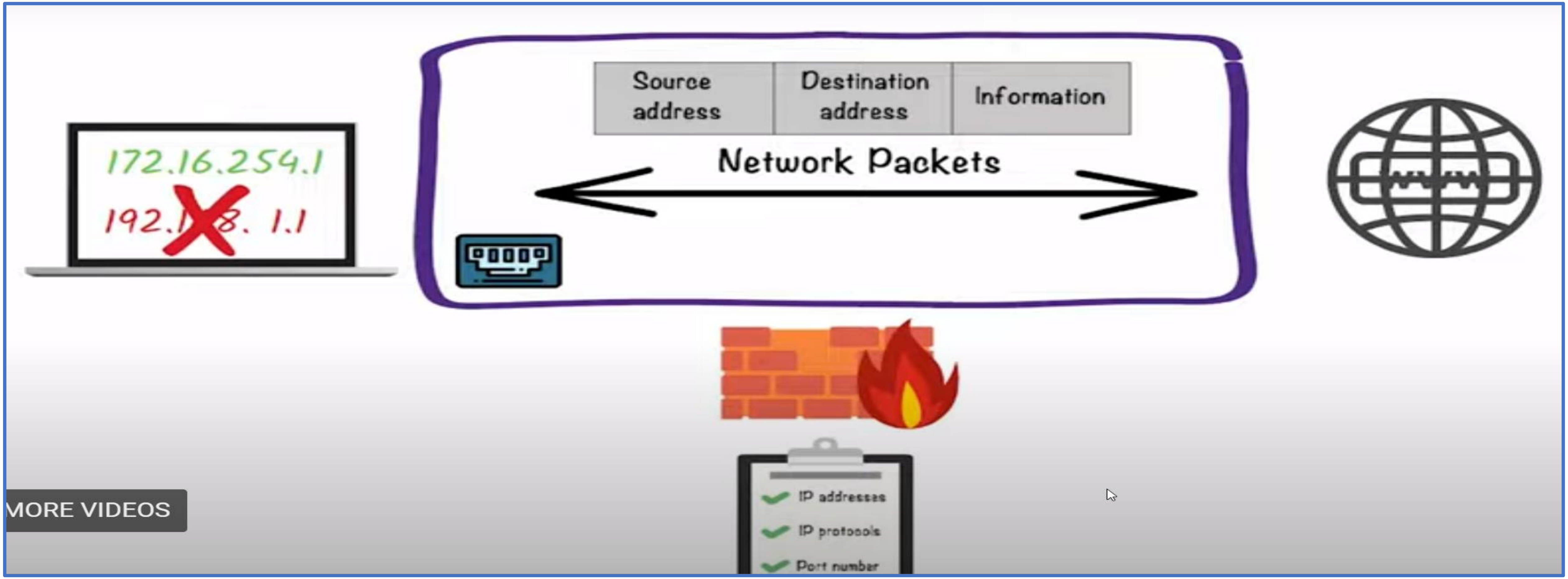
Honours/Minor Degree Program
in
Cyber Security

Topic – Elements of Hardware Security

Firewall

A firewall is a network security component that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Firewall

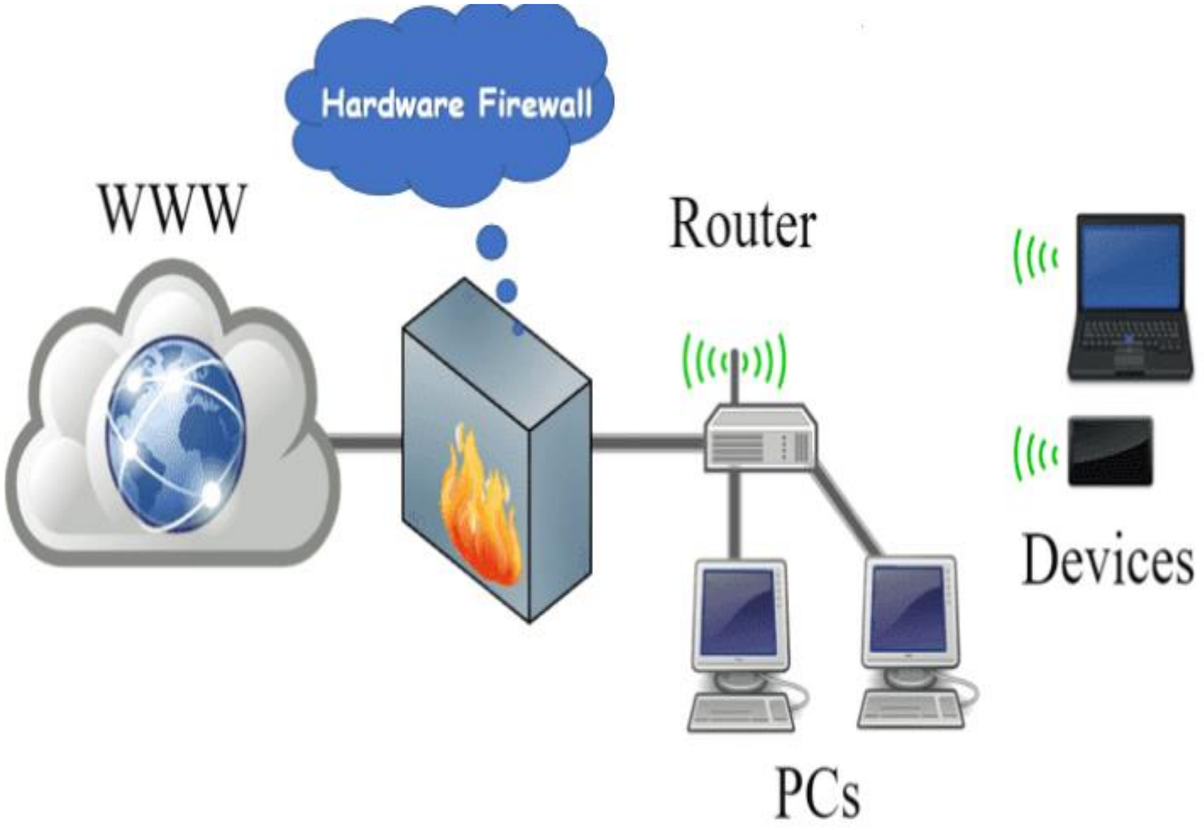


Firewall acts as a barrier between the private network and the Internet by rejecting the malicious packet and thus protect from the cyber attack but allows the traffic from the trusted network.

How does firewall work?

- It carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks

Firewall

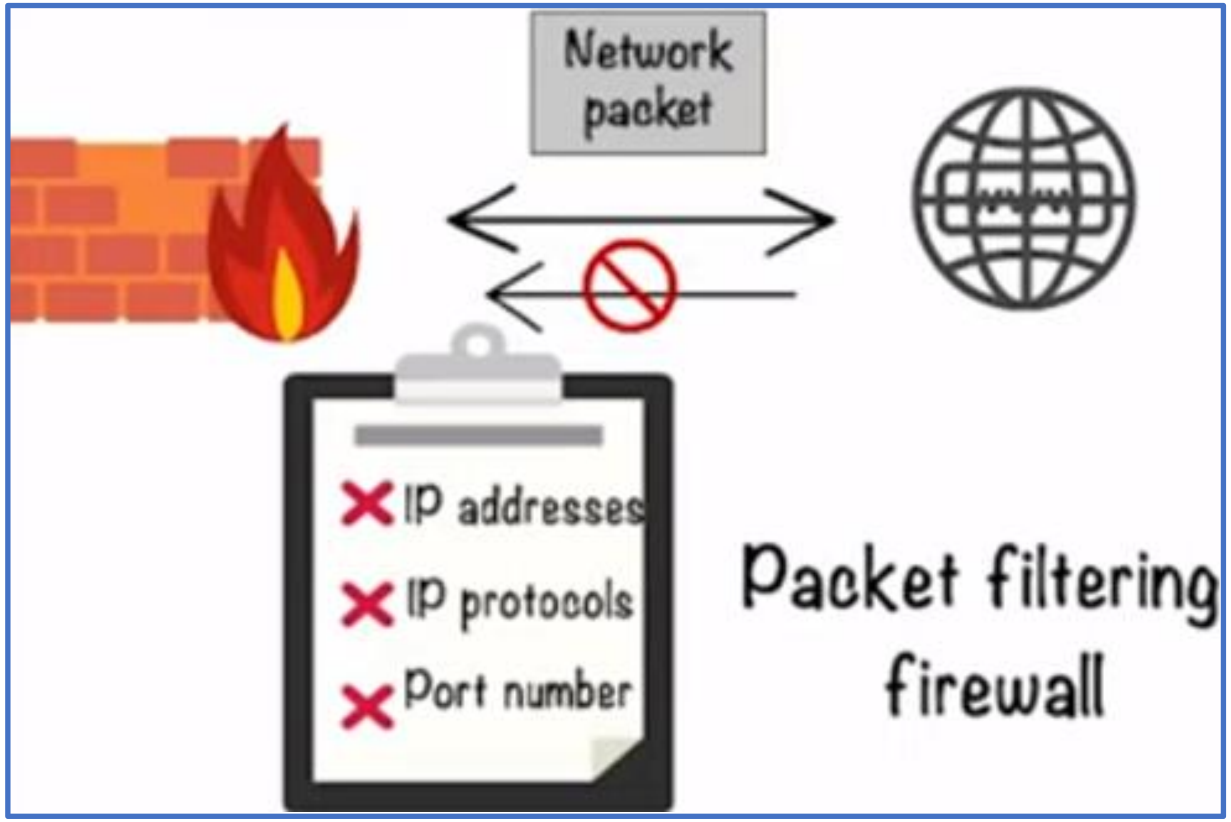


- Firewall is organization’s first line of defence.
- It is essential/ fundamental component of the network security
- It can be a software, hardware or both
- Hardware firewall is device installed between the Gateway and your network

Different types of firewall based on

- Traffic Filtering Method
- Structure
- Functionality

Packet Filtering Firewall

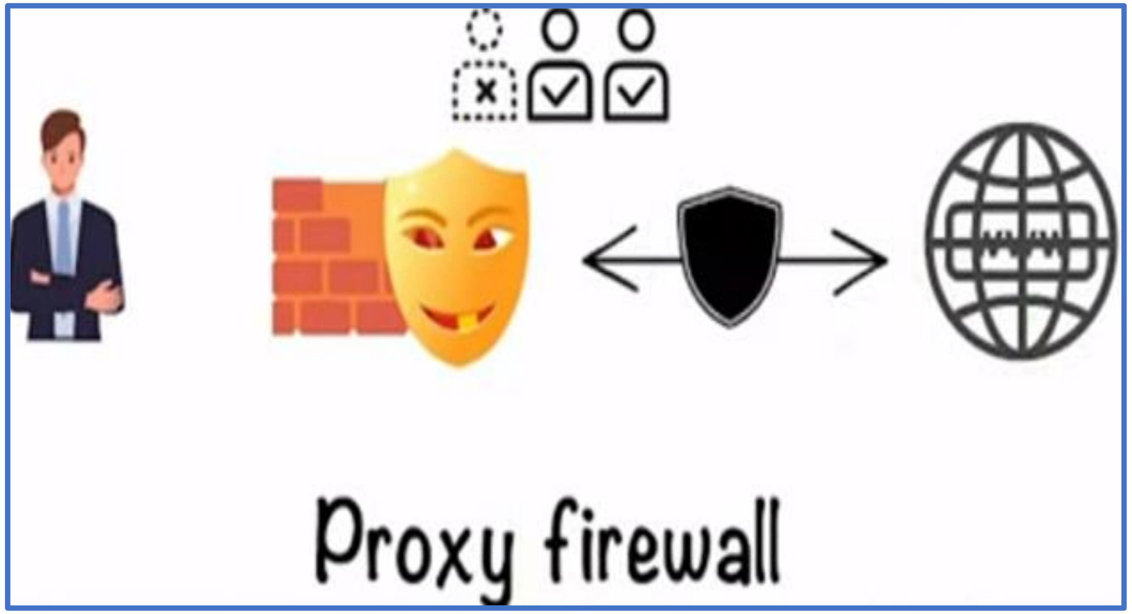


Disadvantage

- Just check trusted source address but don’t check the content of the request.
- A malicious request can be sent from the trusted sources.
- Can be vulnerable to IP spoofing attacks

- Basic firewall
- Need to configure the rules for either allow or deny traffic from the IP address, IP Protocols , Port numbers, etc.
- It is the most common type of firewall, examine packets and prohibit them from passing through if they don’t match an established security rule set.
- It checks the packet’s source and destination IP addresses. If packets match those of an “allowed” rule on the firewall, then it is trusted to enter the network.
- Performs only Packet header inspection and don’t perform the deep packet inspection
- Packet-filtering firewalls are divided into two categories: **Stateful and Stateless**.
- **Stateless firewalls** examine packets independently of one another and lack context, making them easy targets for hackers.
- **Stateful firewalls** remember information about previously passed packets and are considered much more secure.

Proxy Firewall



- Protect networks from attacks at the application layer.
- The proxy acts an intermediary between two end systems.
- Both the client and the server are forced to conduct the session through an intermediary -- the proxy server that hosts an application layer firewall.
- Each time an external client requests a connection to an internal server or vice versa, the client will open a connection with the proxy instead. If the connection request meets the criteria in the firewall rule base, the proxy firewall will open a connection to the requested server.
- Monitor traffic for layer 7 protocols (Application Layer) such as HTTP and FTP and use both stateful and deep packet inspection to detect malicious traffic.

Advantages

- Block specific content, such as known malware or certain websites, and recognize when certain applications and protocols, such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP) and domain name system (DNS), are being misused.

Nest Generation Firewall (NGFW)

- NGFW combine traditional firewall technology with additional functionality, such as encrypted traffic inspection, intrusion prevention systems, anti-virus, Network Address Translation (NAT), Uniform Resource Locator (URL) blocking and virtual private networks (VPNs), etc.

- It includes deep packet inspection (DPI).

- NGFWs support intent-based networking by including Secure Sockets Layer (SSL) and Secure Shell (SSH) inspection, and reputation-based malware detection. NGFWs also use deep packet inspection (DPI) to check the contents of packets and prevent malware.

Backdoor / Trapdoor

- It is a kind of secret entry point into the program that allow anyone to gain access to any system without going through the usual security access procedures.

- Bypassing normal authentication methods. It is also known as a back door.

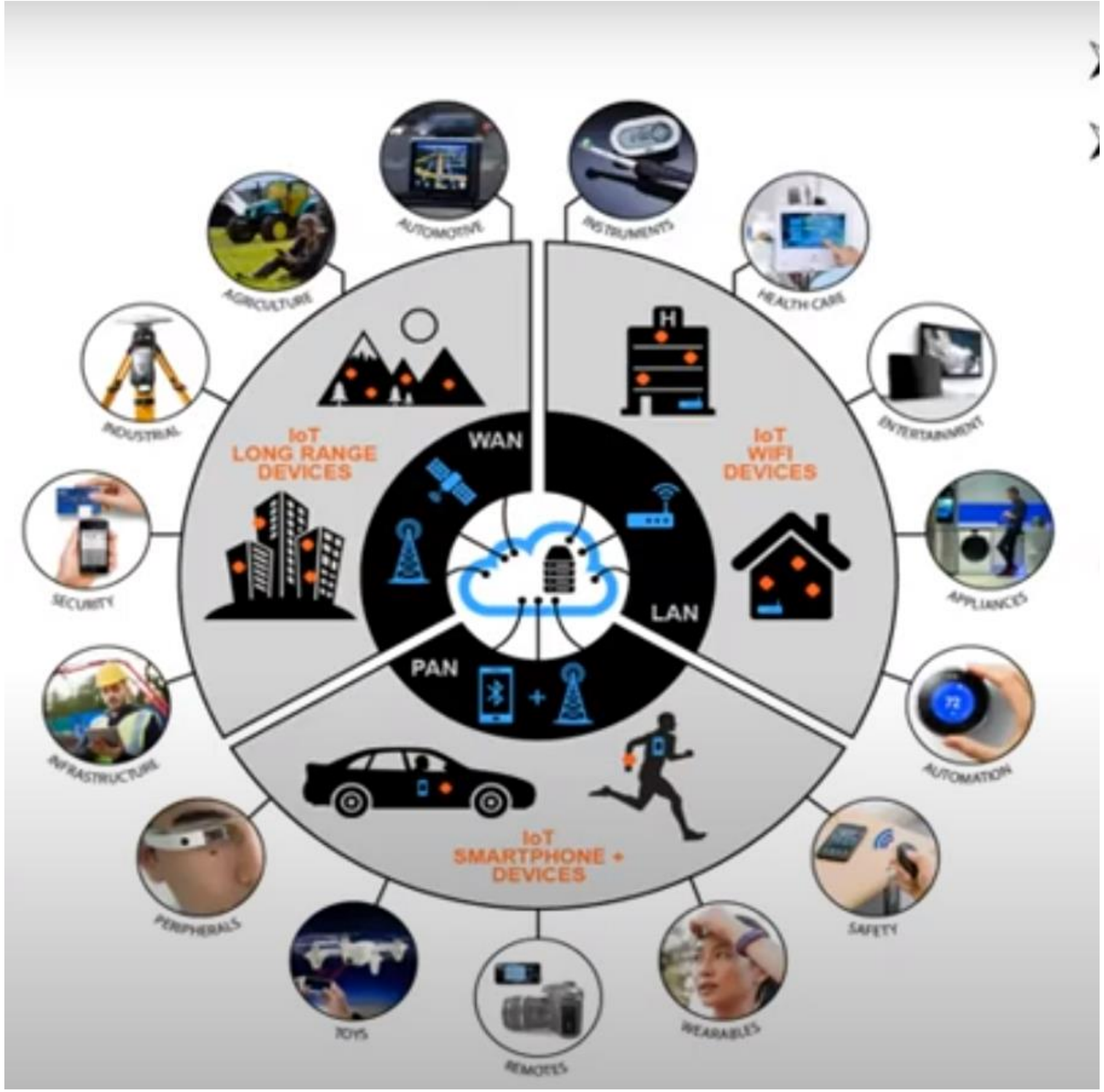
- Trap Doors are quite difficult to detect

- Trap doors turn to threats when any adversary gain illegal access

Side Chanel Attack

- Hardware Hacking
- A side channel attack is any attack based on the information gained from the implementation of a system, rather than the security weakness in the system.
- A side-channel attack **does not target a program or its code directly**. It attempts to gather information by measuring or exploiting indirect effects of the system or its hardware.
- It aim at extracting secrets from a chip or a system, through measurement and analysis of physical parameters.
- This can be achieved by measuring or analysing various physical parameters e.g. include supply current, execution time, and electromagnetic radiation emission.
- Side-channel attack vectors:
  - Timing attack: Analyses the time a system spends executing cryptographic algorithms. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems
  - Electromagnetic (EM) attack: Measures and performs a signal analysis on the electromagnetic radiation emitted from a device.
  - Simple power analysis (SPA): Directly observes the power and

Physical Unclonable Function (PUF)



Each device is cyber physical device, and it is a potential threat and a source of the cyber attack

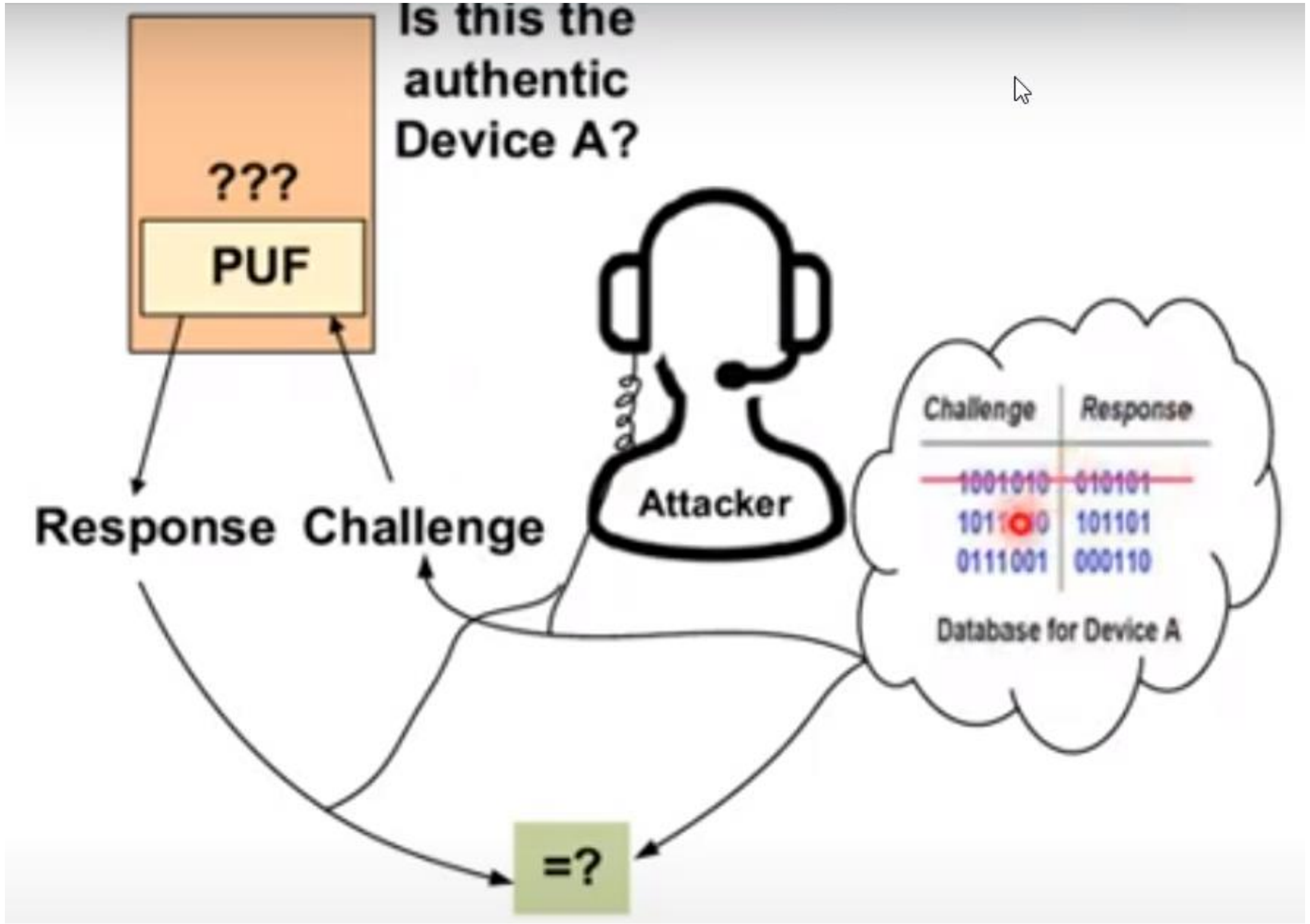
- Unauthorized access
- Data/identity Theft
- Electronic counterfeiting
- Reverse Engg,
- Side Channel Attack

You have two identical devices; how can you differentiate them?

- Embedded security module in each device
- Hardware security primitive such as physical unclonable function
- PUF is digital fingerprint for the devices that serve as the unique identifier for the authentication - analogous to biometrics for humans
- Fingerprint can be made at each chip level

PUF

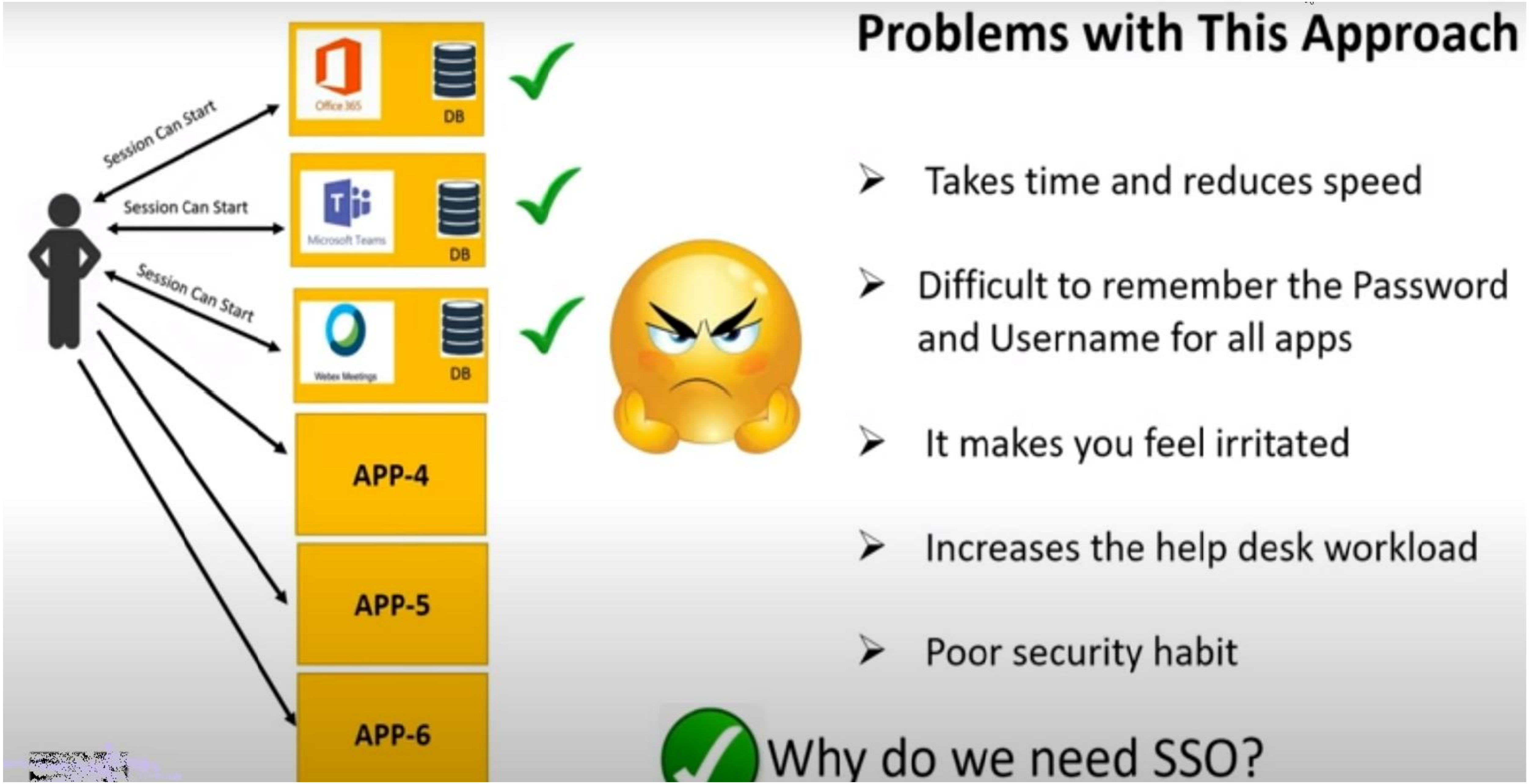
- Physically unclonable functions (PUFs) are a technique in hardware security that exploits inherent device variations to produce an unclonable, unique device response to a given input.
- PUFs are usually implemented in **integrated circuits** and are typically used in applications with high-security requirement.
- PUF is a small electrical differences occurring at the chip level. These process variations manifest in ways like differing path delays, transistor threshold voltages, voltage gains, and countless others.



Challenge	Response
~~1001010~~	~~010101~~
101[illegible]0	101101
0111001	000110

- PUFs work by implementing challenge-response authentication. For a given PUF, a specific input, known as a “challenge”, will generate an output response that is unique to the specific PUF and therefore unclonable.
- When manufactured, the PUF will be fed a series of different challenges and have its responses recorded. Through this exercise, the designers know each PUF’s unique response to a given challenge and can use this information to prevent counterfeiting, create and store cryptographic keys, and many other security feats.

Single Sign On (SSO)



Problems with This Approach

- Takes time and reduces speed
- Difficult to remember the Password and Username for all apps
- It makes you feel irritated
- Increases the help desk workload
- Poor security habit

✓ Why do we need SSO?