slightly more technical angle, the Open FAIR body of knowledge defines cyber risk as the probable frequency and probably magnitude of loss. Sounds complicated, until we break it down: “For starters,” Rudis says”, there is no ethereal risk. Something is at risk, be it a system, device, business process, bank account, your firm’s reputation or human life.”

This is where cybersecurity teams can begin to measure that risk:

1. Estimate how often an adversary or attacker is likely to attempt to exploit a vulnerability to cause the desired harm.
2. Gauge how well your existing systems, controls and processes can stand up to those attempts.
3. Determine the value of the impact or harm the adversary may cause if the adversary is indeed successful.

One way of describing risk was consequence X likelihood, but as security teams have advanced their processes and intelligence, we see that you have to also account for the safeguards you’ve already put in place.

Risk = threat x vulnerability

The four types of information security

There are four types of information technology security you should consider or improve upon:

- Network Security.
- Cloud Security.
- Physical Security
- Application Security.
- Internet of Things Security.

The four types of information security

Network Security

Most attacks occur over the network, and network security solutions are designed to identify and block these attacks. These solutions include data and access controls such as Data Loss Prevention (DLP), IAM (Identity Access Management), NAC (Network Access Control), and NGFW (Next-Generation Firewall) application controls to enforce safe web use policies.

Advanced and multi-layered network threat prevention technologies include IPS (Intrusion Prevention System), NGAV (Next-Gen Antivirus), Sandboxing, and CDR (Content Disarm and Reconstruction). Also important are network analytics, threat hunting, and automated SOAR (Security Orchestration and Response) technologies.

The four types of information security

Cloud Security

As organizations increasingly adopt cloud computing, securing the cloud becomes a major priority. A cloud security strategy includes cyber security solutions, controls, policies, and services that help to protect an organization’s entire cloud deployment (applications, data, infrastructure, etc.) against attack.

While many cloud providers offer security solutions, these are often inadequate to the task of achieving enterprise-grade security in the cloud. Supplementary third-party solutions are necessary to protect against data breaches and targeted attacks in cloud environments.

The four types of information security

Physical Security

This security layer ensures that both the physical assets like files, computers, people are protected against known and unknown threats and risks.

Measures can include Security surveillance CCTVs, controlled and monitored access points, ventilation, fire detection and suppression systems e.t.c.

The four types of information security

Application Security

Web/Desktop/Mobile applications, like anything else are targets for threat actors. Since 2007, OWASP has tracked the top 10 threats to critical web application security flaws such as injection, broken authentication, misconfiguration, and cross-site scripting to name a few.

With application security, the OWASP Top 10 attacks can be stopped. Application security also prevents bot attacks and stops any malicious interaction with applications and APIs. With continuous learning, apps will remain protected even as DevOps releases new content.

The four types of information security

Internet of Things Security

Your laptop that you take to meetings. Your phone that you use for Slack and calling clients. The printer you sent a memo to. Your Wi-Fi router that needs unplugged and plugged back in every once in a while. These are a few of the “things” make up the internet of things (IoT). If you’ve tethered a device to your network, it opens a portal for potential security threats.

Threats can come in at any point in the IoT journey. It is important to conduct a security risk assessment to find vulnerabilities in your network system and devices. This assessment should look at everything from web code to policy management and users. There are many layers within IoT, and that amount grows as your business grows. Don’t wait to ramp up your security.

Parameters	CYBER SECURITY	INFORMATION SECURITY
Basic Definition	It is the practice of protecting the data from outside the resource on the internet.	It is all about protecting information from unauthorized users, access, and data modification or removal in order to provide confidentiality, integrity, and availability.
Protect	It is about the ability to protect the use of cyberspace from cyber attacks.	It deals with the protection of data from any form of threat.
Scope	Cybersecurity to protect anything in the cyber realm.	Information security is for information irrespective of the realm.
Threat	Cybersecurity deals with the danger in cyberspace.	Information security deals with the protection of data from any form of threat.
Attacks	Cybersecurity strikes against Cyber crimes, cyber frauds, and law enforcement.	Information security strikes against unauthorized access, disclosure modification, and disruption.

By: Michael Maigwa M. Kangethe

Parameters	CYBER SECURITY	INFORMATION SECURITY
Professionals	Cyber security professionals deal with the prevention of active threats or Advanced Persistent threats (APT).	Information security professionals are the foundation of data security and security professionals associated with it are responsible for policies, processes, and organizational roles and responsibilities that assure confidentiality, integrity, and availability.
Deals with	It deals with threats that may or may not exist in the cyber realm such as protecting your social media account, personal information, etc.	It deals with information Assets and integrity, confidentiality, and availability.
Defense	Acts as first line of defense.	Comes into play when security is breached.
Professionals	Cyber security professionals deal with the prevention of active threats or Advanced Persistent threats (APT).	Information security professionals are the foundation of data security and security professionals associated with it are responsible for policies, processes, and organizational roles and responsibilities that assure confidentiality, integrity, and availability.

Parameters	CYBER SECURITY	INFORMATION SECURITY
Deals with	It deals with threats that may or may not exist in the cyber realm such as protecting your social media account, personal information, etc.	It deals with information Assets and integrity, confidentiality, and availability.
Deals with	It deals with threats that may or may not exist in the cyber realm such as protecting your social media account, personal information, etc.	It deals with information Assets and integrity, confidentiality, and availability.
Deals with	It deals with threats that may or may not exist in the cyber realm such as protecting your social media account, personal information, etc.	It deals with information Assets and integrity, confidentiality, and availability.
Deals with	It deals with threats that may or may not exist in the cyber realm such as protecting your social media account, personal information, etc.	It deals with information Assets and integrity, confidentiality, and availability.

Security Attacks

A security attack is an attempt by a person or entity to gain unauthorized access to disrupt or compromise the security of a system, network, or device. These are defined as the actions that put at risk an organization’s safety. They are further classified into 2 sub-categories:

- **Passive Attack**
  - Attacks in which a third-party intruder tries to access the message/ content/ data being shared by the sender and receiver by keeping a close watch on the transmission or eave-dropping the transmission is called Passive Attacks.
- **Active Attack**
  - involve the attacker actively disrupting or altering system, network, or device activity. Active attacks are typically focused on causing damage or disruption, rather than gathering information or intelligence.

Passive Attack

- **Eavesdropping**: This involves the attacker intercepting and listening to communications between two or more parties without their knowledge or consent. Eavesdropping can be performed using a variety of techniques, such as packet sniffing, or man-in-The-Middle (MITM)
- **Traffic analysis**: This involves the attacker analyzing network traffic patterns and metadata to gather information about the system, network, or device. Here the intruder can’t read the message but only understand the pattern and length of encryption. Traffic analysis can be performed using a variety of techniques, such as network flow analysis, or protocol analysis man-in-the-middle attacks.

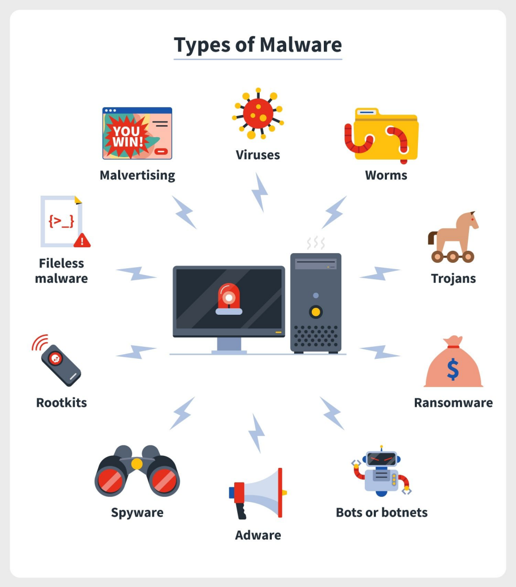
Active Attacks

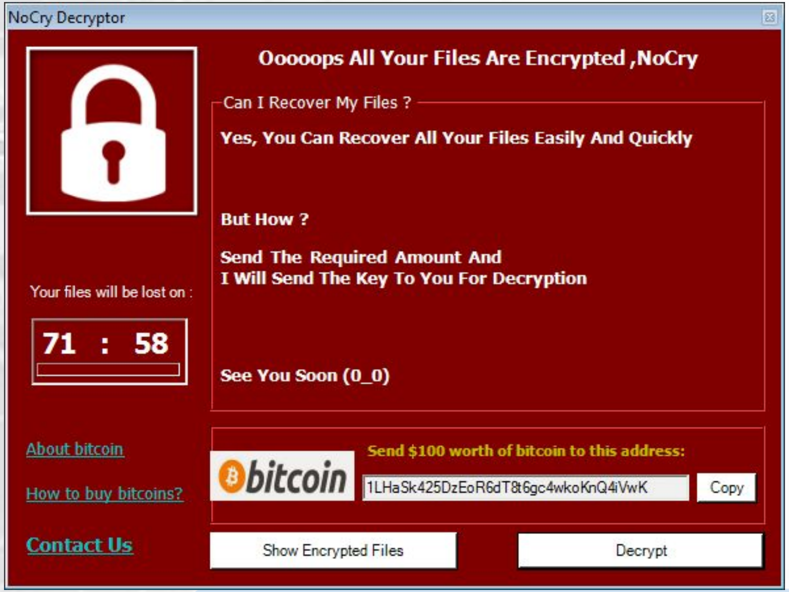
- **Masquerade** is a type of attack in which the attacker pretends to be an authentic sender in order to gain unauthorized access to a system. This type of attack can involve the attacker using stolen or forged credentials, or manipulating authentication or authorization controls in some other way.
- **Replay** is a type of active attack in which the attacker intercepts a transmitted message through a passive channel and then maliciously or fraudulently replays or delays it at a later time.
- **Modification of Message** involves the attacker modifying the transmitted message and making the final message received by the receiver look like it’s not safe or non-meaningful. This type of attack can be used to manipulate the content of the message or to disrupt the communication process.
- **Denial of service (DoS)** attacks involve the attacker sending a large volume of traffic to a system, network, or device in an attempt to overwhelm it and make it unavailable to legitimate users.

10 Types of Cyber Attacks You Should Be Aware in 2023

- **Malware Attack** (**Mal**icious Soft**ware**)

This is one of the most common types of cyber attacks. “Malware” refers to malicious software viruses including worms, spyware, ransomware, adware, and trojans.





Ooooops All Your Files Are Encrypted ,NoCry

Can I Recover My Files ?

Yes, You Can Recover All Your Files Easily And Quickly

But How ?

Send The Required Amount And
I Will Send The Key To You For Decryption

See You Soon (0_0)

Your files will be lost on :

71 : 58

Send $100 worth of bitcoin to this address:

1LHaSk425DzEoR6dT8t6gc4wkoKnQ4iVwK

By: Michael Maigwa M. Kangethe

The Evolution of the Cyber Security Threat Landscape

The cyber threats of today are not the same as even a few years ago. As the cyber threat landscape changes, organizations need protection against cybercriminals’ current and future tools and techniques.

The Gen V Attacks

The cyber security threat landscape is continually evolving, and, occasionally, these advancements represent a new generation of cyber threats. To date, we have experienced five generations of cyber threats and solutions designed to mitigate them, including:

Gen V Attacks

- **Gen I (Virus)**: In the late 1980s, virus attacks against standalone computers inspired the creation of the first antivirus solutions.
- **Gen II (Network)**: As cyberattacks began to come over the Internet, the firewall was developed to identify and block them.
- **Gen III (Applications)**: Exploitation of vulnerabilities within applications caused the mass adoption of intrusion prevention systems (IPS)
- **Gen IV (Payload)**: As malware became more targeted and able to evade signature-based defenses, anti-bot and sandboxing solutions were necessary to detect novel threats.
- **Gen V (Mega)**: The latest generation of cyber threats uses large-scale, multi-vectors attacks, making advanced threat prevention solutions a priority.

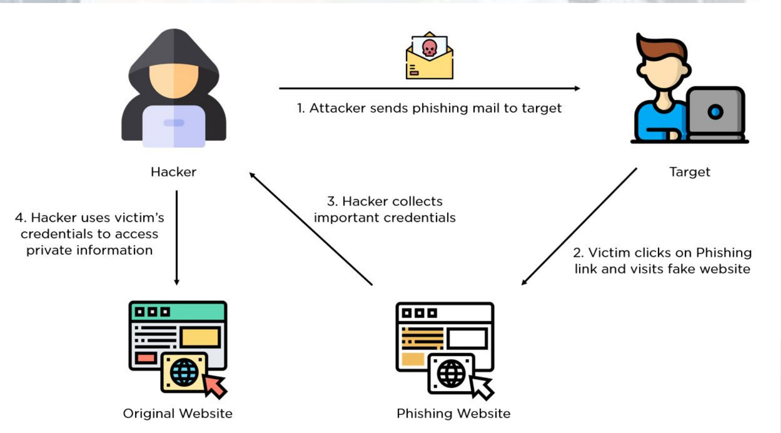
Gen V Attacks

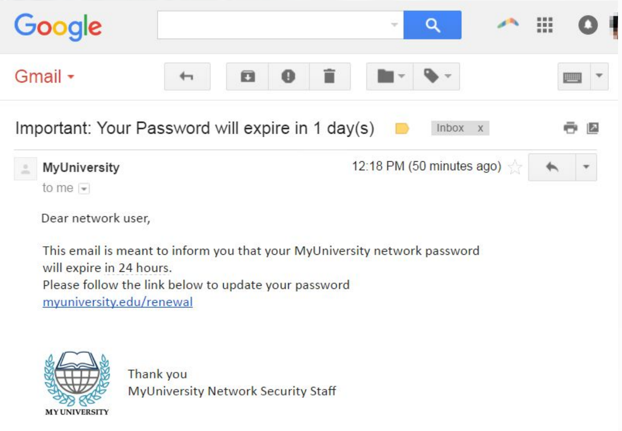
Each generation of cyber threats made previous cyber security solutions less effective or essentially obsolete. Protecting against the modern cyber threat landscape requires Gen V cyber security solutions.

10 Types of Cyber Attacks You Should Be Aware in 2023

- **Phishing Attack**

Phishing attacks are one of the most prominent widespread types of cyber attacks. It is a type of social engineering attack wherein an attacker impersonates to be a trusted contact and sends the victim fake mails. Unaware of this, the victim opens the mail and clicks on the malicious link or opens the mail's attachment. By doing so, attackers gain access to confidential information and account credentials. They can also install malware through a phishing attack.


Hacker
1. Attacker sends phishing mail to target
Target
3. Hacker collects important credentials
4. Hacker uses victim's credentials to access private information
2. Victim clicks on Phishing link and visits fake website
Original Website
Phishing Website



Important: Your Password will expire in 1 day(s)

MyUniversity
to me
12:18 PM (50 minutes ago)

Dear network user,

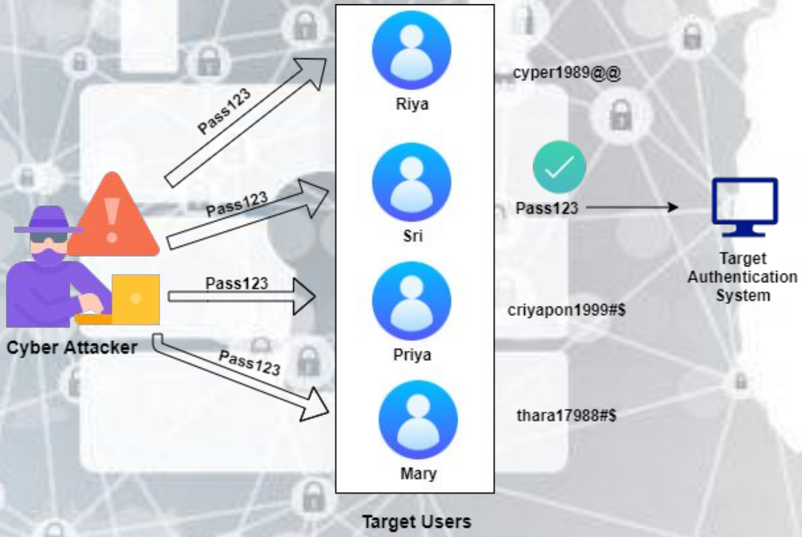
This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal

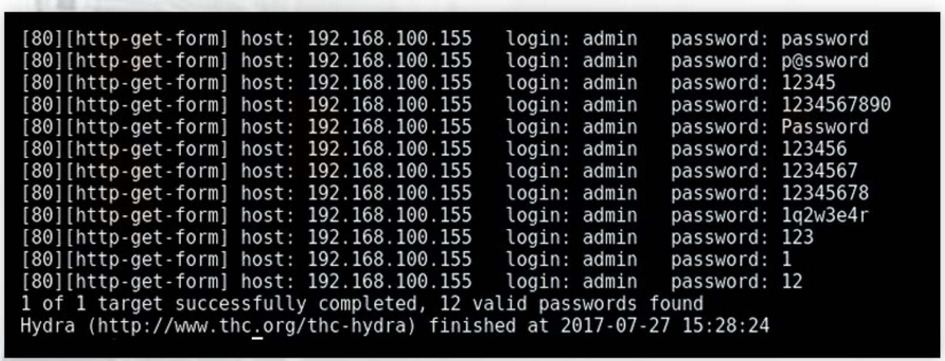
Thank you
MyUniversity Network Security Staff

10 Types of Cyber Attacks You Should Be Aware in 2023

- **Password Attack**

It is a form of attack wherein a hacker cracks your password with various programs and password cracking tools like Aircrack, Cain, Abel, John the Ripper, Hashcat, etc. There are different types of password attacks like brute force attacks, dictionary attacks, and keylogger attacks.



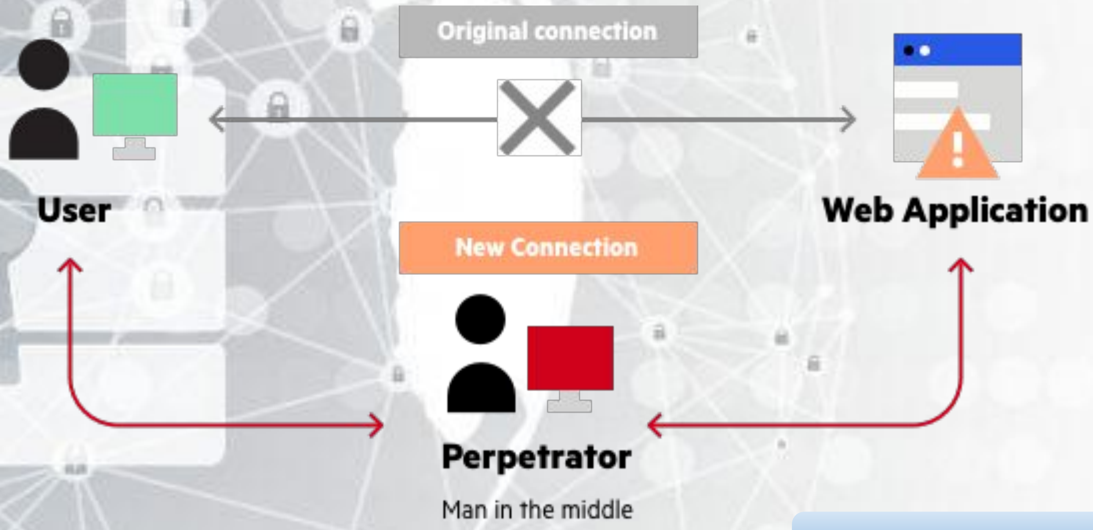


```
[80][http-get-form] host: 192.168.100.155   login: admin   password: password
[80][http-get-form] host: 192.168.100.155   login: admin   password: p@ssword
[80][http-get-form] host: 192.168.100.155   login: admin   password: 12345
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1234567890
[80][http-get-form] host: 192.168.100.155   login: admin   password: Password
[80][http-get-form] host: 192.168.100.155   login: admin   password: 123456
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1234567
[80][http-get-form] host: 192.168.100.155   login: admin   password: 12345678
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1q2w3e4r
[80][http-get-form] host: 192.168.100.155   login: admin   password: 123
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1
[80][http-get-form] host: 192.168.100.155   login: admin   password: 12
1 of 1 target successfully completed, 12 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-07-27 15:28:24
```

10 Types of Cyber Attacks You Should Be Aware in 2023

- **Man-in-the-Middle Attack**

A Man-in-the-Middle Attack (MITM) is also known as an eavesdropping attack. In this attack, an attacker comes in between a two-party communication, i.e., the attacker hijacks the session between a client and host. By doing so, hackers steal and manipulate data.

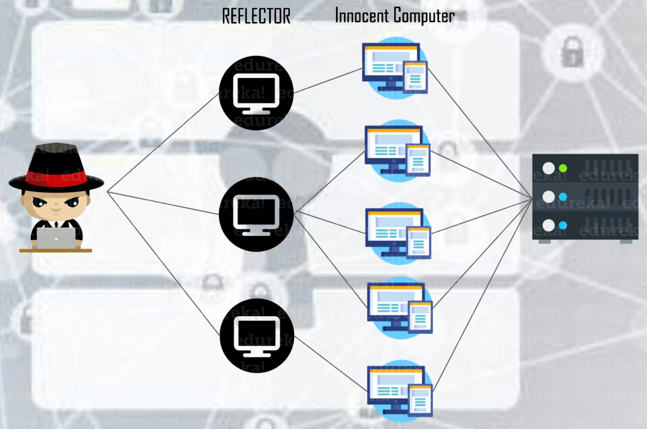


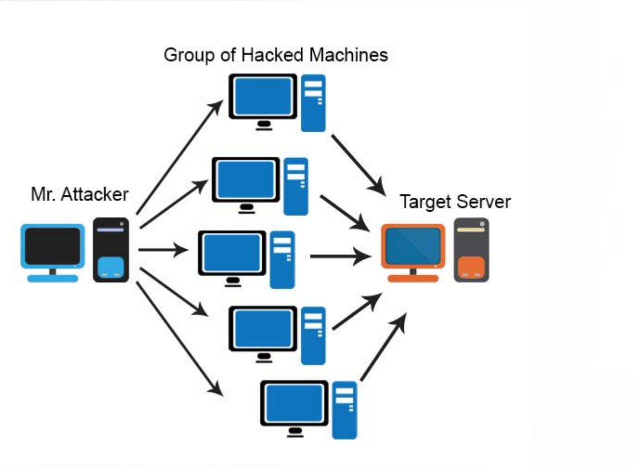
By: Michael Maigwa M. Kangethe

10 Types of Cyber Attacks You Should Be Aware in 2023

- **Denial-of-Service Attack**

A Denial-of-Service Attack is a significant threat to companies. Here, attackers target systems, servers, or networks and flood them with traffic to exhaust their resources and bandwidth.
When this happens, catering to the incoming requests becomes overwhelming for the servers, resulting in the website it hosts either shut down or slow down. This leaves the legitimate service requests unattended.



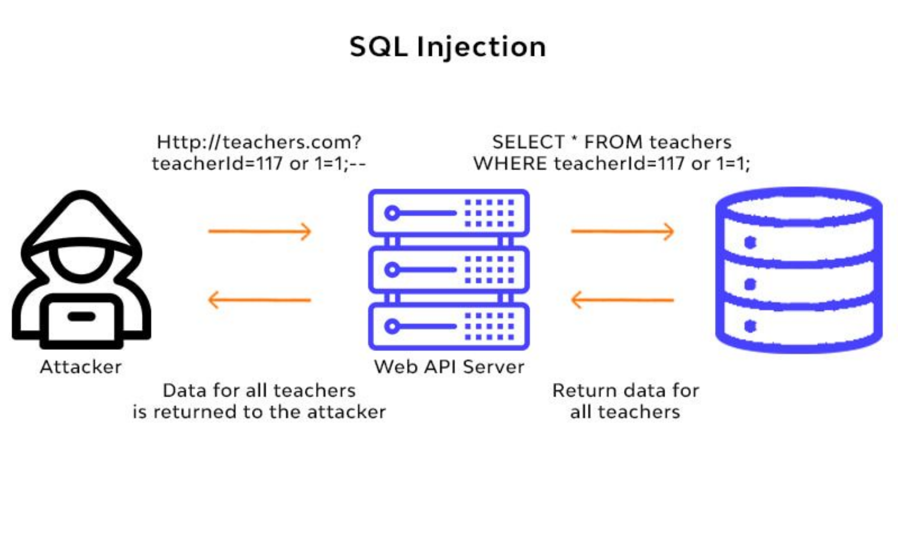


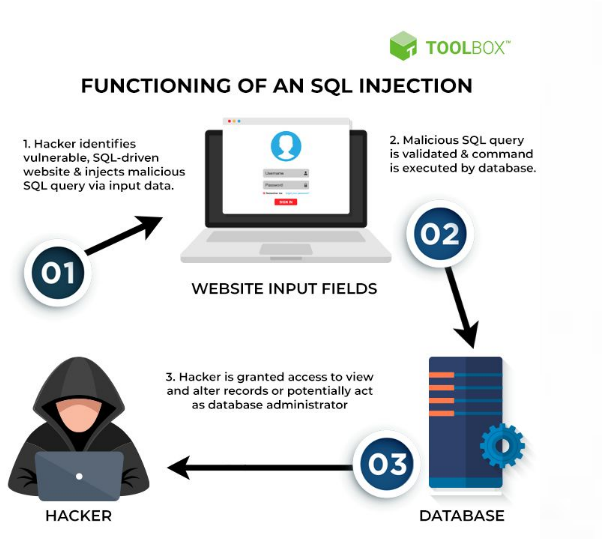
By: Michael Maigwa M. Kangethe

10 Types of Cyber Attacks You Should Be Aware in 2023

- **SQL Injection Attack**

A Structured Query Language (SQL) injection attack occurs on a database-driven website when the hacker manipulates a standard SQL query. It is carried by injecting a malicious code into a vulnerable website search box, thereby making the server reveal crucial information.




TOOLBOX™
FUNCTIONING OF AN SQL INJECTION
1. Hacker identifies vulnerable, SQL-driven website & injects malicious SQL query via input data.
2. Malicious SQL query is validated & command is executed by database.
01
02
WEBSITE INPUT FIELDS
3. Hacker is granted access to view and alter records or potentially act as database administrator
03
HACKER
DATABASE

By: Michael Maigwa M. Kangethe

10 Types of Cyber Attacks You Should Be Aware in 2023

- **Insider Threat**

As the name suggests, an insider threat does not involve a third party but an insider. In such a case; it could be an individual from within the organization who knows everything about the organization. Insider threats have the potential to cause tremendous damages.

Insider threats are rampant in small businesses, as the staff there hold access to multiple accounts with data. Reasons for this form of an attack are many, it can be greed, malice, or even carelessness. Insider threats are hard to predict and hence tricky.

- **Cryptojacking**

The term Cryptojacking is closely related to cryptocurrency. Cryptojacking takes place when attackers access someone else's computer for mining cryptocurrency.

The access is gained by infecting a website or manipulating the victim to click on a malicious link. They also use online ads with JavaScript code for this. Victims are unaware of this as the Crypto mining code works in the background; a delay in the execution is the only sign they might witness.

10 Types of Cyber Attacks You Should Be Aware in 2023

- **Zero-Day Exploit**

A Zero-Day Exploit happens after the announcement of a network vulnerability; there is no solution for the vulnerability in most cases. Hence the vendor notifies the vulnerability so that the users are aware; however, this news also reaches the attackers.

Depending on the vulnerability, the vendor or the developer could take any amount of time to fix the issue. Meanwhile, the attackers target the disclosed vulnerability. They make sure to exploit the vulnerability even before a patch or solution is implemented for it.

- **Watering Hole Attack**

The victim here is a particular group of an organization, region, etc. In such an attack, the attacker targets websites which are frequently used by the targeted group. Websites are identified either by closely monitoring the group or by guessing.

After this, the attackers infect these websites with malware, which infects the victims' systems. The malware in such an attack targets the user's personal information. Here, it is also possible for the hacker to take remote access to the infected computer.

Five ways the human factor can increase your cybersecurity risk

1. **Suspicious URLs and Emails:** Explain to employees that if something looks strange – it probably is! Encourage staff to pay attention to URLS, delete emails that don't have content or look like they are coming from a spoofed address, and stress the importance of guarding personal information. As the IT professional, it's your responsibility to raise awareness of potential cybersecurity threats.
2. **Password Idleness:** We know that holding on to the same password for ages isn't a great idea. But, Bob in finance may not understand that. Educate employees about the importance of frequently changing passwords and using strong combinations. We all carry a plethora of passwords and since it's a best practice not to duplicate your passwords, it's understandable that some of us need to write them down somewhere. Provide suggestions on where to store passwords.

Five ways the human factor can increase your cybersecurity risk

3. **Personally Identifiable Information:** Most employees should understand the need to keep personal browsing, like shopping and banking tasks, to their own devices. But everybody does a bit of browsing for work, right? Emphasize the importance of keeping an eye on what websites may lead to others. And, that includes social media. Karen in customer service may not realize that sharing too much on Facebook, Twitter, Instagram, etc. (like personally identifiable information) is just one way hackers can gather intel.
4. **Backups and Updates:** It’s fairly easy for an unsavvy tech consumer to go about their daily business without backing up their data regularly and updating their system’s anti-virus. This is a job for the IT department. The biggest challenge here is getting employees to understand when they need your help with these items.

Five ways the human factor can increase your cybersecurity risk

5. **Physical Security for Devices:** Think about how many people in your office leave their desk for meetings, gatherings and lunch breaks. Are they locking their devices? Highlight the need to protect information each and every time a device is left unattended. You can use the airport analogy. Airport staff are constantly telling us to keep track of our bags and never leave them unattended. Why? Well, because you just don’t know who is walking by. Encourage employees to protect their devices with as much care as they protect their baggage.

How to Prevent Cyber Attacks?

Although we had a look at several ways to prevent the different types of cyber attacks we discussed, let's summarize and look at a few personal tips which you can adopt to avoid a cyberattack on the whole.

1. Change your passwords regularly and use strong alphanumeric passwords which are difficult to crack. Refrain from using too complicated passwords that you would tend to forget. Do not use the same password twice***(Outdated by 2FA and MFA)***.
2. Update both your operating system and applications regularly. This is a primary prevention method for any cyber attack. This will remove vulnerabilities that hackers tend to exploit. Use trusted and legitimate Anti-virus protection software.
3. Use a firewall and other network security tools such as Intrusion prevention systems, Access control, Application security, etc.
4. Avoid opening emails from unknown senders. Scrutinize the emails you receive for loopholes and significant errors.
5. Make use of a VPN. This makes sure that it encrypts the traffic between the VPN server and your device.

How to Prevent Cyber Attacks?

6. Regularly back up your data. According to many security professionals, it is ideal to have three copies of your data on two different media types and another copy in an off-site location (cloud storage). Hence, even in the course of a cyber attack, you can erase your system's data and restore it with a recently performed backup.
7. Employees should be aware of cybersecurity principles. They must know the various types of cyberattacks and ways to tackle them.
8. Use Two-Factor or Multi-Factor Authentication. With two-factor authentication, it requires users to provide two different authentication factors to verify themselves. When you are asked for over two additional authentication methods apart from your username and password, we term it as multi-factor authentication. This proves to be a vital step to secure your account.
9. Secure your Wi-Fi networks and avoid using public Wi-Fi without using a VPN.
10. Safeguard your mobile, as mobiles are also a cyberattack target. Install apps from only legitimate and trusted sources, make sure to keep your device updated.

Security Mechanism

The mechanism that is built to identify any breach of security or attack on the organization.

Also responsible for protecting a system, network, or device against unauthorized access, tampering, or other security threats. Security mechanisms can be implemented at various levels within a system or network and can be used to provide different types of security, such as confidentiality, integrity, or availability.

Security Mechanism cont..

- **Encipherment (Encryption)** involves the use of algorithms to transform data into a form that can only be read by someone with the appropriate decryption key. Encryption can be used to protect data it is transmitted over a network, or to protect data when it is stored on a device.
- **Digital signature** is a security mechanism that involves the use of cryptographic techniques to create a unique, verifiable identifier for a digital document or message, which can be used to ensure the authenticity and integrity of the document or message.
- **Traffic padding** is a technique used to add extra data to a network traffic stream in an attempt to obscure the true content of the traffic and make it more difficult to analyze.
- **Routing control** allows the selection of specific physically secure routes for specific data transmission and enables routing changes, particularly when a gap in security is suspected.

Security Services

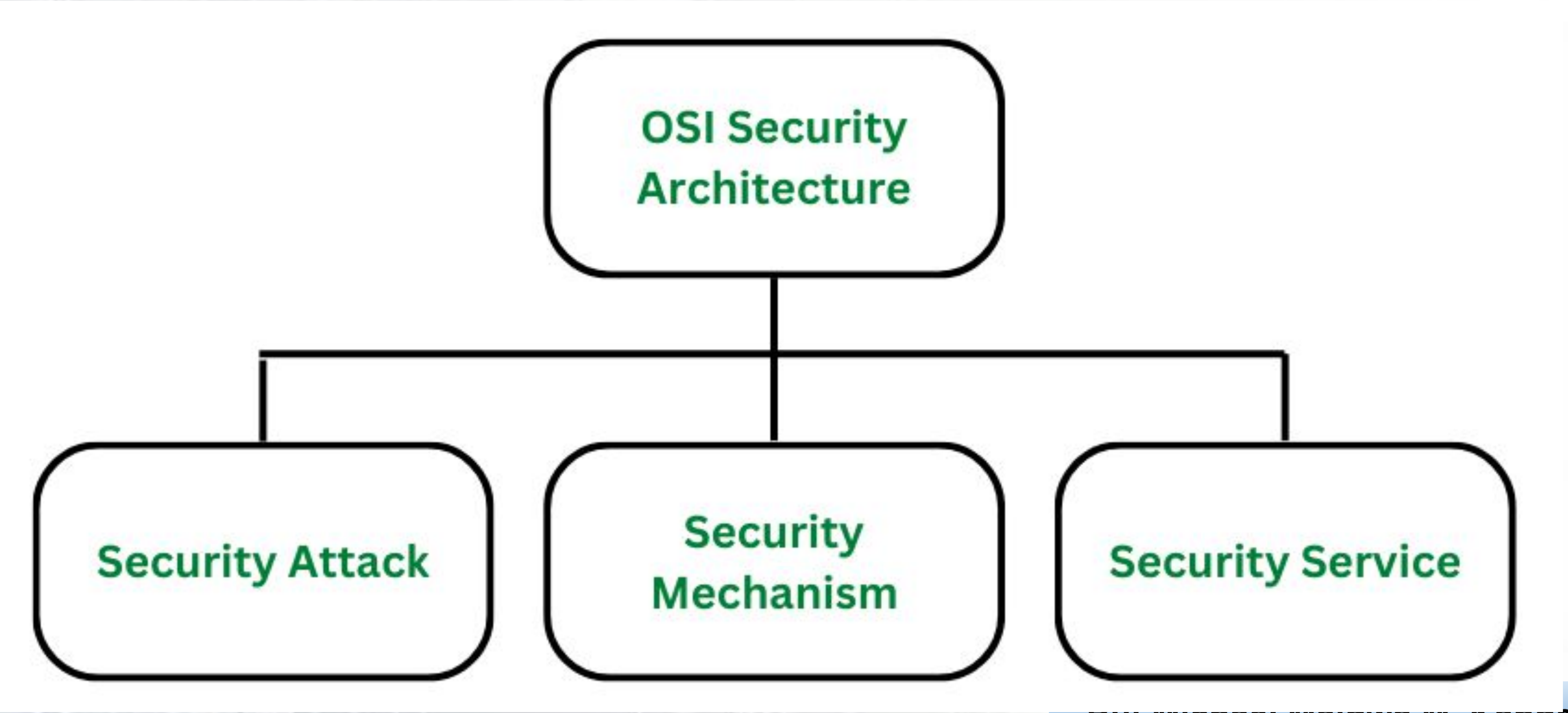
Security services refer to the different services available for maintaining the security and safety of an organization. They help in preventing any potential risks to security. Security services are divided into 5 types:

- **Authentication** is the process of verifying the identity of a user or device in order to grant or deny access to a system or device.
- **Access control** involves the use of policies and procedures to determine who is allowed to access specific resources within a system.
- **Data Confidentiality** is responsible for the protection of information from being accessed or disclosed to unauthorized parties.
- **Data integrity** is a security mechanism that involves the use of techniques to ensure that data has not been tampered with or altered in any way during transmission or storage.
- **Non- repudiation** involves the use of techniques to create a verifiable record of the origin and transmission of a message, which can be used to prevent the sender from denying that they sent the message.

The OSI Security Architecture

he OSI (Open Systems Interconnection) Security Architecture defines a systematic approach to providing security at each layer. It defines security services and security mechanisms that can be used at each of the seven layers of the OSI model to provide security for data transmitted over a network. These security services and mechanisms help to ensure the confidentiality, integrity, and availability of the data. OSI architecture is internationally acceptable as it lays the flow of providing safety in an organization. T

The OSI Security Architecture



OSI Security Architecture

Security Attack

Security Mechanism

Security Service

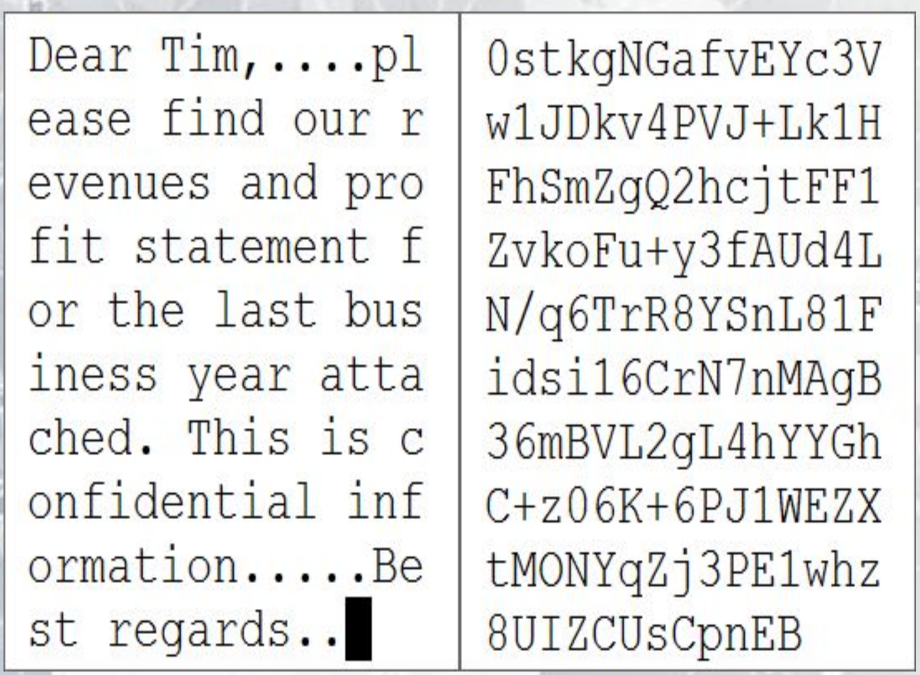
Benefits of OSI Architecture

Below listed are the benefits of OSI Architecture in an organization:

1. **Providing Security:**
   - OSI Architecture in an organization provides the needed security and safety, preventing potential threats and risks.
   - Managers can easily take care of the security and there is hassle-free security maintenance done through OSI Architecture.
2. **Organising Task:**
   - The OSI architecture makes it easy for managers to build a security model for the organization based on strong security principles.
   - Managers get the opportunity to organize tasks in an organization effectively.
3. **Meets International Standards**:

- Security services are defined and recognized internationally meeting international standards.
- The standard definition of requirements defined using OSI Architecture is globally accepted.

Cryptography



```
Dear Tim,....pl
ease find our r
evenues and pro
fit statement f
or the last bus
iness year atta
ched. This is c
onfidential inf
ormation.....Be
st regards..█
```

```
0stkgNGafvEYc3V
w1JDkv4PVJ+Lk1H
FhSmZgQ2hcjtFF1
ZvkoFu+y3fAUd4L
N/q6TrR8YSnL81F
idsi16CrN7nMAgB
36mBVL2gL4hYYGh
C+z06K+6PJ1WEZX
tMONYqZj3PE1whz
8UIZCUsCpnEB
```

The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form.

Encryption is the process of transforming information in such a way that an unauthorized third party cannot read it; a trusted person can decrypt data and access it in its original form though.

Why Cryptography?

- **Confidentiality**
  - Eyes Only
  - Hide your Stash
  - Secure communication e.t.c
- **Integrity**
  - Data integrity verification

You MIGHT get HACKED!! So relax and Encrypt

Cryptography Terms

Plaintext The original intelligible message

Cipher text The transformed message

Cipher An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods

Key Some critical information used by the cipher, known only to the sender & receiver

Encipher (encode) The process of converting plaintext to cipher text using a cipher and a key

Decipher (decode) the process of converting ciphertext back into plaintext using a cipher and a key

Cryptography Terms cont…

Cryptanalysis The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key. Also called code breaking

Cryptology Both cryptography and cryptanalysis

Code An algorithm for transforming an intelligible message into an unintelligible one using a code-book

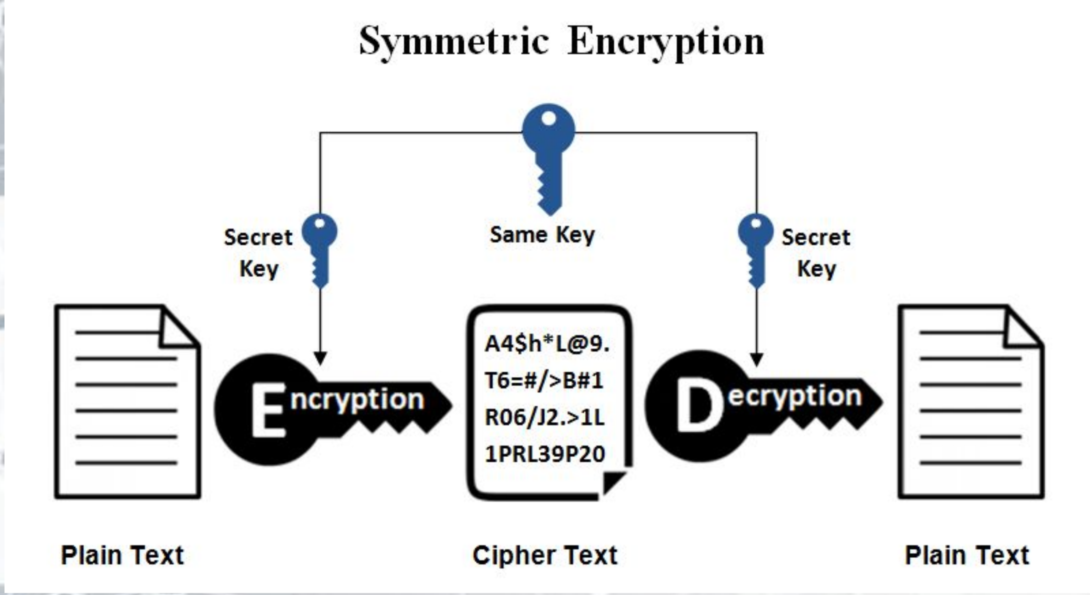
Classification of Ciphers

Classifications of Cyphers Depends on three Factors:

1. **Key Type**
   1. Symmetric (Same Key)
   2. Asymmetric (Different Keys)
2. **Data chunk limits**
   1. Block (For Files)
   2. Stream (For streaming data e.g VOIP, GSM Calls, Radio e.t.c)
3. **Reversibility**
   1. Reversible (File and most types of Encryption Systems)
   2. Non-Reversible (Hashing used in password storage and data verification)

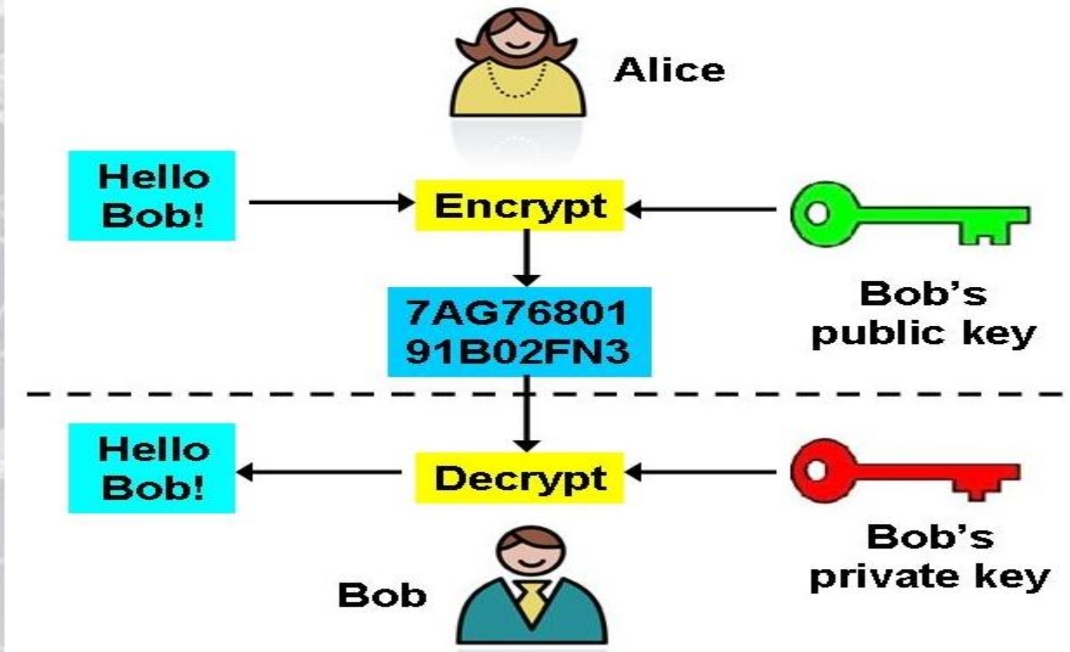
Private (Symmetric) Key Encryption

Uses The Same Key for Encrypting and Decrypting the Message



Public (Asymmetric) Key Encryption

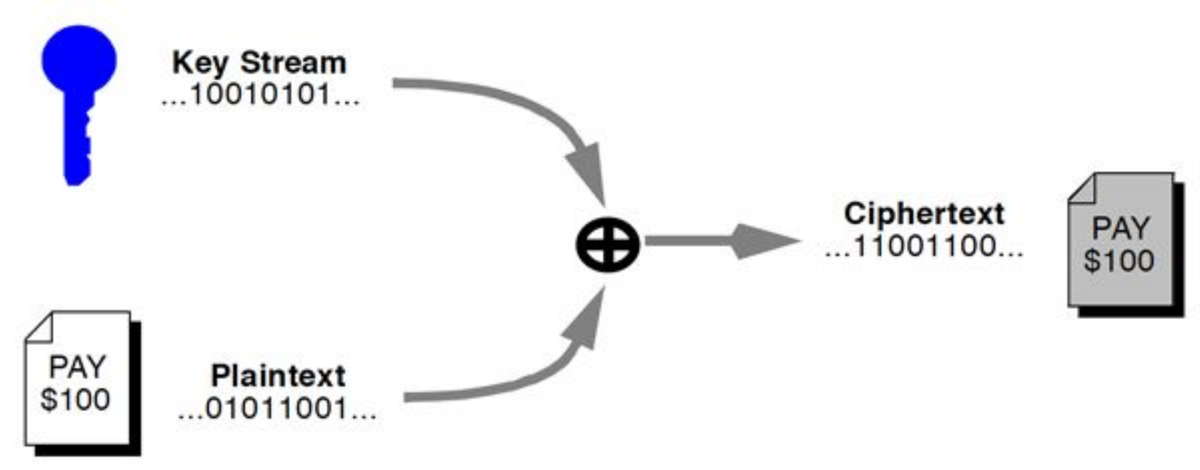
Uses Two Different Keys one for Encrypting the Message and the other For Decrypting the Message



By: Michael Maigwa M. Kangethe

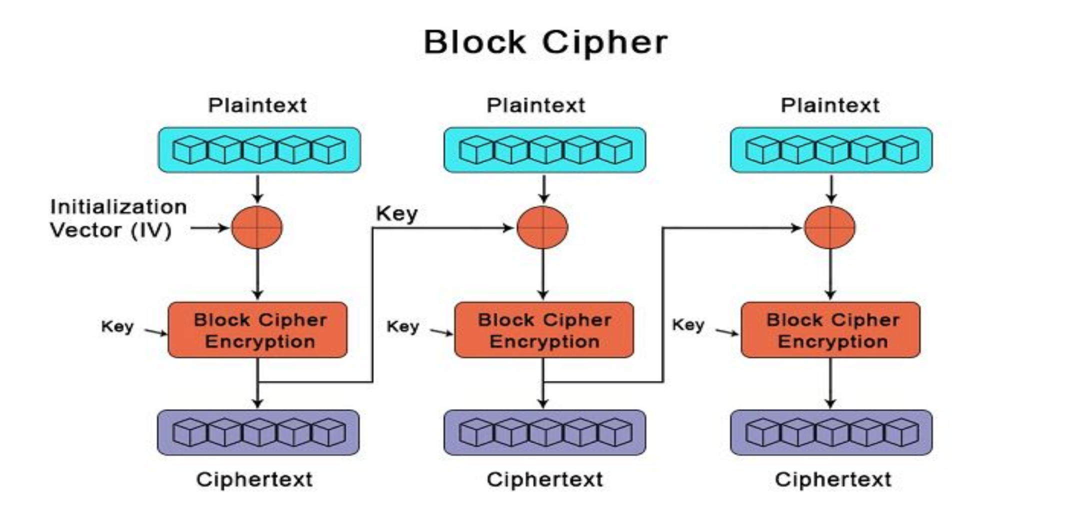
Stream Ciphers

This is where the data is encrypted one bit at a time until the data is no longer transmitted. It is useful for radio communication and streaming data where you do not know the size of the data before hand.



Block Ciphers

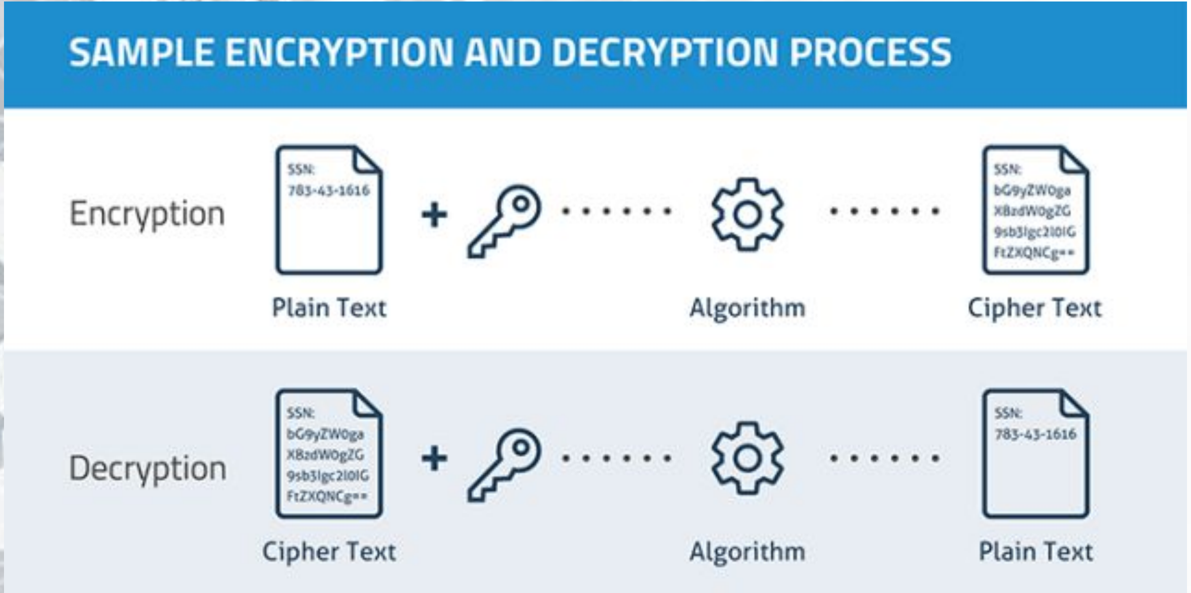
This is where the data is first divided into chunks of a certain bit size e.g 128 bits then each chunk is encrypted one chunk at a time until the whole file is encrypted. It is useful for file and storage encryption where you do know the size of the data before hand.



By: Michael Maigwa M. Kangethe

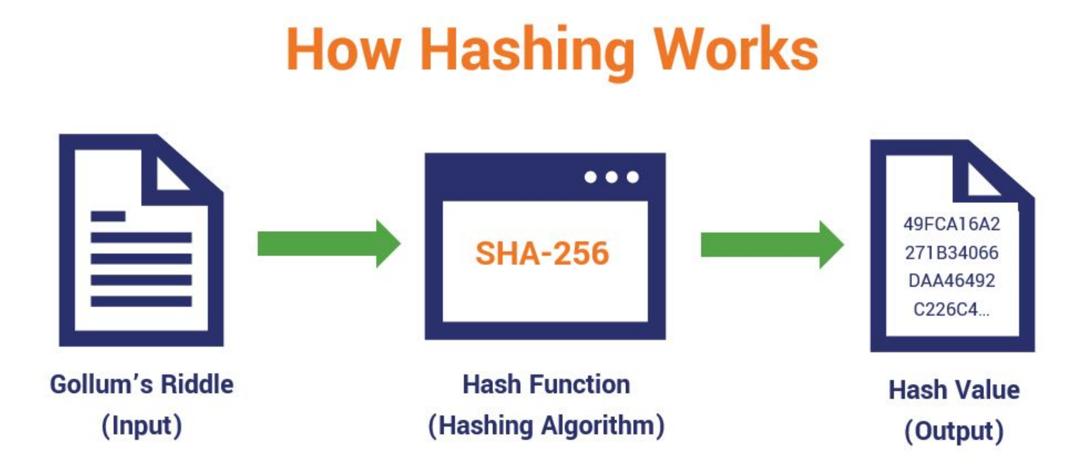
Reversible Encryption

This is the most common type of encryption. It is the type of encryption where you can reverse the encryption process to get the original plaintext data.


SAMPLE ENCRYPTION AND DECRYPTION PROCESS
Encryption
SSN: 783-43-1616
Plain Text
+
Algorithm
SSN: bG9yZW0ga XBzdW0gZG 9sb3Igc2l0IG FtZXQNCg==
Cipher Text
Decryption
SSN: bG9yZW0ga XBzdW0gZG 9sb3Igc2l0IG FtZXQNCg==
Cipher Text
+
Algorithm
SSN: 783-43-1616
Plain Text

Non-Reversible Encryption (Hashing)

This is the mostly used for password storage so that you prevent even the system owners from knowing what your password is. It is the type of encryption where you cannot reverse the encryption process to get the original plaintext data once you have encrypted the data.



Tools used in Practical Labs

- Wireshark
- Metasploit
- Airmon-ng
- BurpSuite
- Nginx
- mitmproxy
- https://grabify.link/
- Most if not All tools can be found packaged with the Kali Linux/Parrot OS

References

- https://thrivedx.com/resources/article/25-cyber-security-terms
- https://www.geeksforgeeks.org/osi-security-architecture/
- https://www.splunk.com/en_us/blog/learn/vulnerability-vs-threat-vs-risk.html#:~:text=Vulnerability%20vs%20threat%20vs%20risk&text=In%20short%2C%20we%20can%20see,when%20the%20threat%20does%20occur
- https://www.bitsight.com/blog/cybersecurity-vs-information-security#:~:text=If%20you're%20in%20information,data%20from%20unauthorized%20electronic%20access
- https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks
- https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks
- https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity
- https://www.comptia.org/content/articles/what-is-cybersecurity
- https://microage.ca/cybersecurity-layering-approach/