



Security

IT security, Part. 1

What is meant by the term “Cyber”?

Cyber means anything that is digital. It can be your devices that are performing the digital computation. Anything that is related to the Internet falls under the category of Cyber.

While Cyberspace should not be confused with the internet, the term is used to represent identities or events that take place in the communication process itself. For Example, think of a Website, it also exists in CyberSpace. Social interactions whether you do a post, upload a picture or even share a message, these all social interactions exist in Cyber Space and this Cyber Space is expanding not in minutes but in seconds.

What is Cyber Security?

- Cybersecurity refers to the technologies and processes designed to protect computers, networks, and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cybercriminals
- Cybersecurity is necessary since it helps in securing data from threats such as data theft or misuse, also safeguards your system from viruses
- With an increasing amount of people getting connected to the Internet, the security threats that cause massive harm are increasing also.

Security vs Information Security

- Security can be of any physical security, it includes everything in security and Information Security can be of any digital security and is bounded to information..

Security vs Network Security

- Information Security(IT) is of wider scope, it includes web, network anything related to IT, and network security is bounded to network. **System Security** includes security of devices like mobile phones, computers, etc.

Cyber Security vs IT Security

- Cyber Security includes digital security and IT security includes cybersecurity and also includes the physical security of systems highest which cybersecurity doesn't include physical security of systems.

Note: InfoSec is short for Information Security and Pentest is short of Penetration Testing.

Domains of Cyber Security

Access Control
Systems and
Methodology

Telecommunications
and Network
Security

Business Continuity
Planning and
Disaster Recovery
Planning

Security
Management
Practices

Security
Architecture and
Models

Law, Investigation,
and Ethics

Application and
Systems
Development
Security

Cryptography

Computer
Operations Security

Physical Security

1-Access Control Systems and Methodology

- The main purpose of Cyber Security is to protect your data. So first will get to know more about Data and what are the various access control systems and methodology.

Six Dimensions of Data Quality Assessment:

A Data Quality(DQ) Dimension is a recognized term used to describe the feature of data that can be assessed or measured against defined standards in order to measure the quality of data.

The six core data quality dimensions are:

1. Consistency
2. Completeness
3. Correctness
4. Accessibility
5. Timeliness
6. Accuracy

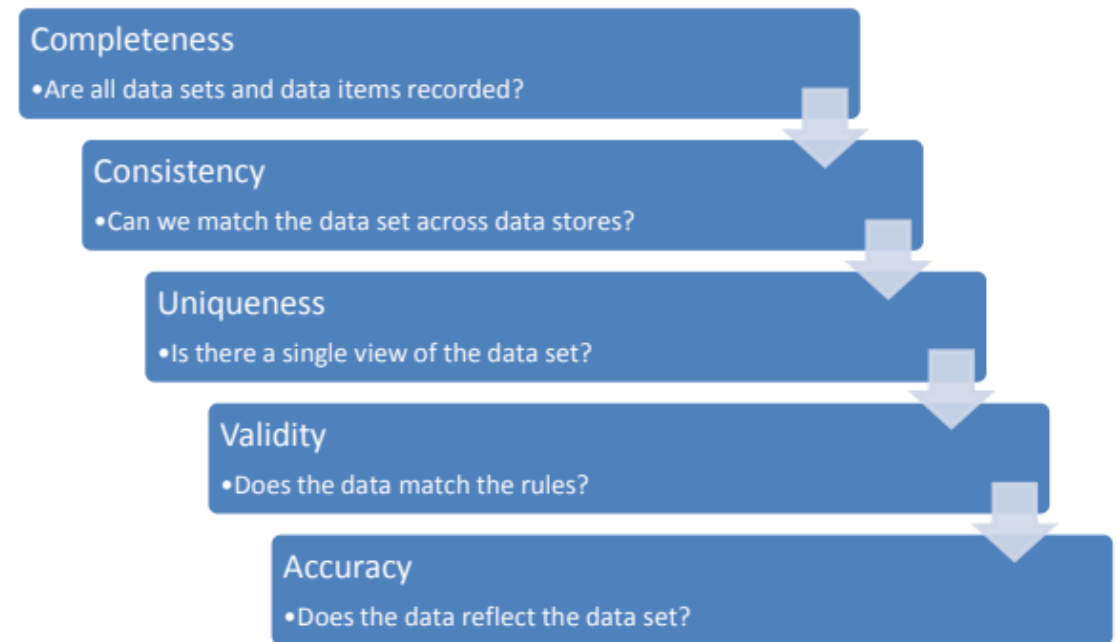


Figure 1 - Example of the application of different data quality dimensions to a data set

States of Data

Understanding the different states of digital data can be helpful for you to select the different sorts of security measures and encryption techniques to apply on the data. Here we will discuss three states of data.

1- Data at rest/storage:

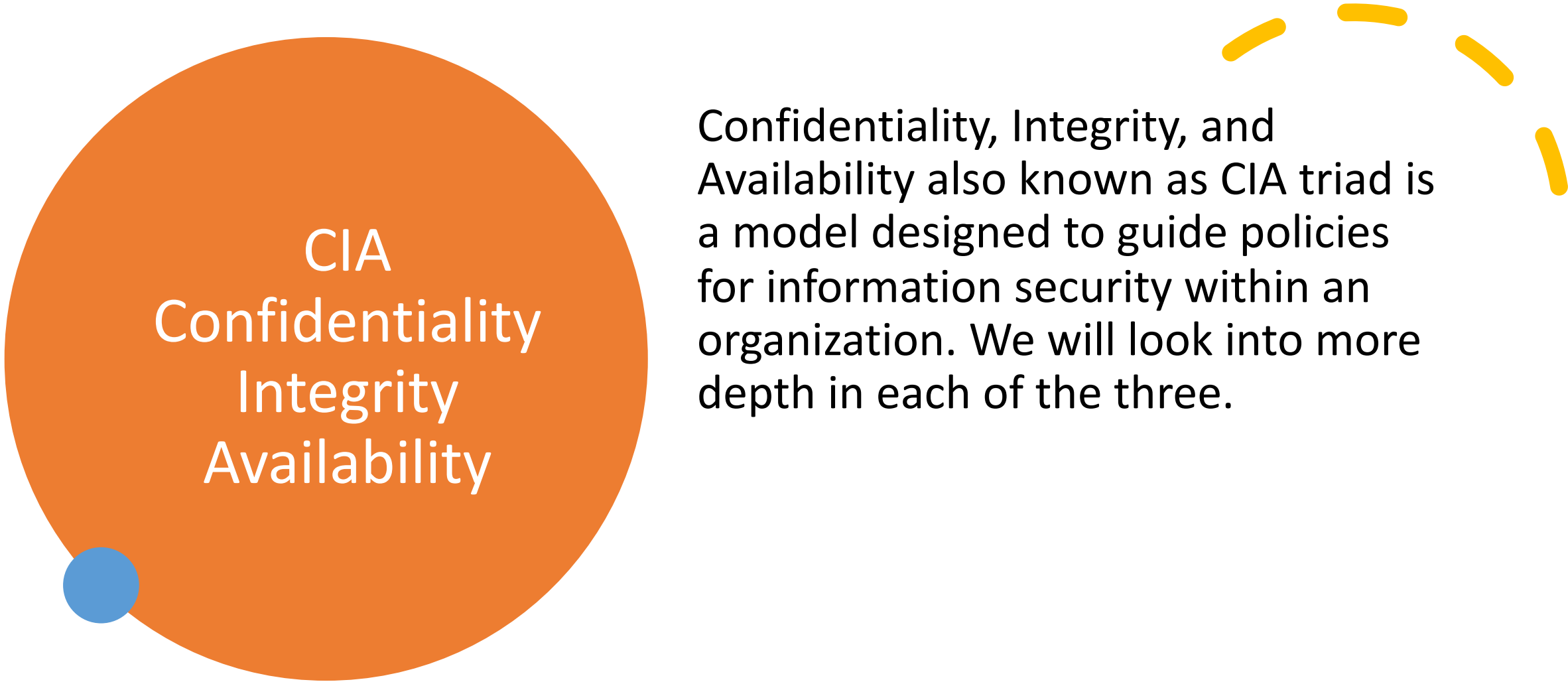
- Data at rest refers to the data that has been stored on some sort of physical medium or backup medium like data stored on hard disks or even in mobile devices. What makes its data at rest that data is in an inactive form and is not currently being transmitted or processed.

2-Data in motion/transmission:

- The second phase of data is in motion. Data in motion is currently transmitting on a network or is sitting on a computer's RAM ready to be read, updated, or processed. It can be emails or data transferred through FTP or SSH.

3- Data in process:

- The third phase of data is in process or use. This state of data is not being stored passively on a storage medium. This is the data that is being processed by one or more applications. This is the data currently being generated, updated, appended, or erased.



CIA
Confidentiality
Integrity
Availability

Confidentiality, Integrity, and Availability also known as CIA triad is a model designed to guide policies for information security within an organization. We will look into more depth in each of the three.

1-Confidentiality

- It ensures that computer-related assets are accessed only by authorized parties sometimes called **secrecy** or **privacy**

- Measure undertaken to prevent sensitive information from reaching the wrong people and making sure that an authorized person can access it.

- Technique used is **Encryption**

Encryption to ensure Confidentiality

Suppose we want to word “HELLO” , we can apply encryption technique to replace every alphabet of HELLO with its neighbor alphabet like H replace with I, E with F, etc which makes the word not meaningful. Then we decrypt with the same technique used on another side

Bitlocker is a disk/drive-level encryption. We cannot apply BitLocker on file.

Windows use the NTFS file system. There is **EFS(Encrypted File System)-File Level Encryption**. Right-click on file (Compress the contents in blue color).

Features of EFS: There are two colors that show encryption and decryption.

This whole process depends on Policies. To keep backup of data. When an employee resigns the company formats the system which also loses the BitLocker keys and other stuff.

Encryption & Decryption



Types of Encryption

There are two top-level types of encryption. Symmetric and Asymmetric

1-Symmetric Encryption :

Uses the Same Key to encrypt or decrypt data.

Consider a desktop password manager application. You enter your password and they encrypted with your own personal key. When the data is to be retrieved, the same key is used, and the data is decrypted

2-Asymmetric Encryption:

Uses a Private key and Public Key pair.

Either key can encrypt but a single key can't decrypt its own encrypted data. To decrypt, you need the paired key.

Asymmetric encryption is used for things like Transport Layer Security(TLS) used in HTTPS and data signing



Access Controls

Access controls authenticate and authorize individuals to access the information they are allowed to see and use

Something you know — (you know passwords)

Something you are — (biometric scan)

Something you have — (ATM card)

Something you do — (signature style)

Integrity of Data

Integrity: It means that assets be modified only by authorized parties or only in authorized ways. Ensures that information is in a format that is true and correct to its original purposes. It involves maintaining the consistency, accuracy, and trustworthiness of data in its entire life cycle.

The technique used is **Hash**

Hash

- **Hash: Hash Calculator** which takes a file as input and applies algorithm. The purpose of hashing is to show that the original file is not modified.
- Let's have a practical implementation of hashing using the Microsoft File Checksum Integrity Verifier. You can download it from the internet.

Microsoft File Checksum Integrity Verifier

Important! Selecting a language below will dynamically change the complete page content to that language.

Language:

English

[Download](#)

The Microsoft File Checksum Integrity Verifier tool is an unsupported command line utility that computes MD5 or SHA1 cryptographic hashes for files.

[+ Details](#)

[+ System Requirements](#)

[+ Install Instructions](#)

[+ Related Resources](#)

Hash, 1

```
CEO@Haier-PC MINGW64 ~/OneDrive - Microsoft Student Partners/Desktop/fciv
$ fciv readme.txt -sha1
//
// File Checksum Integrity Verifier version 2.05.
//
a0c8d486e74930c8b0969df47d8b80adaeccc20e readme.txt
```

You have to open a command prompt in the directory where your file is located. We will check the integrity of a text file. To apply this hashing technique :

**fciv “filename with the extension” hashing algorithm
=> fciv readme.txt -sha1**

Hash, 2

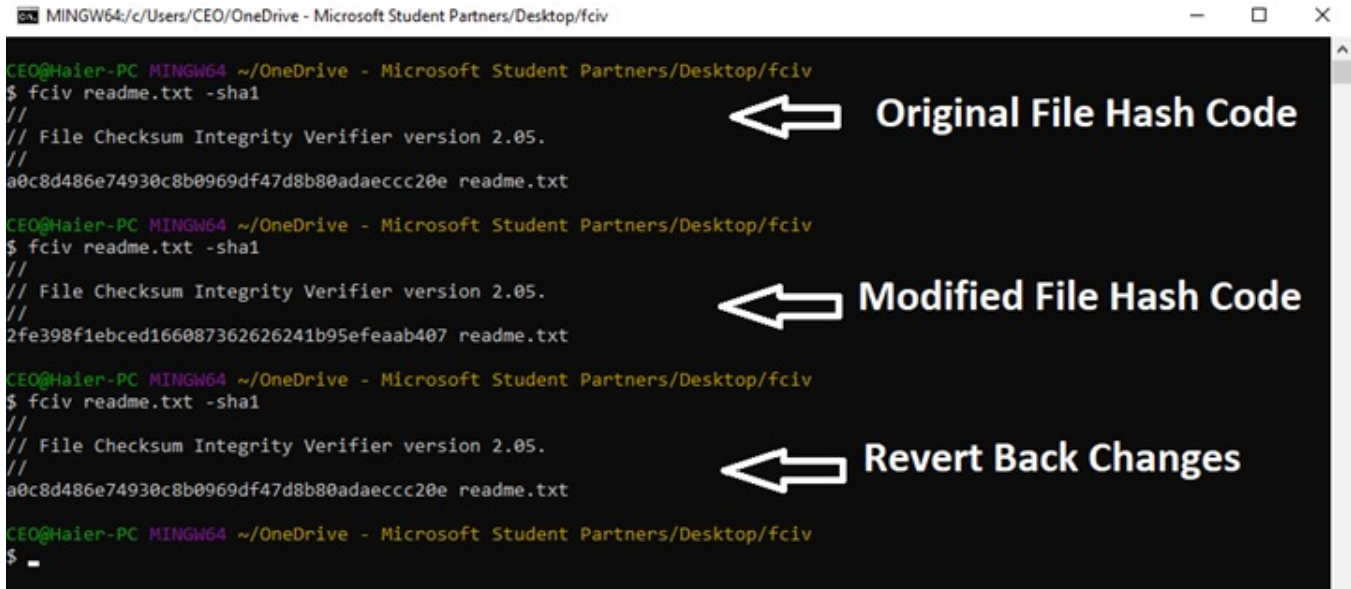
```
CEO@Haier-PC MINGW64 ~/OneDrive - Microsoft Student Partners/Desktop/fciv
$ fciv readme.txt -sha1
//
// File Checksum Integrity Verifier version 2.05.
//
a0c8d486e74930c8b0969df47d8b80adaeccc20e readme.txt

CEO@Haier-PC MINGW64 ~/OneDrive - Microsoft Student Partners/Desktop/fciv
$ fciv readme.txt -sha1
//
// File Checksum Integrity Verifier version 2.05.
//
2fe398f1ebced1660873626241b95efeaab407 readme.txt
```

Here you can see a Hash code generated of that file. Now we will modify the file by adding some letters in the text file and will again apply the hashing technique on the same file.

Hash, 3

Here you can see a Hash code generated of that file. Now we will modify the file by adding some letters in the text file and will again apply the hashing technique on the same file.



```
MINGW64/c/Users/CEO/OneDrive - Microsoft Student Partners/Desktop/fciv
CEO@Haier-PC MINGW64 ~/OneDrive - Microsoft Student Partners/Desktop/fciv
$ fciv readme.txt -sha1
//
// File Checksum Integrity Verifier version 2.05.
//
a0c8d486e74930c8b0969df47d8b80adaeccc20e readme.txt

CEO@Haier-PC MINGW64 ~/OneDrive - Microsoft Student Partners/Desktop/fciv
$ fciv readme.txt -sha1
//
// File Checksum Integrity Verifier version 2.05.
//
2fe398f1ebced1660873626241b95efeaab407 readme.txt

CEO@Haier-PC MINGW64 ~/OneDrive - Microsoft Student Partners/Desktop/fciv
$ fciv readme.txt -sha1
//
// File Checksum Integrity Verifier version 2.05.
//
a0c8d486e74930c8b0969df47d8b80adaeccc20e readme.txt

CEO@Haier-PC MINGW64 ~/OneDrive - Microsoft Student Partners/Desktop/fciv
$ _
```

Original File Hash Code

Modified File Hash Code

Revert Back Changes

Hashing technique

A plaintext on which a hash function has been applied and after applying hash function it generates a hashed text. This hashing technique is also being used in Cyber Forensics.

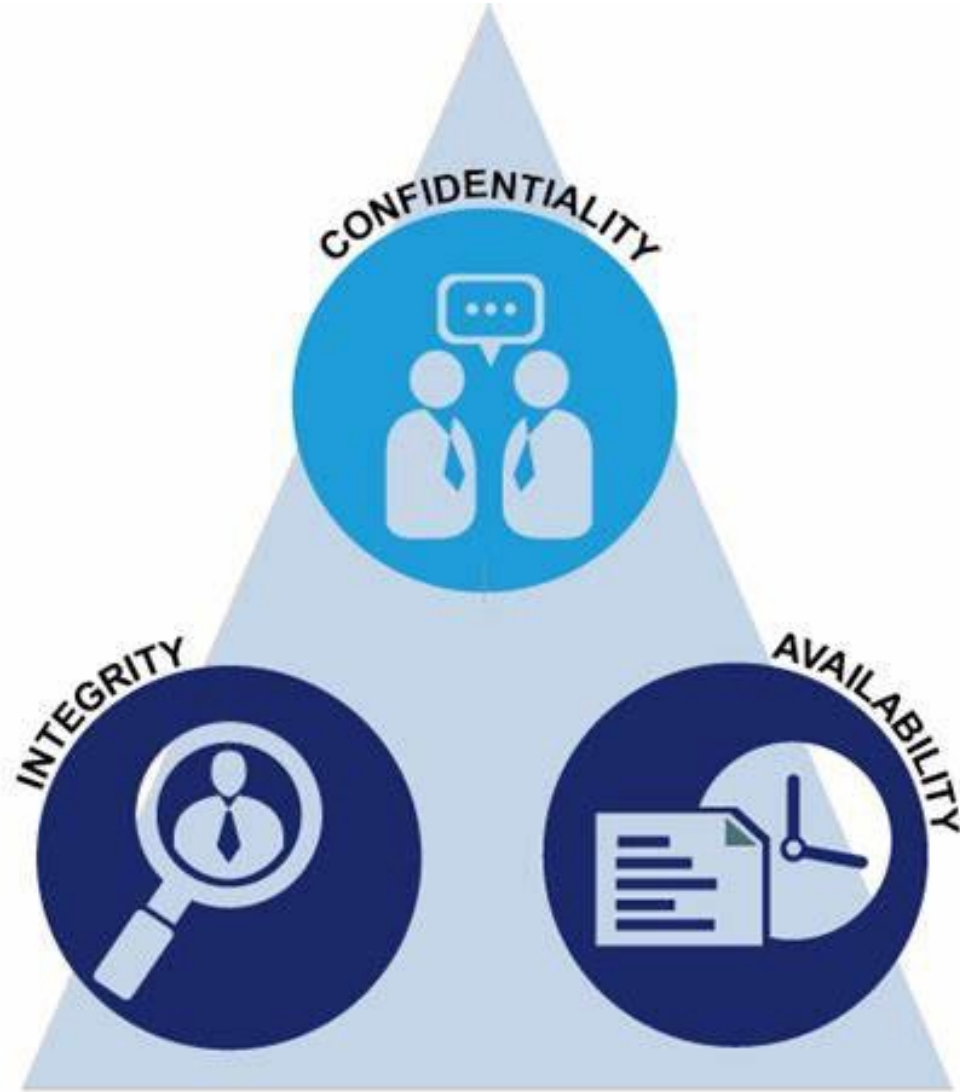


Availability of Data

- It means that assets are accessible to authorized parties at appropriate times. High Availability(99.9%) where 0.1% is error rate ,and when increased 99.999 uptime and 0.0001 error rate.It is implemented using methods such as hardware maintenance, software patching, and network optimization.
- A classic example of a loss of availability to a malicious actor is a **Denial of Service Attack (DOS)**.

SLA

SLA: Service Level Agreement is a binding document. It is a commitment between a service provider and a client. Particular aspects of service — quality, availability, responsibilities are agreed between the service provider and service user. If the service user doesn't receive files in time then service providers are fined.



Ping command

Ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol network. A simple way to verify that a computer can communicate over the network with another computer or network device

Ping 127.0.0.1 (127.0.0.1 is a loopback address)

```
C:\Users\CEO>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```


Types of DOS Attacks

Will discuss a few of the DOS Attacks

0 - Physical DoS

1 - Ping of Death

2 - Ping of Flood

3 - Smurf Attack

4 - Fraggle Attack

5 - The LAND Attack

6 - Distributed Denial of Service (DDoS) Attacks

Physical DOS

- If the attacker has physical access to the system, he or she can create a DoS by physically taking the system offline. This would entail unplugging the system or damaging it in a way that it no longer functions as intended.

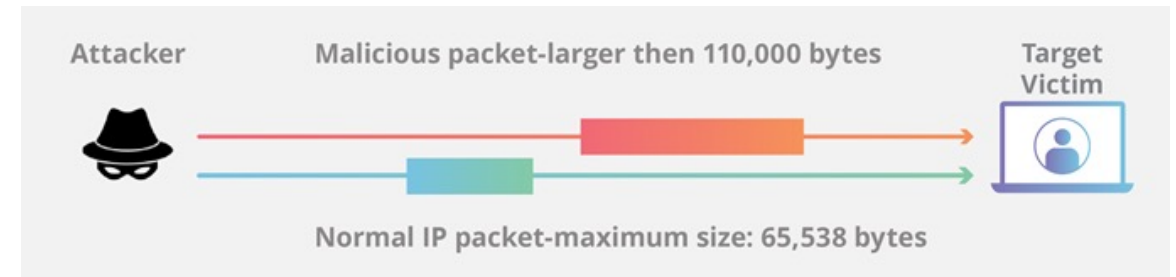
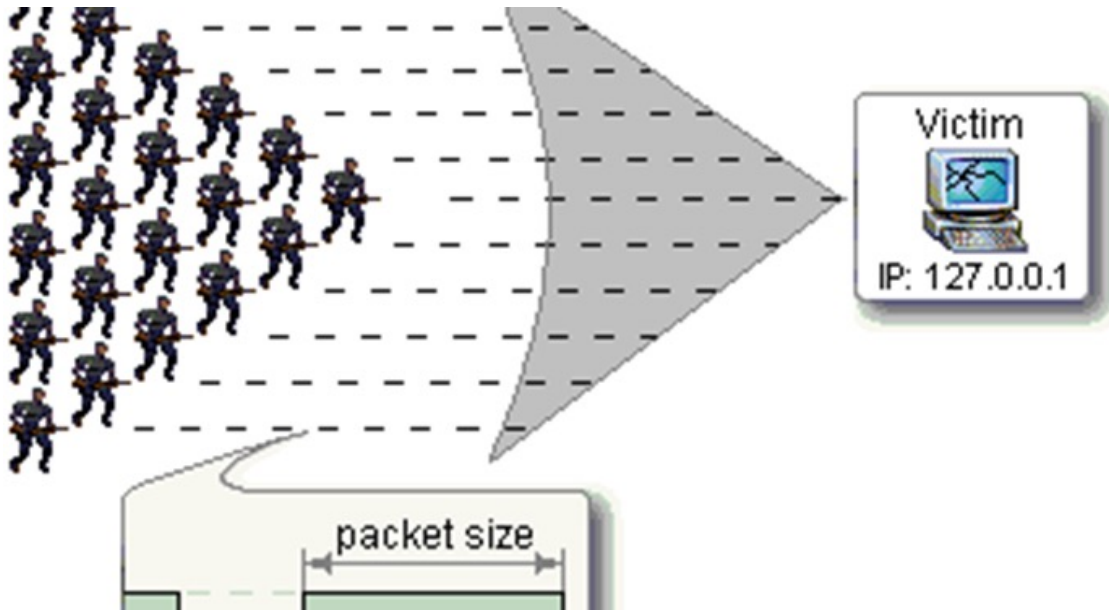


Logical DoS

- In an alternative approach, the attacker gains logical access to the system, allowing the attacker to misconfigure the target system. In a logical access scenario, let's take a wireless gateway router, for instance, which sits on the edge of the network. This wireless gateway router is responsible for providing Internet access to the computers on its LAN connection. Hypothetically speaking, we'll also say that the router's administrator left the router's username and password in its default settings. If the attacker logs into the router via a Web interface connection using the default credentials, then the attacker leaves the administrator no chance.
- There is a well-known saying that if the attacker can gain physical access to your device, there is little you can do to secure it from him. Such is the case in this wireless gateway router scenario. Once logged into the router, the attacker can reset the login credentials to the router, effectively blocking the router's administrator access into the router. From there, the attacker can deny legitimate devices access to the router via MAC address filtering, block access to Web sites, or even reduce the router's built-in firewall settings to nothing. This is a DoS attack.

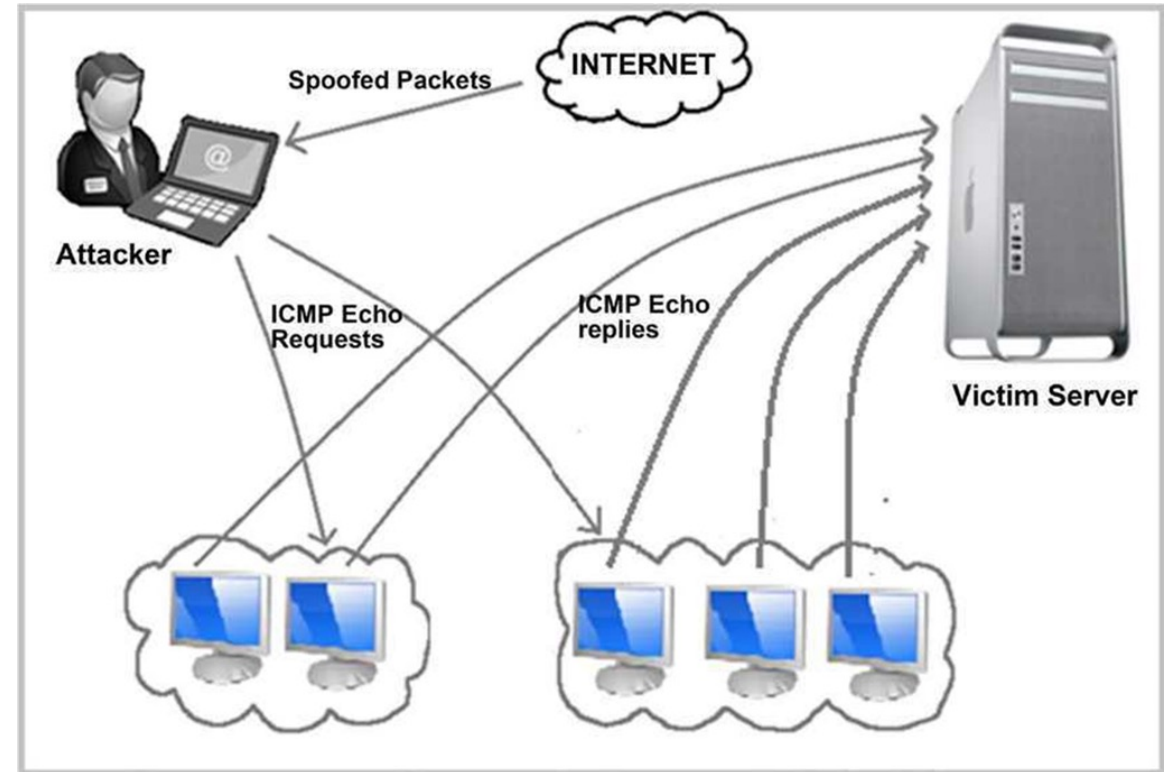
Ping of Death

- A Ping of Death attack is a [Denial of Service](#) (DoS) attack, in which the attacker aims to disrupt a targeted machine by sending a packet larger than the maximum allowable size, causing the target machine to freeze or crash.



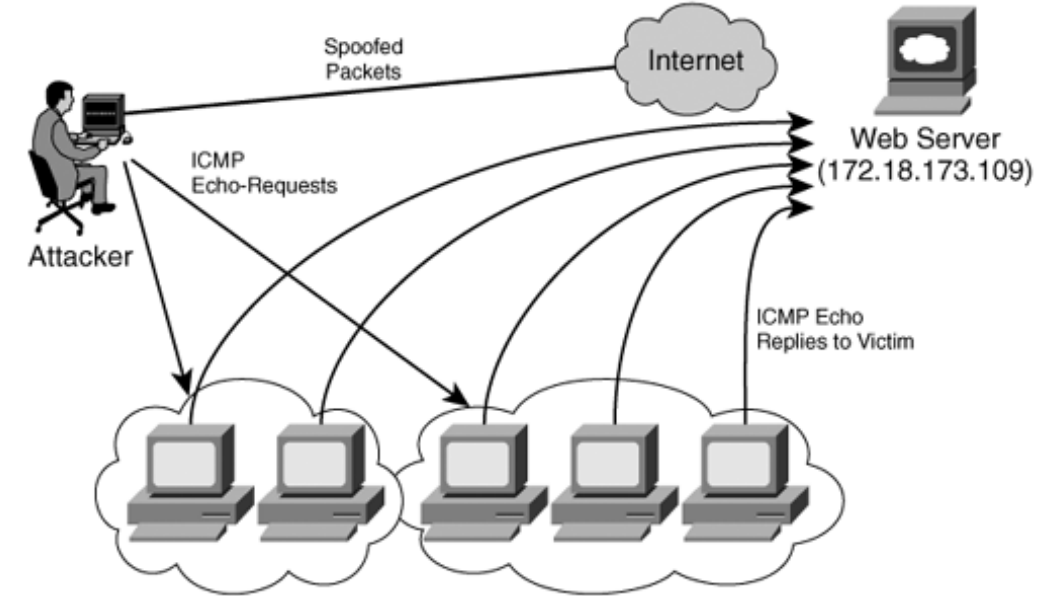
Ping of Flood

- Ping flood, also known as ICMP flood, is a common [Denial of Service](#) (DoS) attack in which an attacker takes down a victim's computer by overwhelming it with ICMP (The Internet Control Message Protocol (ICMP)) echo requests, also known as pings. Example: Education Board Website.



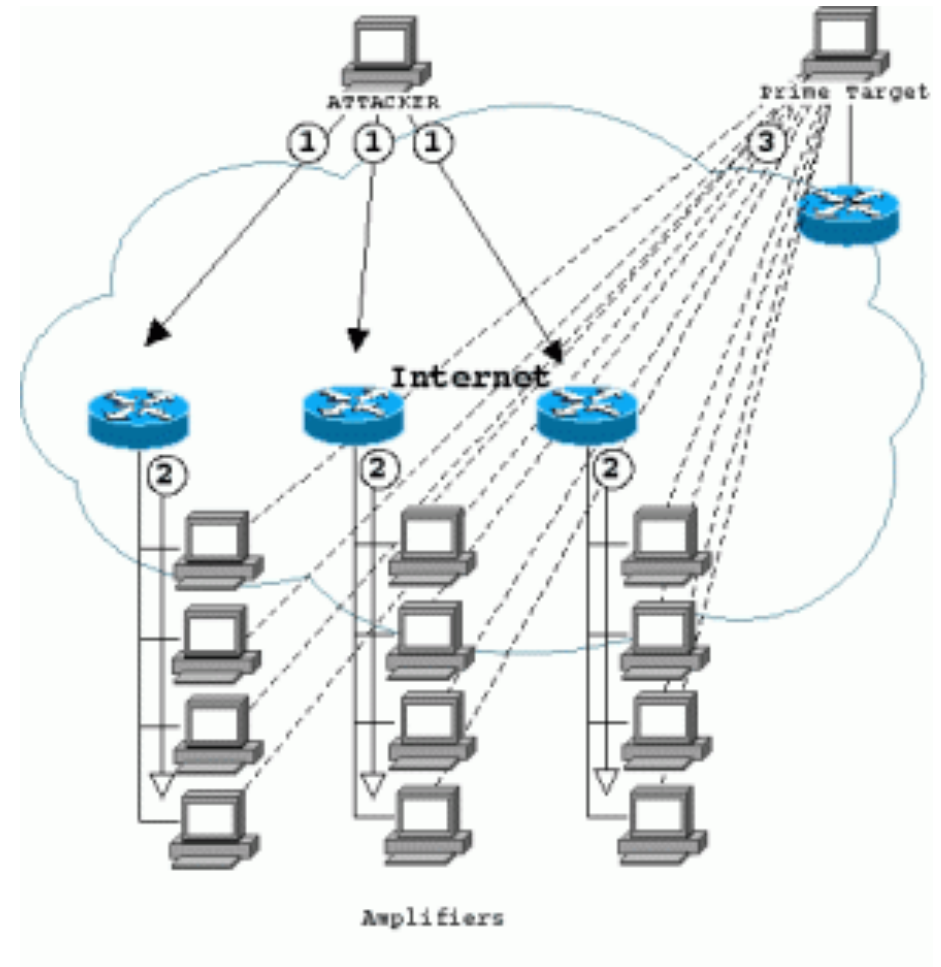
Smurf Attack

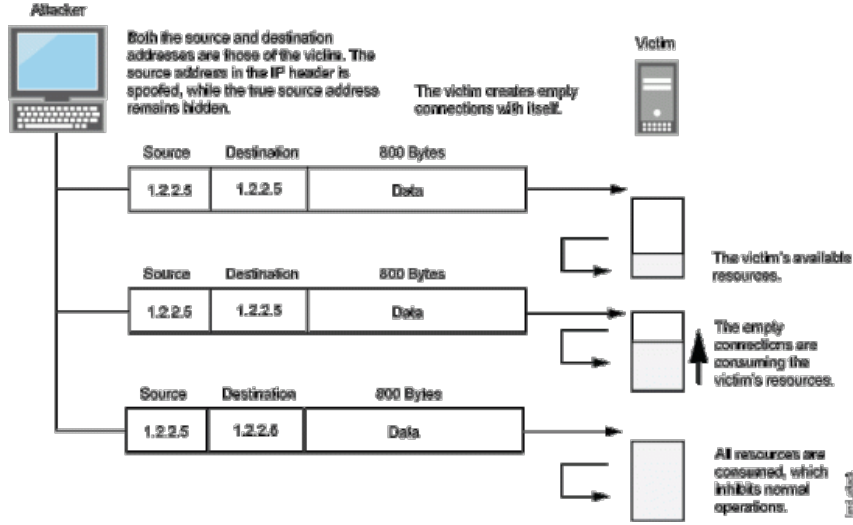
- The “Smurf” attack is a type of DoS attack that abuses ICMP. An ICMP echo request (or ping) is usually unicast. However, in a Smurf attack, the attacker sends the ping out as a broadcast to the network. Every system connected on that network receives this broadcast and should respond back with an echo reply. But, the special thing about the Smurf attack is that the attacker spoofs his source address as the IP address of the target system. The victim, in turn, gets flooded with ICMP echo replies instead. Since the ICMP echo replies are sent to the victim instead, the Smurf attack is considered a type of “Reflected” DoS attack.



Fraggle Attack

- A Fraggle attack is a type of DOS attack, where the attacker sends a large number of spoofed UDP traffic to a router's broadcast address within a network.
- The “Fraggle” attack is similar to the Smurf attack in which the source address is spoofed, but instead of using ICMP, the Fraggle attack sends UDP echoes to a router's broadcast address. The end result is the same as the Smurf attack and, just like with the Smurf attack, the Fraggle attack can be prevented since most routers do not forward broadcast traffic by default.



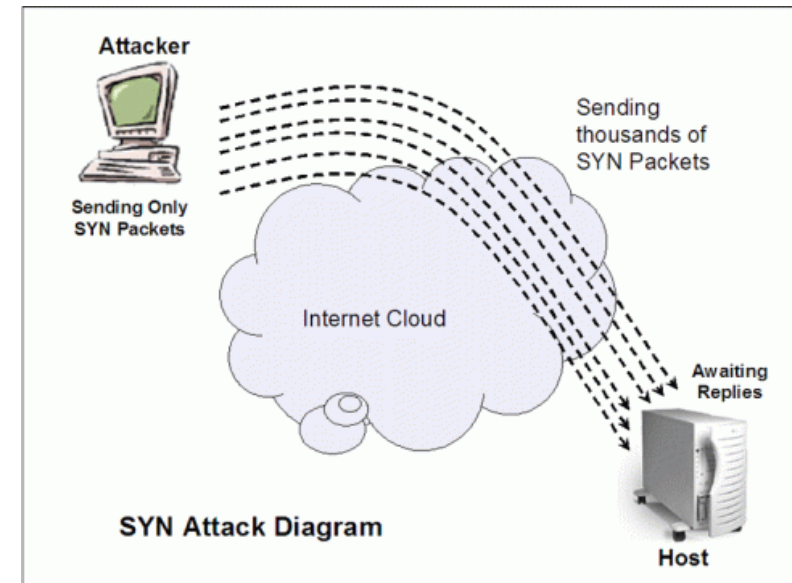


The LAND Attack

- The “Local Area Network Denial” attack, or “LAND” attack, occurs when the attacker floods a system with SYN packets. The source and destination addresses of these SYN packets are spoofed with the target system’s IP address. The target system receives this flood of SYN packets, making it appear as if the target system sent the packets to itself. While the system takes its time to reply to itself, the system becomes unavailable.
- The LAND attack was first discovered in 1997 and many legacy systems remain vulnerable, such as Windows 95, NT, and XP SP2; however, modern systems have seen patches for remediation. Preventing the LAND attack takes good perimeter security, using firewalls and IDS/IPS to detect and drop this malicious traffic. Router ACLs can also be configured to restrict traffic coming into and out of the network to discard any traffic with identical source and destination addresses, or perhaps packets coming from an unknown network.

Distributed Denial of Service (DDoS) Attacks

- In the TCP SYN Flood attack, the attacking computers send the first SYN packet to the target system. Following the rules of TCP, the target system acknowledges the connection with the SYN/ACK. However, the attacking computers never respond with the last ACK packet, which leaves the connection “half-open.” The connection is kept open, in a “SYN_RECV” state. This is normal since the ACK packet may have been lost due to network problems. However, in the TCP SYN Flood attack, the attacker sends thousands of these half-open connections to the target system. As soon as the system’s buffer or queue becomes full, it stops accepting connections, even from legitimate users. As a result the attacker denies the system’s services.





Conclusion

The term cybersecurity is used to refer to the security offered through on-line services to protect your online information.

Cybersecurity refers to the technologies and processes designed to protect computers, networks, and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cybercriminals

Though, cybersecurity is important for network, data and application security

- Cybersecurity is necessary since it helps in securing data from threats such as data theft or misuse, also safeguards your system from viruses
 - With an increasing amount of people getting connected to the Internet, the security threats that cause massive harm are increasing also.
-