Information Security and Internet Fundamentals

JUNE 2021

प्रगत संगणन विकास केन्द्र

CDAC (CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING), MOHALI

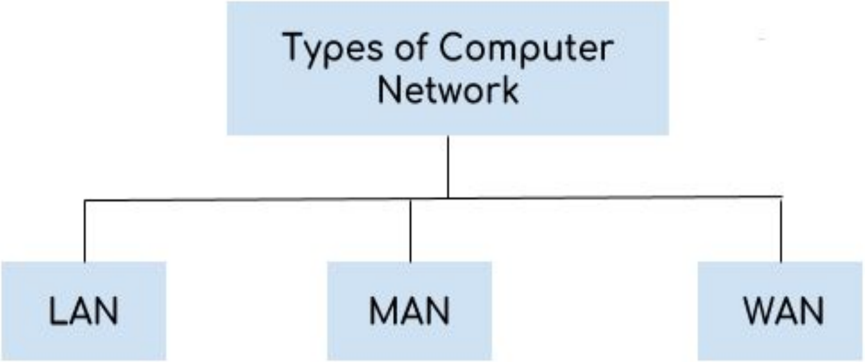
OUTLINES

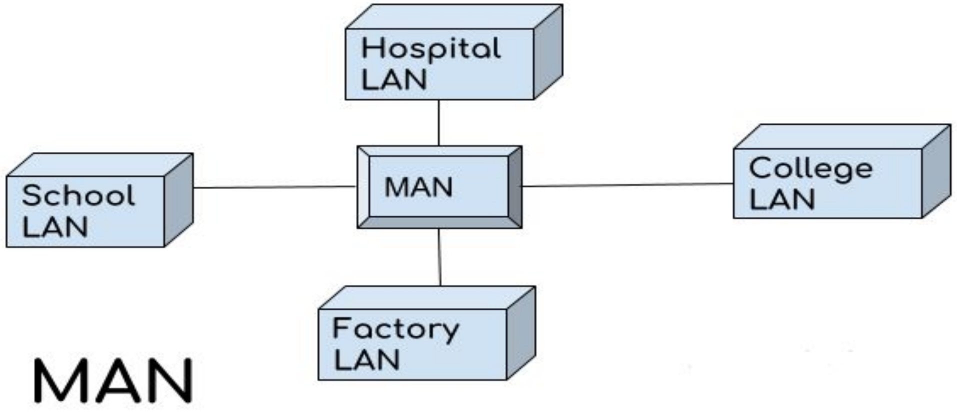
- Internet fundamentals
- Information security
- Basics of Information security
- Analysis of threats and risks
- Cyber security
- Difference between Information, IT and Network security
- Policies of Information Security
- Cyber Security for schools

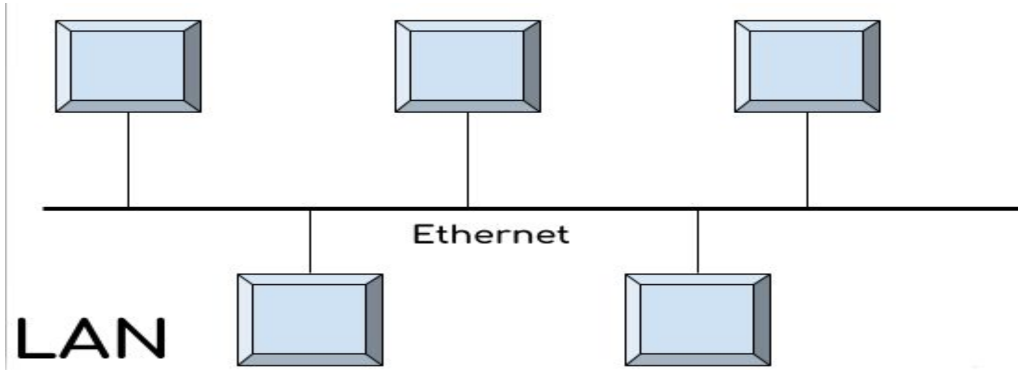
NETWORK AND INTERNET

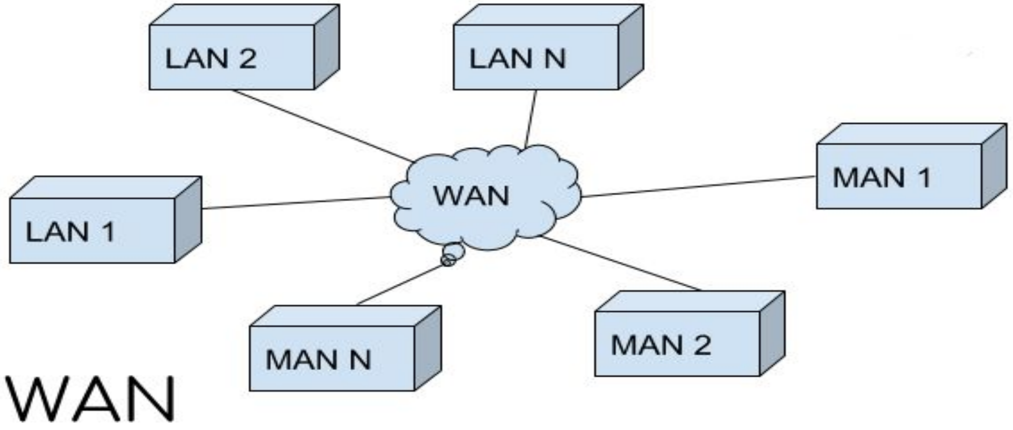
- It is the largest network in the world that connects hundreds of thousands of individual networks all over the world.
- Internet service providers- A commercial organization with permanent connection to the Internet that sells temporary connections to subscribers.
- Examples: Prodigy, America Online, Microsoft network, AT&T Networks.

COMPUTER NETWORK

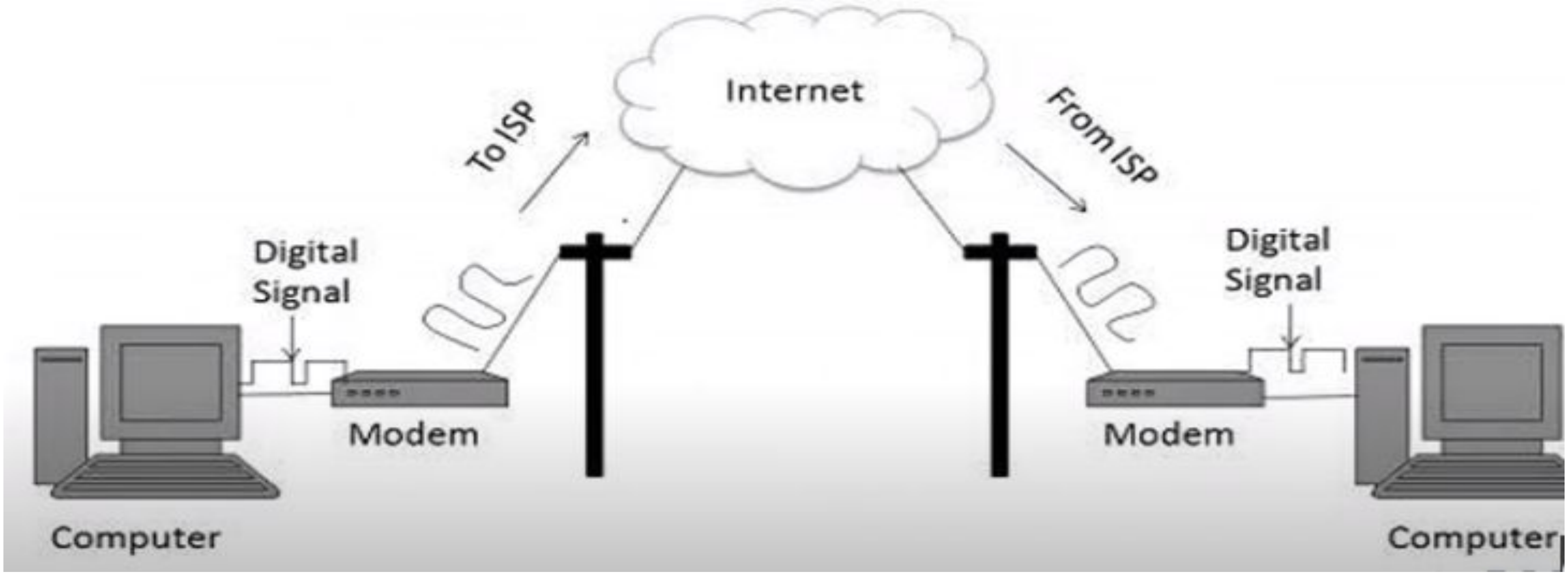








NETWORK AND INTERNET



INTERNET VS INTRANET

IP ADDRESSES

- Each computer running TCP/IP must have a unique IP address
- 32 bit number expressed as 4 denary octets for convenient notation

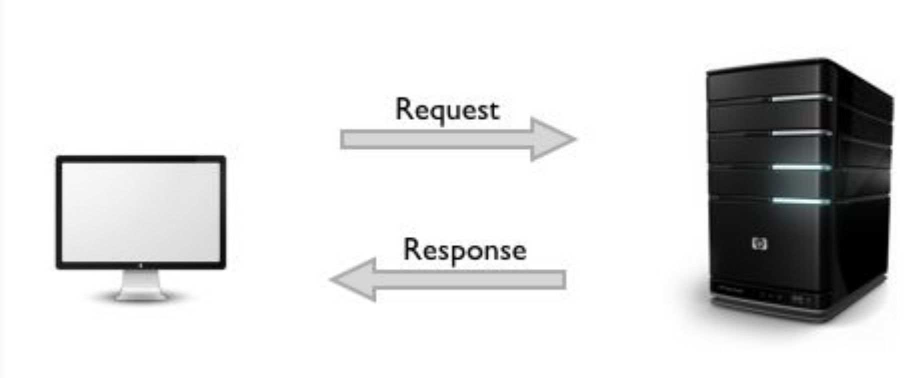
  163.1.125.98
- Computers can be statically or dynamically configured (DHCP)
- Subnet mask identifies computer’s location on network 255.255.255.0
- Default gateway’s IP address provides access to the wider network

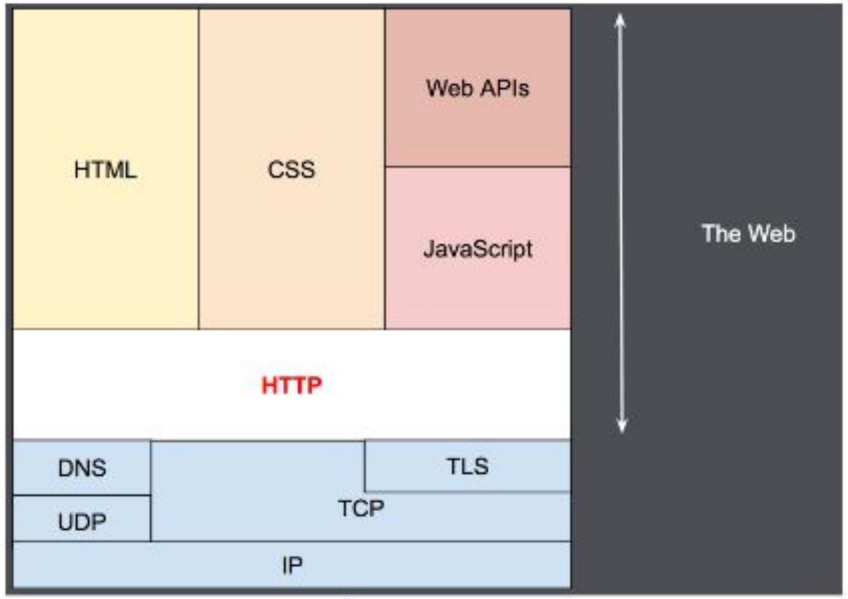
IPv6

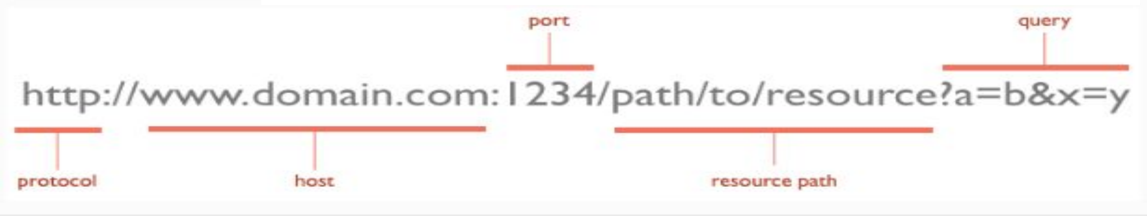
- Most computers still use 32 bit IP addresses, Known as IPv4
- Only 2^{32}(about 4 billion) available addresses
- Gradually switching to 128 bit addresses of IPv6
- Written as eight groups of hexadecimal quartets

UNDERSTANDING THE HTTP PROTOCOL

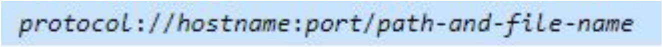
- ❑ HTTP stands for Hypertext Transfer Protocol
- ❑ HTTP is simple, extensible
- ❑ Stateless





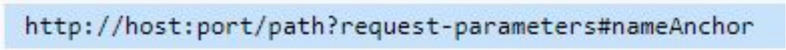


- ❑ URL



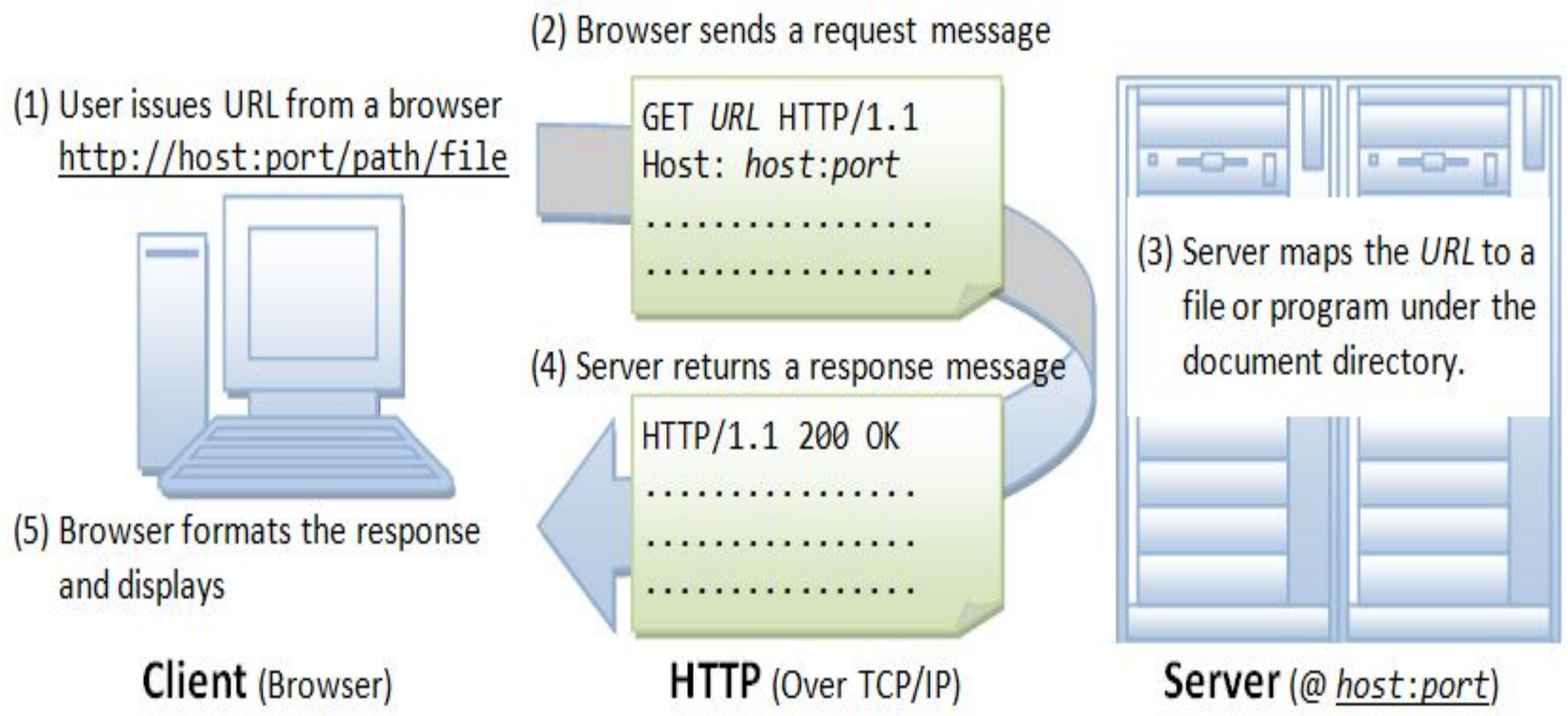
```
protocol://hostname:port/path-and-file-name
```

- ❑ URI



```
http://host:port/path?request-parameters#nameAnchor
```

UNDERSTANDING THE HTTP PROTOCOL



(1) User issues URL from a browser http://host:port/path/file

(2) Browser sends a request message

```
GET URL HTTP/1.1
Host: host:port
.................
.................
```

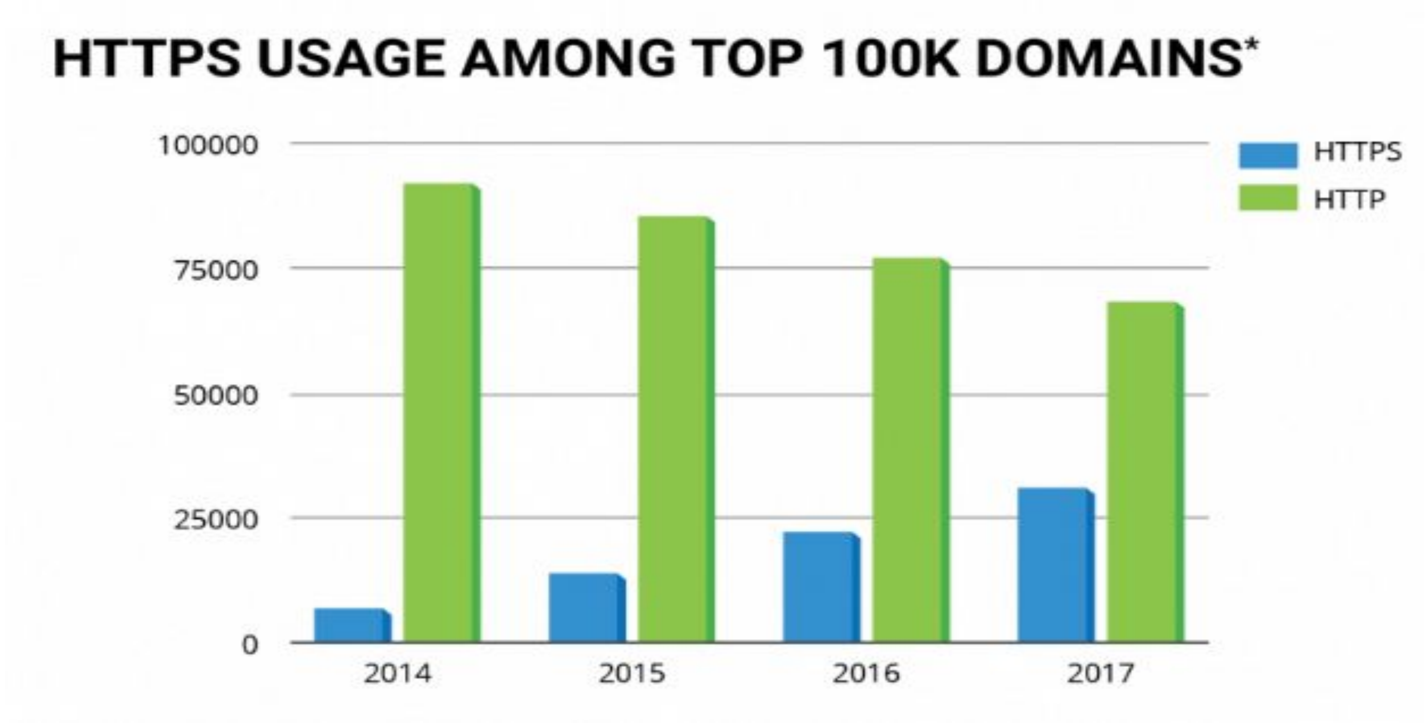
(3) Server maps the *URL* to a file or program under the document directory.

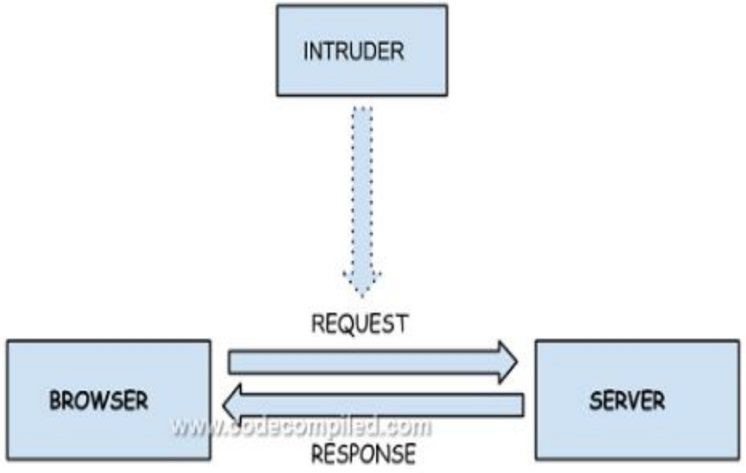
(4) Server returns a response message

```
HTTP/1.1 200 OK
................
................
................
```

(5) Browser formats the response and displays

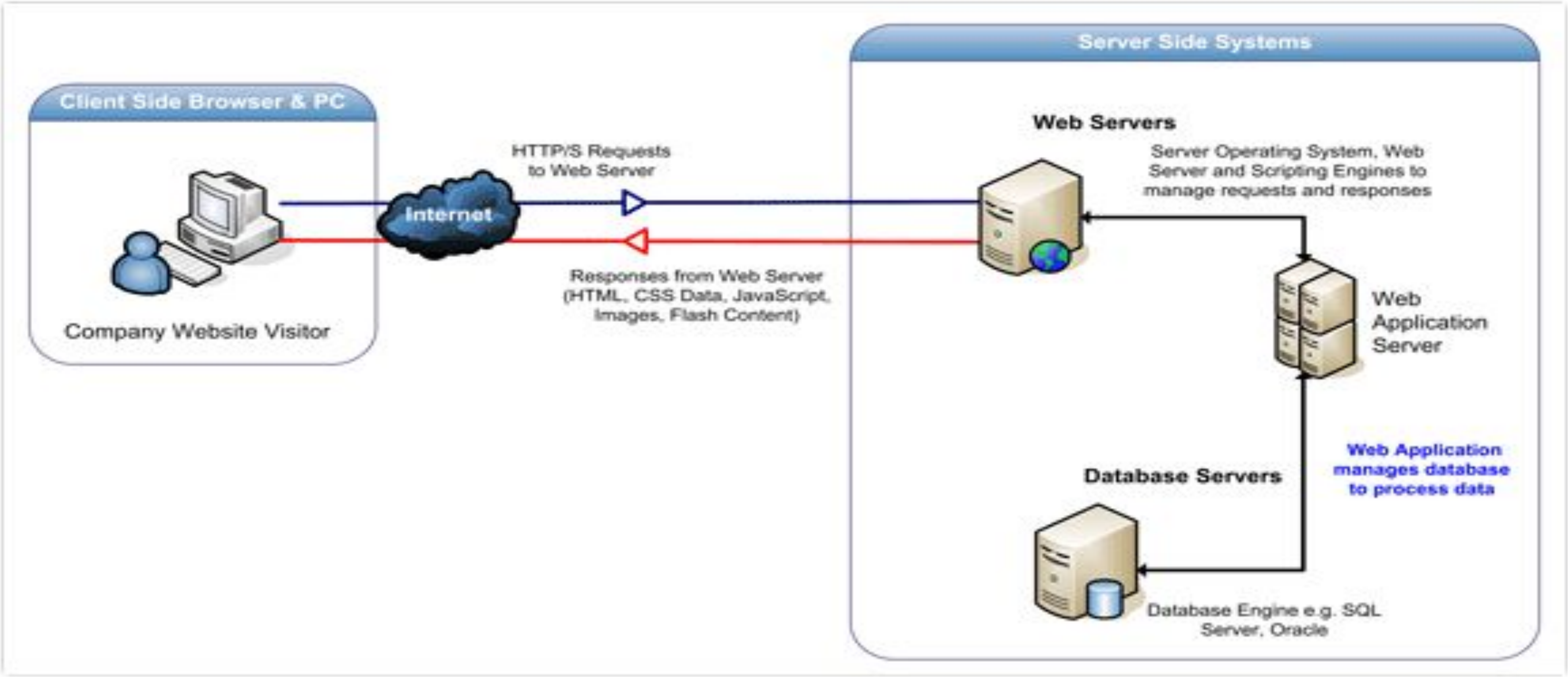
HTTP AND HTTPS



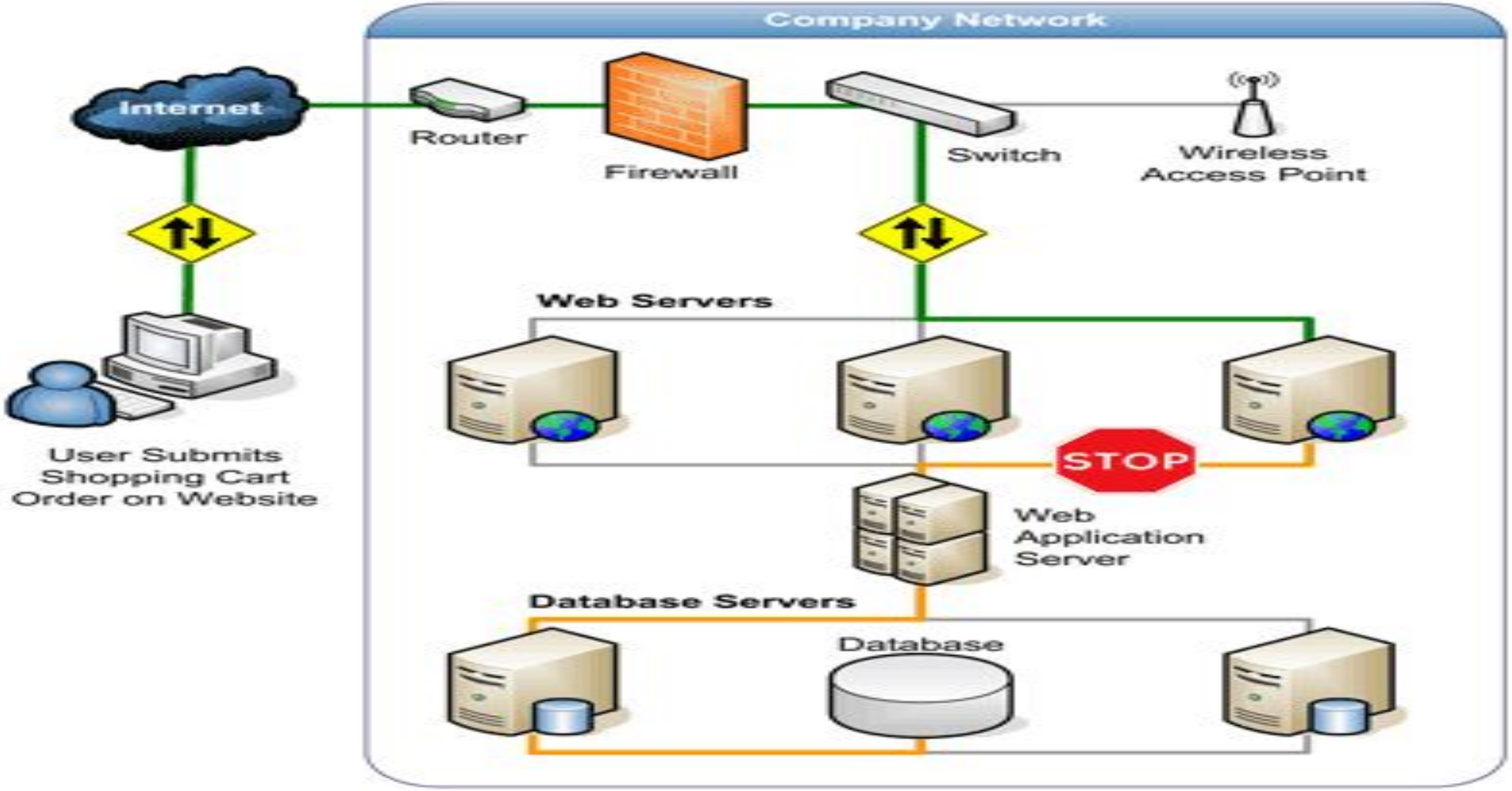


- Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP.

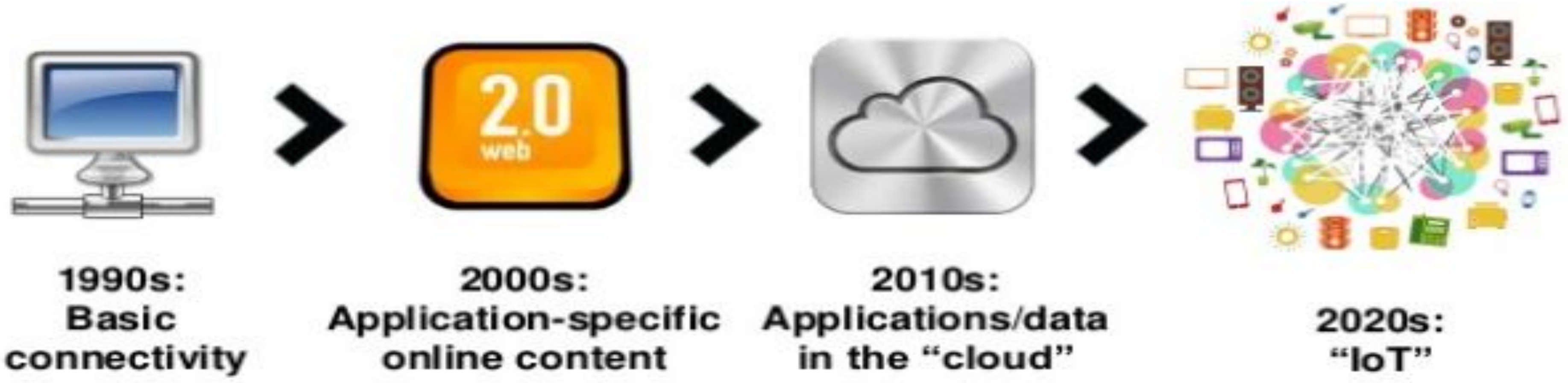
INTERNET COMMUNICATION



HOW A WEB APPLICATION WORKS



AN UNEXPECTED SUCCESS…



1990s:
Basic connectivity

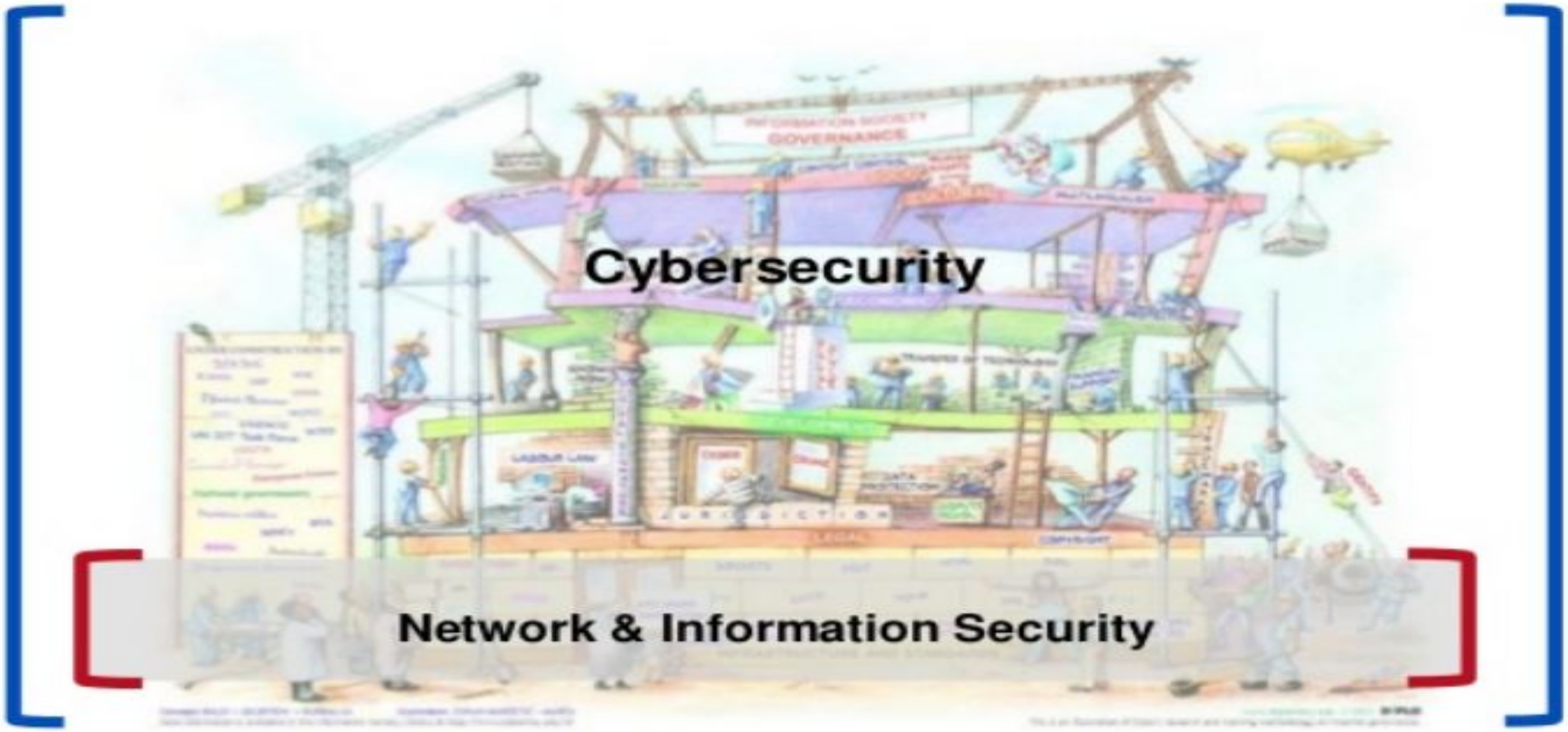
2000s:
Application-specific online content

2010s:
Applications/data in the “cloud”

2020s:
“IoT”

- Evolution of technology, usage and value
- Evolution of security problems and solutions
- Evolution never stops…

THE BIGGER PICTURE



CYBER SECURITY

- Cyber Security means protecting data and information networks. i.e It uses technology for securing IT/ICT products

- Cyber Safety means protecting users from harmful online content. Fundamentally, it focuses on people. It may use technology to help in protecting physical and emotional well being of people.

People Vs. Technolog

IT SECURITY

- Also referred to Computer Security
- It is information security applied to technology
- IT security specialists are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems

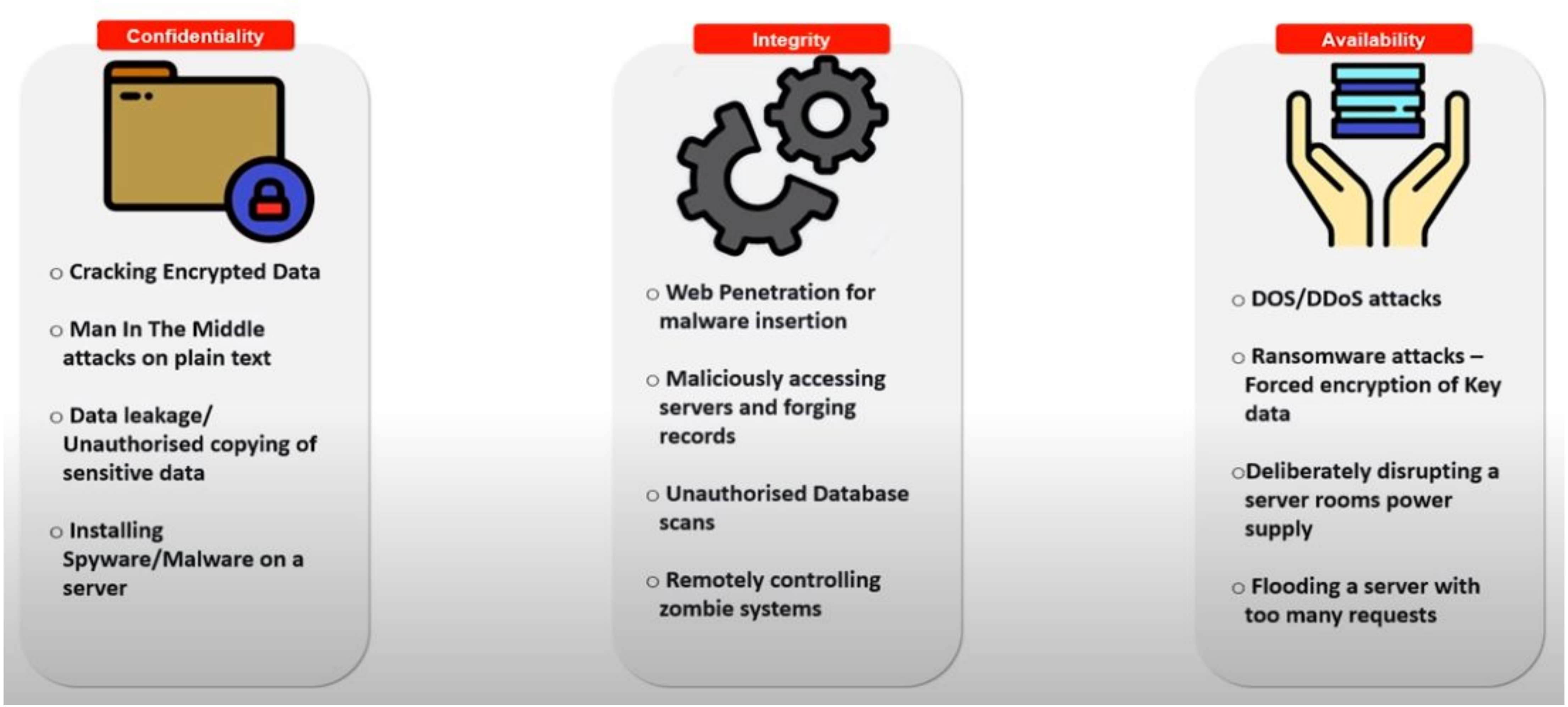
INFORMATION AND INFORMATION SECURITY

- 'Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected‟
- Information Security is the process of protecting the intellectual property of an organization. (Pipkin, 2000)
- Information security is the protection of information and minimizes the risk of exposing information to unauthorized parties.
- Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

WHY INFORMATION SECURITY

- Ensure Availability of Business
- Take care of the risk of loss of Confidentiality, Integrity and Availability of Information Assets
- Protect Data and Information Systems
- Brand and Reputation Loss
- Increased Productivity through best practices
- Higher levels of assurance
- Competitive advantage
- Enable Business Continuity and Disaster Recovery

ATTACK ON CIA



Confidentiality

- Cracking Encrypted Data
- Man In The Middle attacks on plain text
- Data leakage/ Unauthorised copying of sensitive data
- Installing Spyware/Malware on a server

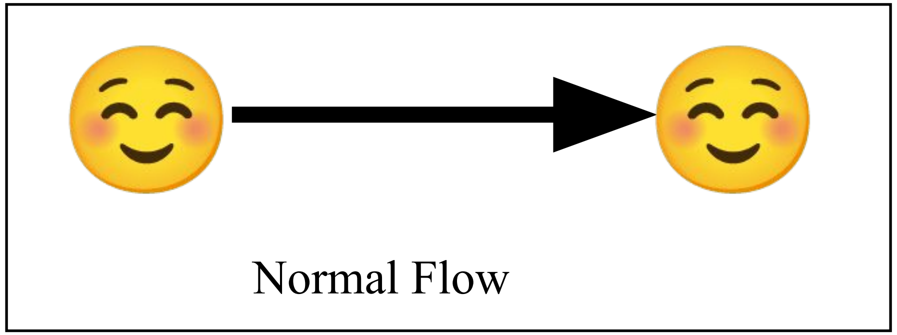
Integrity

- Web Penetration for malware insertion
- Maliciously accessing servers and forging records
- Unauthorised Database scans
- Remotely controlling zombie systems

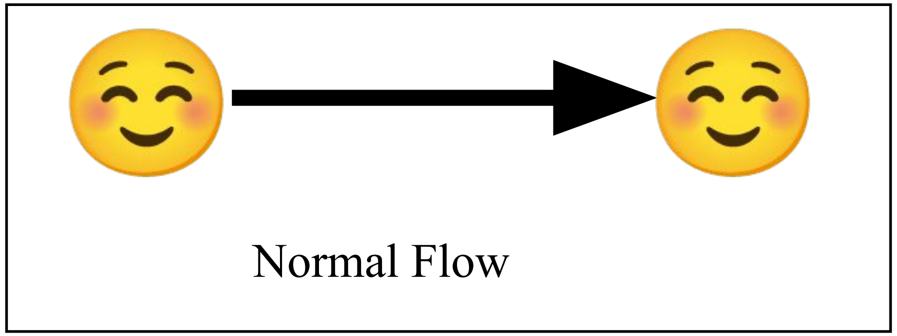
Availability

- DOS/DDoS attacks
- Ransomware attacks – Forced encryption of Key data
- Deliberately disrupting a server rooms power supply
- Flooding a server with too many requests

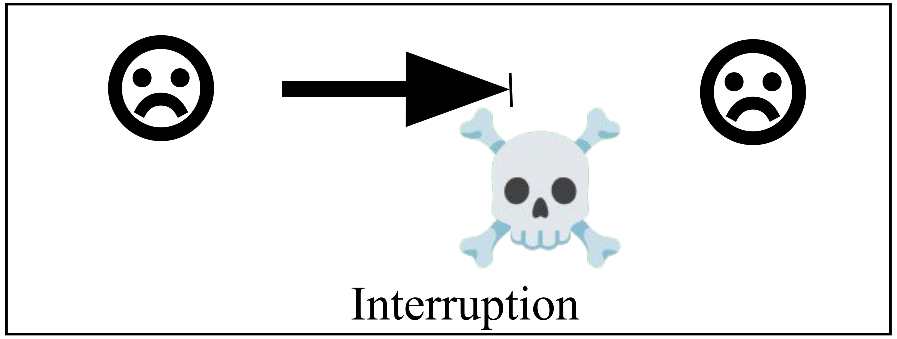
SECURITY ISSUES



SECURITY ISSUES

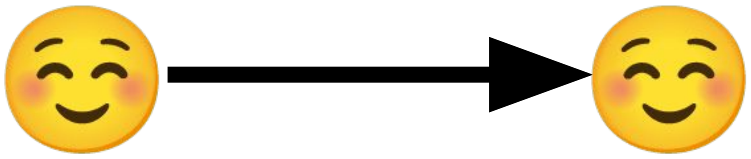


Normal Flow

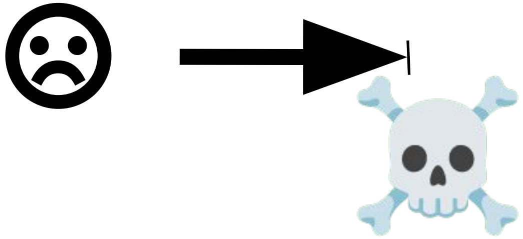


Interruption

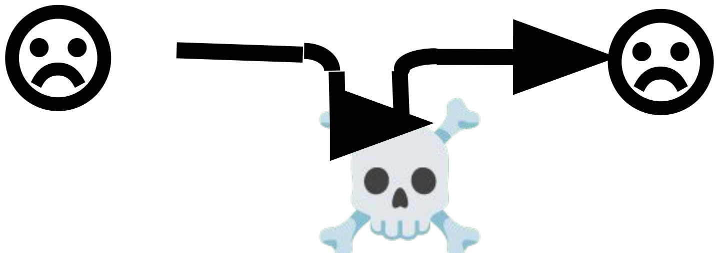
SECURITY ISSUES



Normal Flow

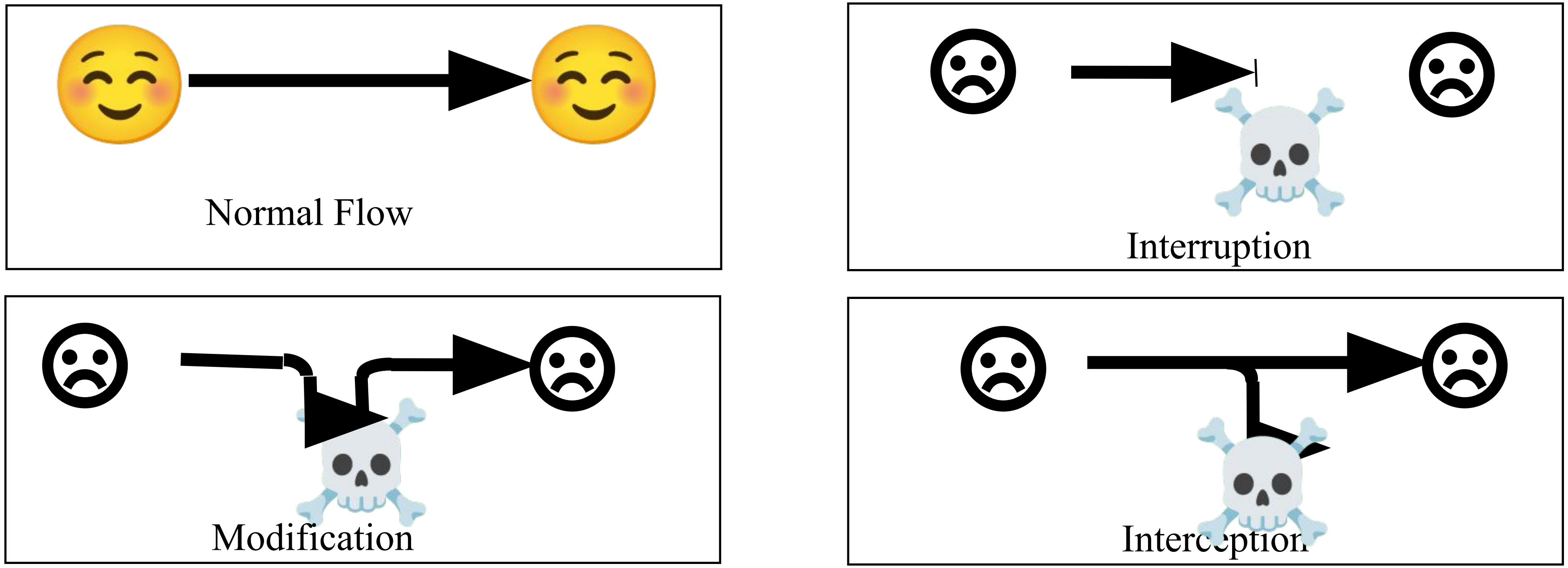


Interruption



Modification

SECURITY ISSUES



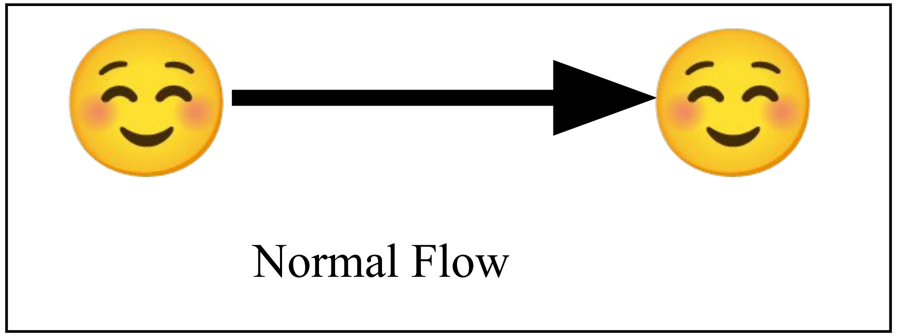
Normal Flow

Interruption

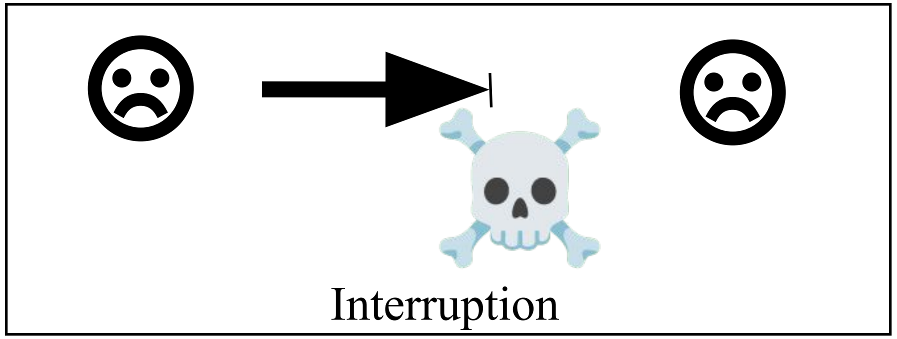
Modification

Interception

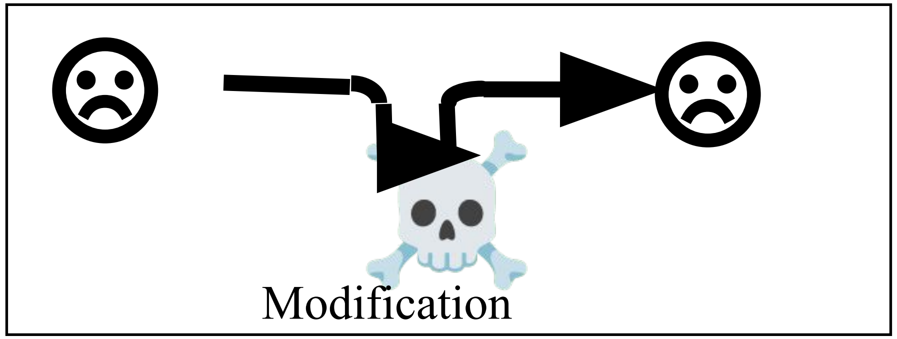
SECURITY ISSUES



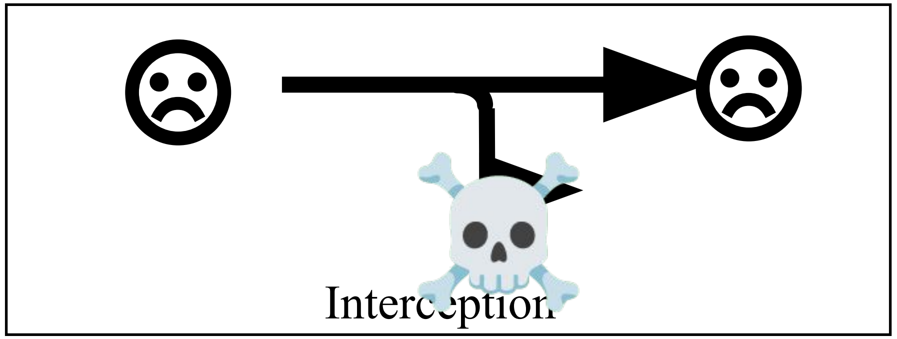
Normal Flow



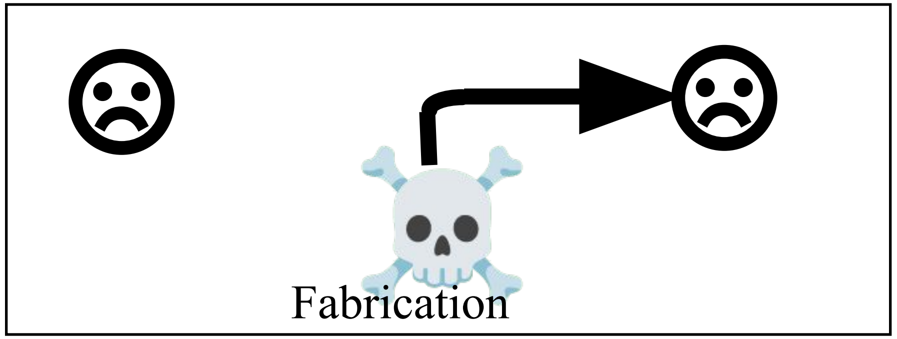
Interruption



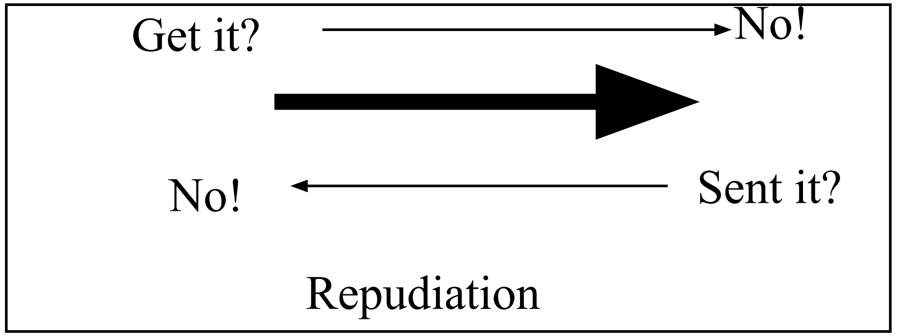
Modification



Interception



Fabrication



Get it?

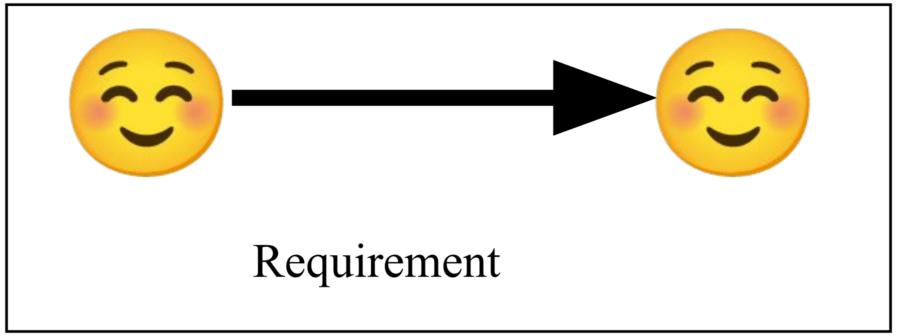
No!

Sent it?

No!

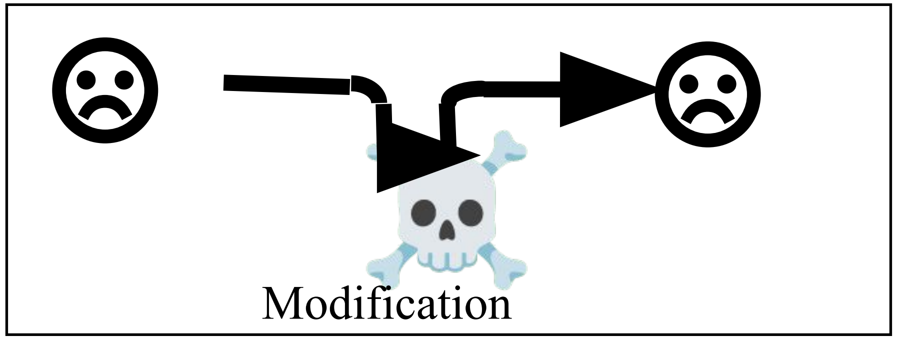
Repudiation

SECURITY ISSUES

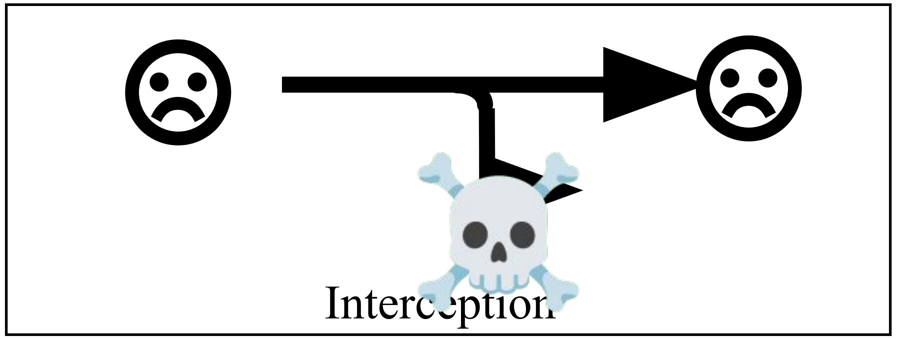


Requirement

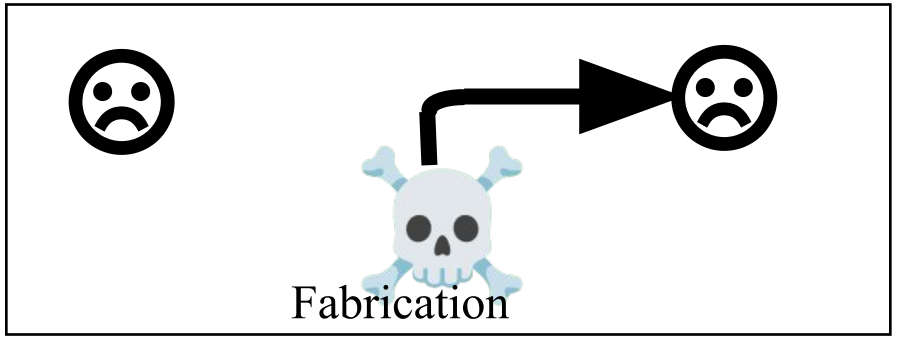
Availability



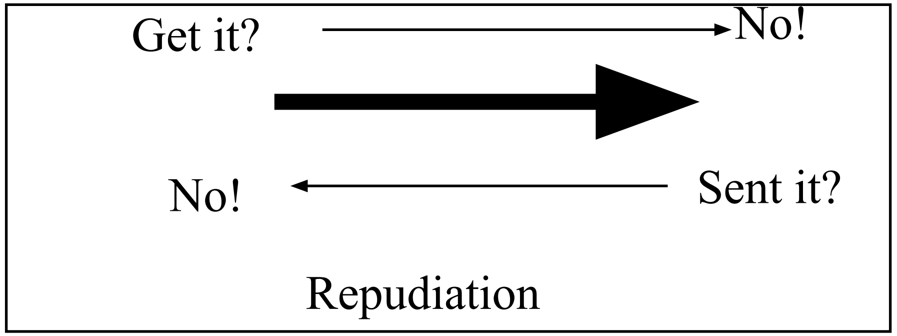
Modification



Interception

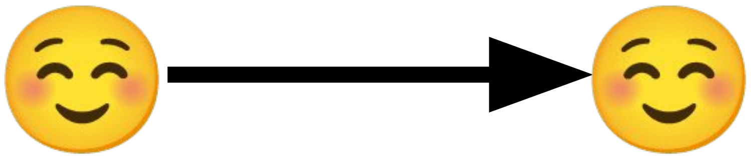


Fabrication



Repudiation

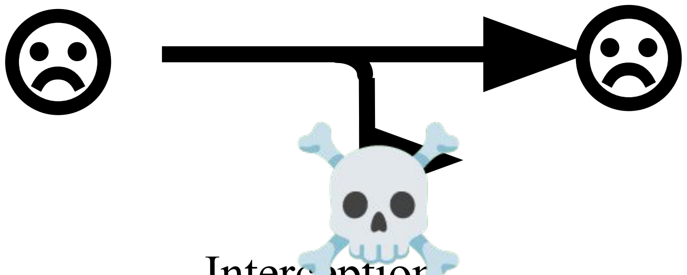
SECURITY ISSUES



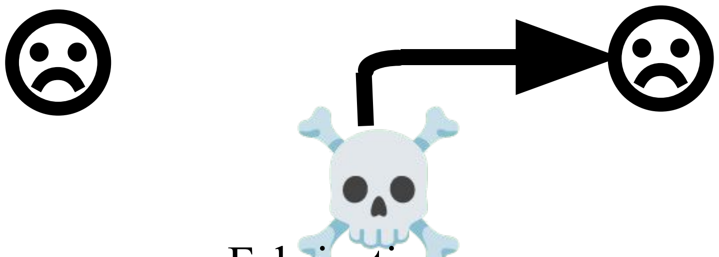
Requirement

Availability

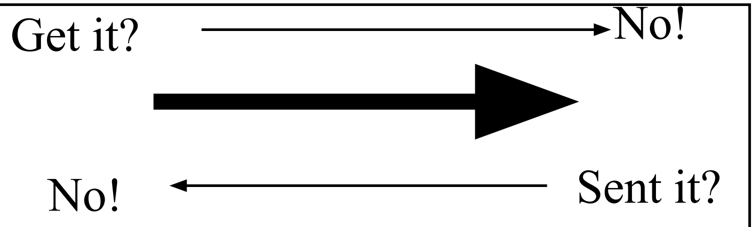
Integrity



Interception



Fabrication



Repudiation

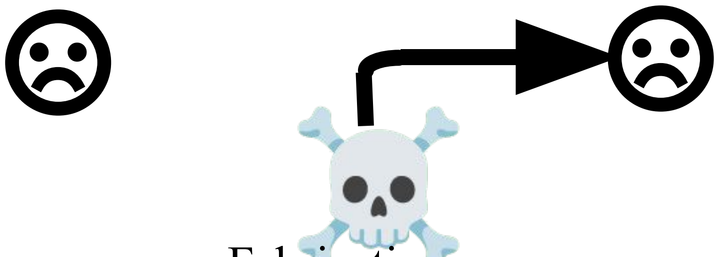
SECURITY ISSUES

Requirement

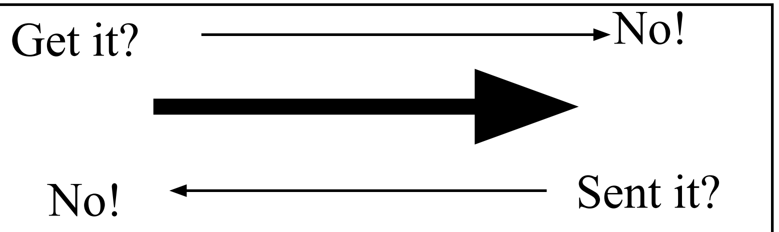
Availability

Integrity

Confidentiality



Fabrication



Repudiation

SECURITY ISSUES

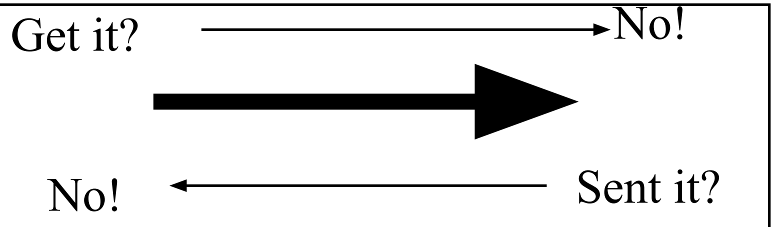
Requirement

Availability

Integrity

Confidentiality

Authenticity



Repudiation

SECURITY ISSUES

Requirement

Availability

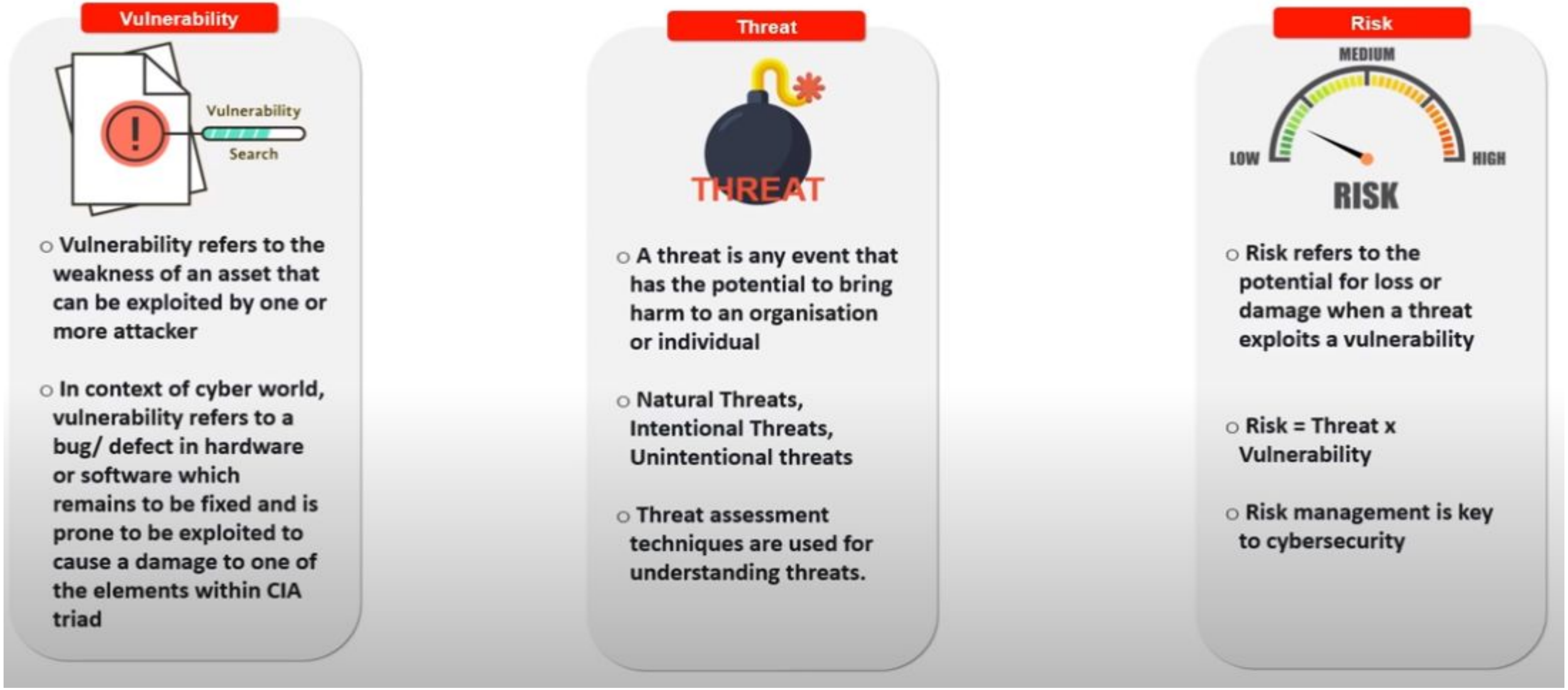
Integrity

Confidentiality

Authenticity

Non Repudiation

VULNERABILITY THREAT AND RISK



Vulnerability

- Vulnerability refers to the weakness of an asset that can be exploited by one or more attacker
- In context of cyber world, vulnerability refers to a bug/ defect in hardware or software which remains to be fixed and is prone to be exploited to cause a damage to one of the elements within CIA triad

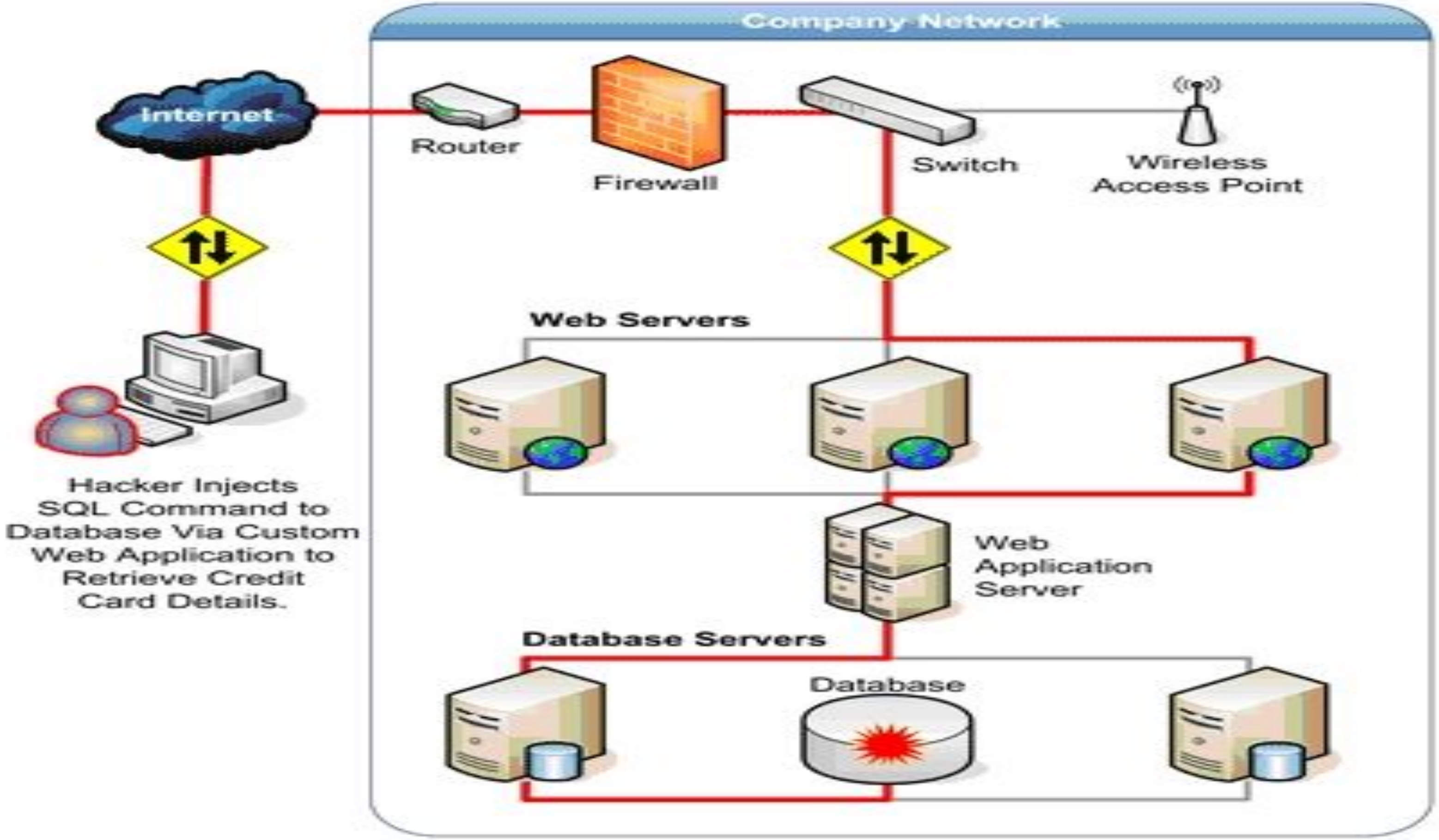
Threat

- A threat is any event that has the potential to bring harm to an organisation or individual
- Natural Threats, Intentional Threats, Unintentional threats
- Threat assessment techniques are used for understanding threats.

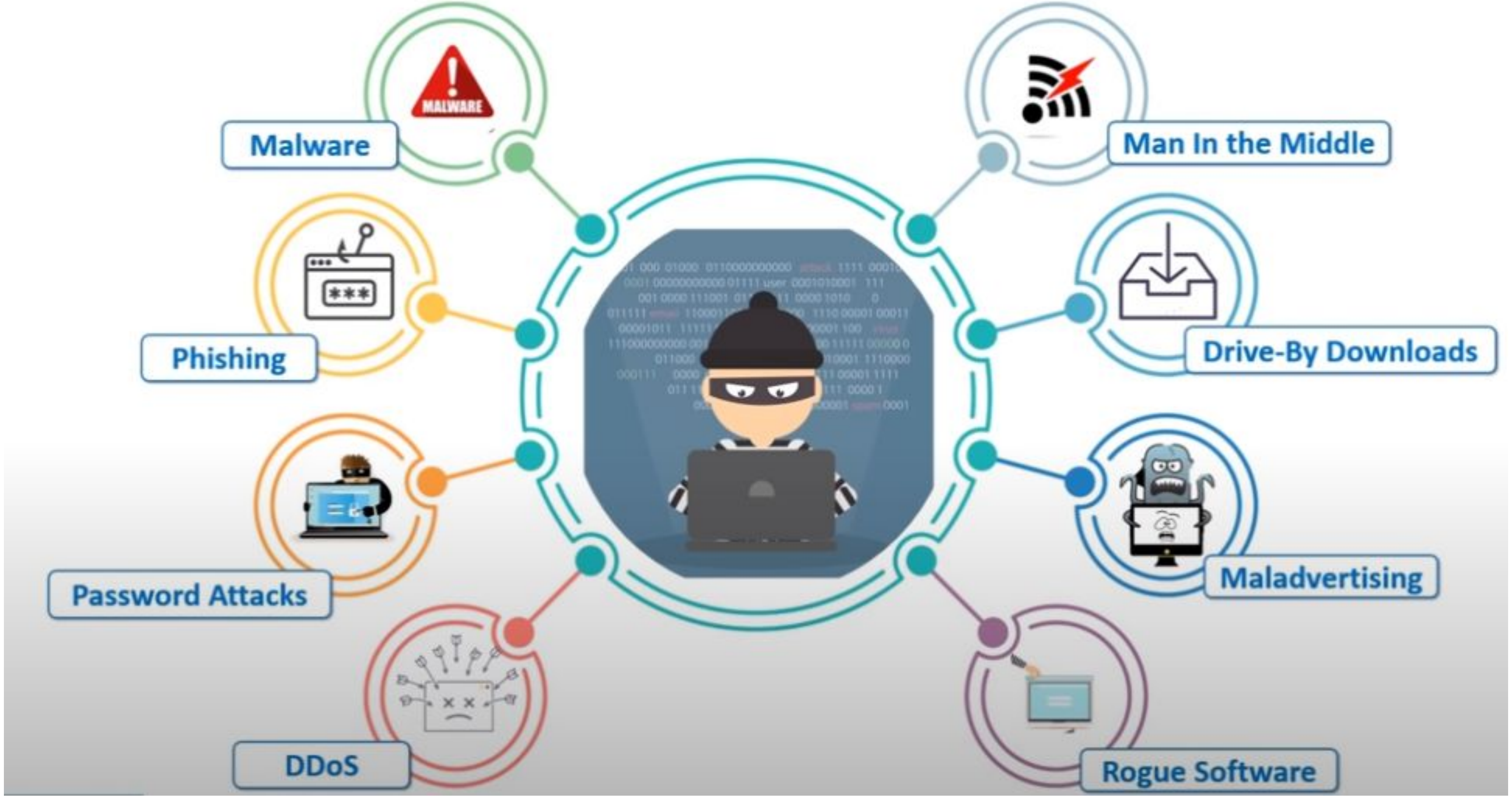
Risk

- Risk refers to the potential for loss or damage when a threat exploits a vulnerability
- Risk = Threat x Vulnerability
- Risk management is key to cybersecurity

HOW AN ATTACKER ATTACKS

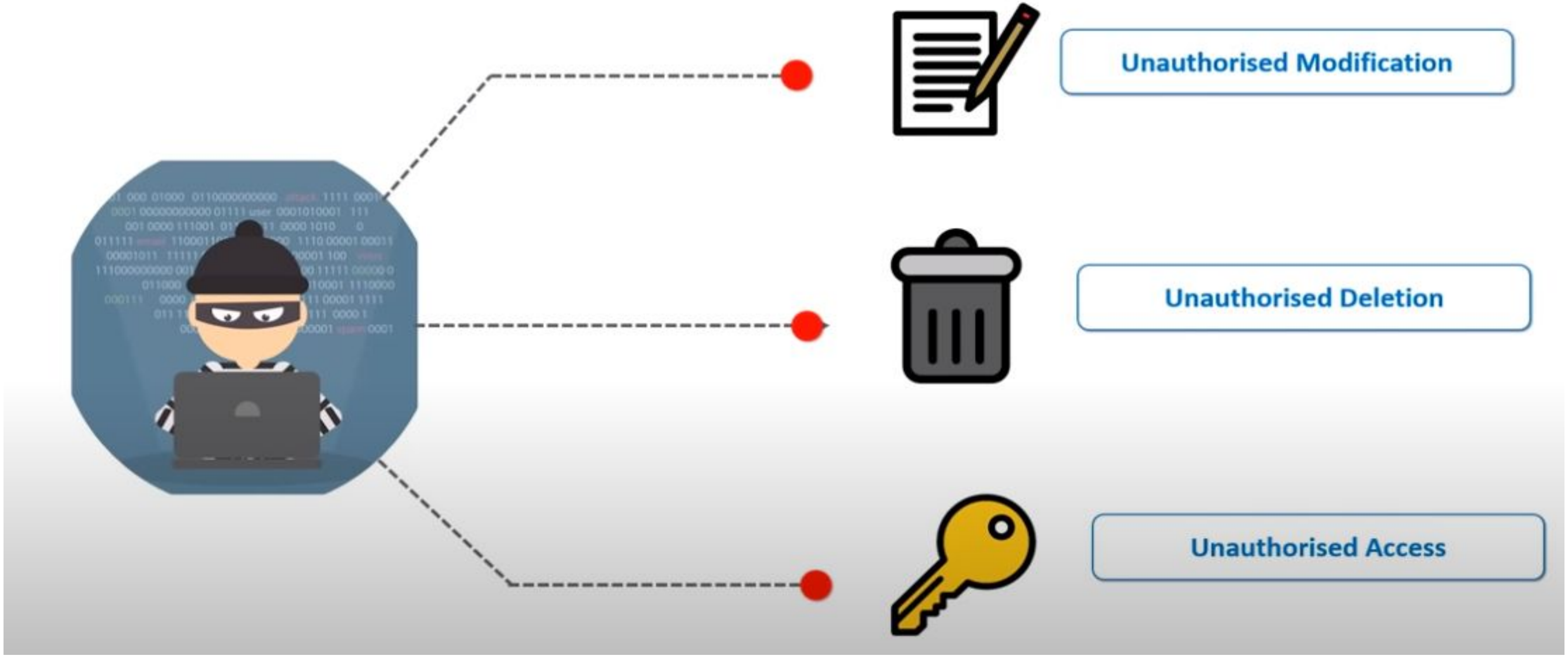


ATTACKS

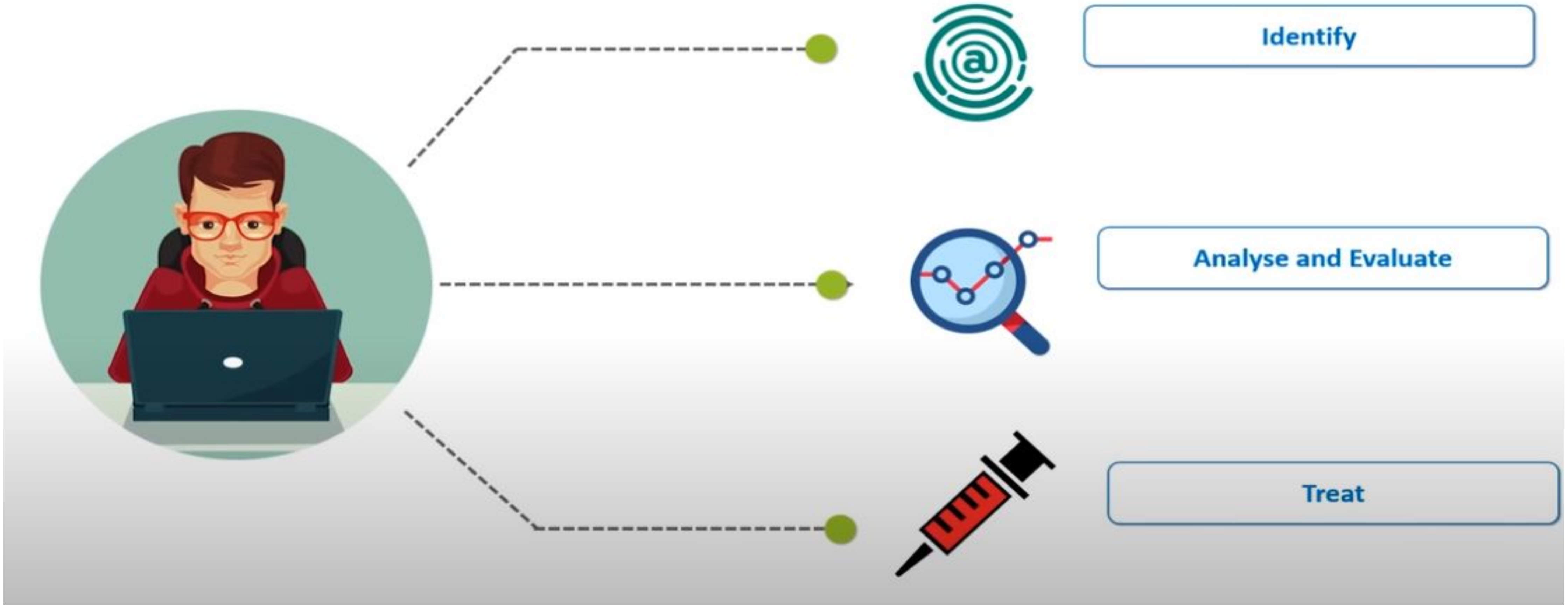


MALWARE
Malware
Man In the Middle
Phishing
Drive-By Downloads
Password Attacks
Maladvertising
DDoS
Rogue Software

PROTECTION FROM?



TIME TO FIX



Identify

Analyse and Evaluate

Treat

WHY SCHOOLS/EDUCATION INSTITUTES ARE A TARGET FOR CYBERCRIME

- **DDoS attacks** –a common type of attack on Education venue. This is where the attacker's motive is to cause widespread disruption to the institute's network, having a negative effect on productivity. This can be a relatively easy attack for amateur cybercriminals to carry out, especially if the target network is poorly protected. There have been instances of students or teachers successfully carrying out a DDoS attack, with motives ranging from simply wanting a day off, or protesting for complaint not handled.
- **Data theft-** The concerning aspect of this type of attack is that hackers can go unnoticed for long periods of time. As was the case at Berkeley, where at least 160000 medical records were stolen from University computers over a number of months.
- **Financial gain –** Another motive for hackers carrying out an attack on an education institution is for financial gain. This might not be as high a risk for public schools, but with private institutions and Universities/Colleges handling a large number of student fees, they're a prime target for cybercriminals.
- **Espionage –** The fourth reason why education is a target for cybercrime is espionage. In the case of higher education institutes like Universities/Colleges, they're often centres for research and hold valuable intellectual property.

AUTHENTICATION AND AUTHORIZATION

- Access Control
  - The ability to permit or deny the use of a resource by a user, through three essential services
- Authentication
  - To reliably identify the users
- Authorization
  - To control which users are allowed to do what with a resource
  - Representing trust, assuming reliable authentication

SECURING YOURSELF

- Awareness
  - What information you have
  - How important it is
  - How secure it is
- Assess
  - What could happen if lost or in the wrong hands
- Adequate
  - Precautions to protect it

SECURING YOURSELF

- Common Sense
- Awareness
- Regularly Update Patches
- Anti Virus, anti spyware…
- Be careful on P2P filesharing
- what you download
- Read the computer message(s)
- Don‘t blindly click next > next > next
- Be careful when you read email especially if it belongs to someone else
- Don‘t try to open every attachment
- Keep your password to yourself
- CybeSecurity – Cyberethics – Cybersafety

THANK YOU

For any query, drop a mail at

karanpreet[at] cdac [dot] in