Chapter 3.1

Wireless Network Security and Physical Security

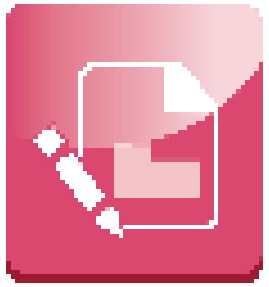
Aim

To discuss the vulnerabilities of wireless communication systems

Instructional Objectives

After completing this chapter, you should be able to:

- Explain SQL injection vulnerabilities and the methods to protect it
- Outline wireless network components and ways to secure it
- Discuss wireless hacking techniques and tools
- Explain reasons that cause vulnerabilities in WEP
- Discuss how viruses and worms impact web applications and networks
- Identify the main components involved in physical security



Learning Outcomes

At the end of this chapter, you are expected to:

- Explain the methods of SQL injection
- Outline the countermeasuresfor SQL injection
- Discuss wireless communication methods and their vulnerabilities
- Differentiate between WEP and WPA
- Outline countermeasures to avoid wireless network hacking, viruses and worms
- List the security breaches due to insufficient physical security and ways to improve them

SQL Injection

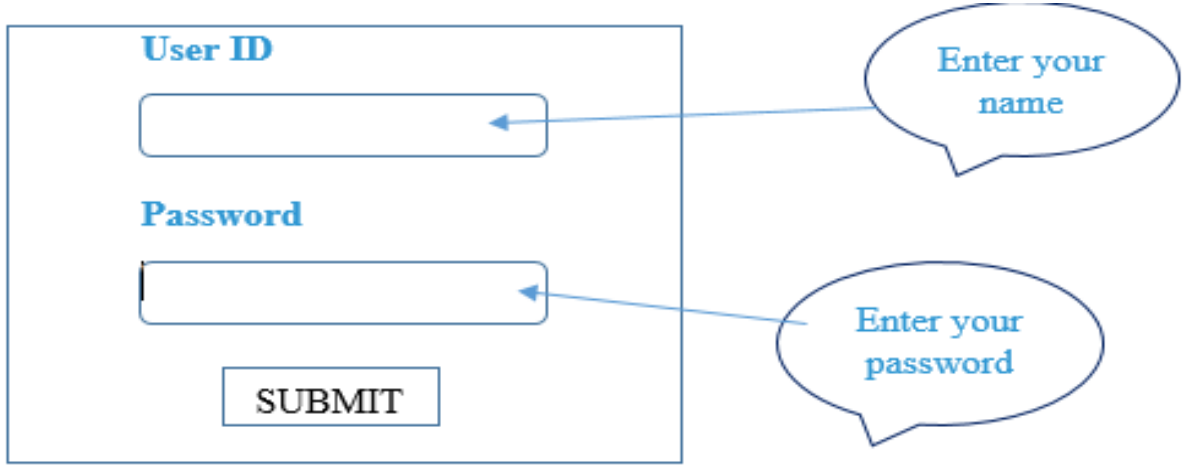
Introduction to Web and SQL Injection

web application is a computer program that allows users to submit their request

web has strengthened the economy in the field of manufacturing, education, banking and even healthcare

An SQL injection is “a code injection technique used in a computer attack in which the attacker successfully alters the SQL statements within the web applications”

SQL Injection



username and password window

showing the status of the user SQL query

```
$uid = $_POST['uid'];$
$pid = $_POST['passid'];
$SQL = "select * from user_details where userid = '$uid' and password = '$pid' ";
$result = mySQL_query($SQL);
```

SQL Injection Vulnerabilities and Attacks

- Missing Input Validation
- All input is treated as data by the servers
- Stored procedures use dynamic SQL statements
- Use of escape user input

SQL Attack : Steps

- Identify vulnerable websites
- Fingerprint the backend database
- Enumerate data such as table dumps, usernames and passwords
- Exploit the system once the hacker gains access to the required information

Common SQL injection URL patterns

- - - *or* single quote (‘).
- “/*”Statement containing UNIONALL, SELECT and FROM keywords
- Benchmarks
- Statements containing “information_schema” Again. What “those”?

Example of SQL Statement for Benchmarks

```
1 UNION SELECT IF(SUBSTRING(user_password,1,1) =
CHAR(50),BENCHMARK(5500000,ENCODE('MSG','by 5 seconds')),null)
FROM users WHERE user_id = 1;
```

Lack of Strong Typing

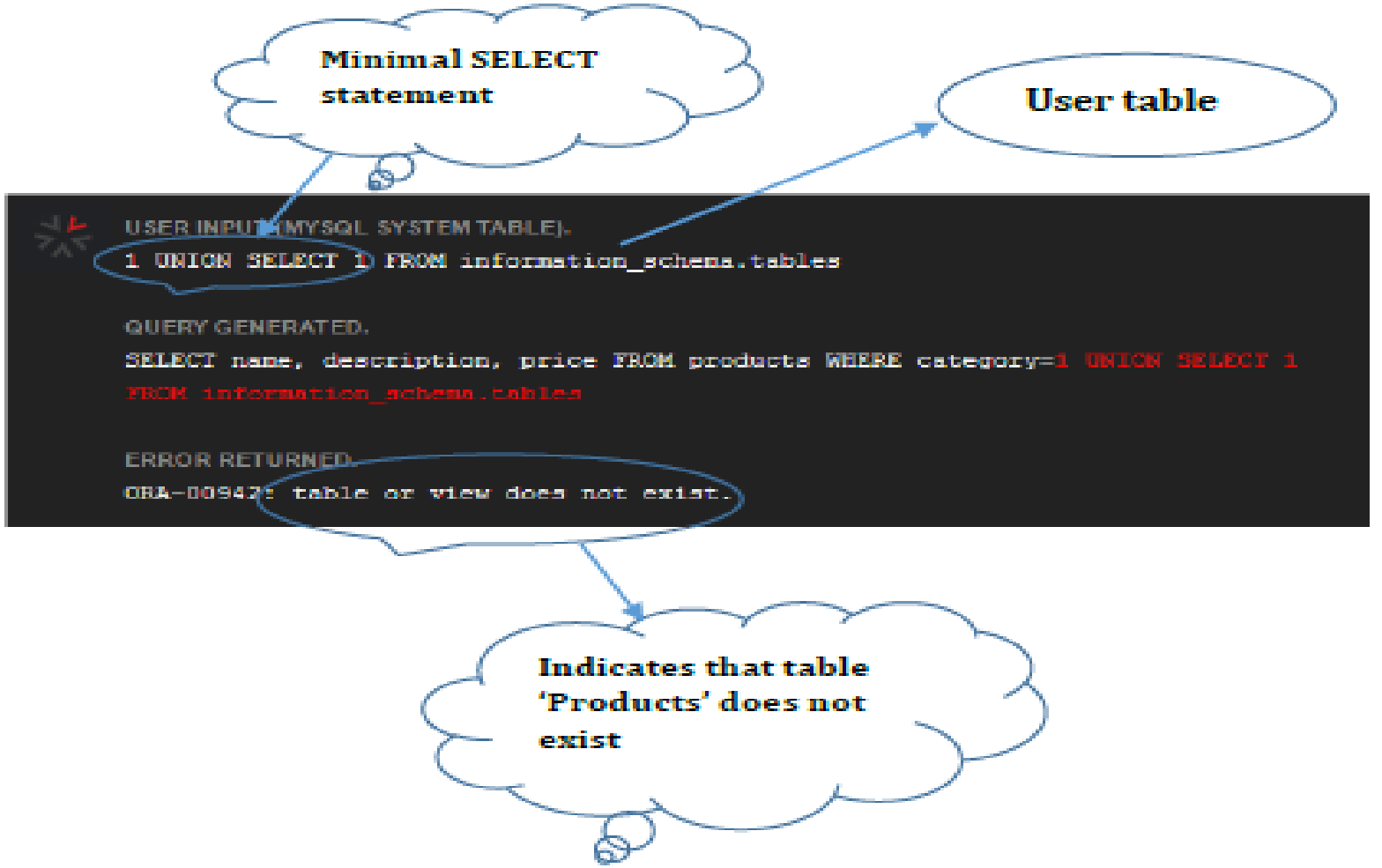
- Strong typing refers to the practise of predefining datatypes like an integer, decimal or text as a part of the programming language which is used to develop web applications.
- Later expecting the web applications to only accept those input values that adhere to this rule.
- Failing to implement this feature will expose an SQL server to injection attacks.

Example

Select Studentname from Students where StudentID= ’ “ + StudentID + “ ‘ ; “

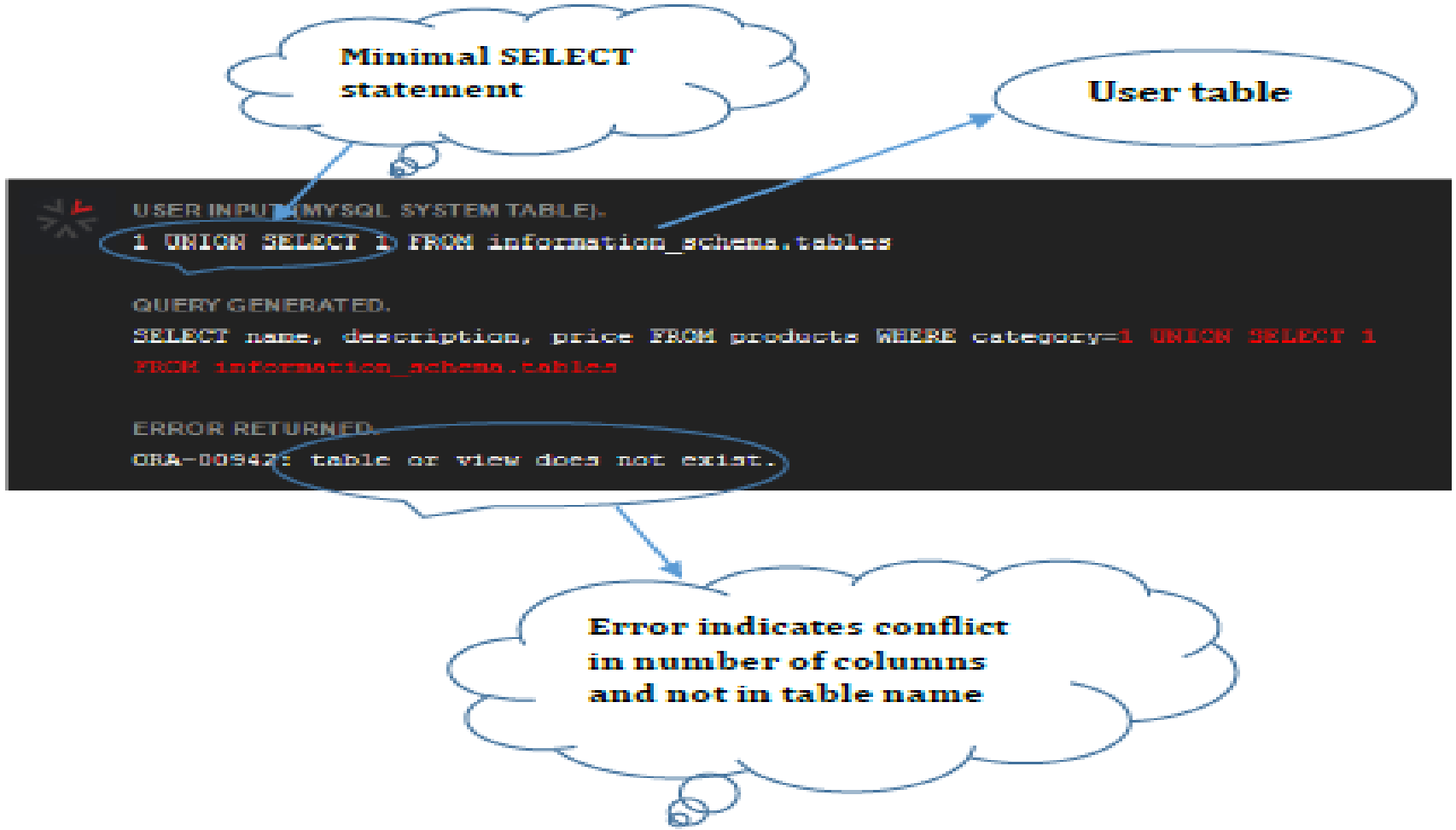
SQL Injection using UNION

Deletion of Table due to Misinterpretation of the SQL Statement



SQL Injection using UNION

Error due to more SELECT statements



Vulnerable Stored Procedures

Microsoft SQL Server syntax has been used to demonstrate how stored procedures become vulnerable

Example:

```
CREATE PROCEDURE getDescription
        @vname VARCHAR(50)
AS
        Exec (' select description FROM products WHERE name= ' ' ' + @vname+ ' ' ' ' )
RETURN
```

SQL Injection Hacking Tools

Havij	Havij:	The Mole	SQLNinja	BSQL Hacker (Blind SQL)
• Automated SQL injection tool used for a web page • Higher success rate • Friendly GUI • Most preferred tool that penetration testers and hackers use	• Target Web applications • Automated testing tool • Used to test database security	• **UNION** technique or Boolean query to identify vulnerabilities • By proving its URL and a valid string on the particular website	• web applications that use an MS SQL server as a backend database • Gets an interactive shell on the remote database server • Used on a target network	• *Virtually* exploits the vulnerabilities in any database

Countermeasures for SQL Injection Attacks

SQL server vulnerabilities can be controlled by including some of the below mentioned coding practices:

1. Recommending the use of strong passwords and regularly changing them
2. Enforcinga check on numeric inputs — 'integers'
3. Avoiding the use ofdynamic SQL queries and multiple queries
4. Installing security patches
5. Not allowing access to databases for all the users
6. Employing the Windows Authentication method
7. Running checks on web configuration files

Quiz / Assessment

1) To test whether a database is vulnerable to an attack, a hacker places a single quote character into the query string of a URL. What type of error message will be generated?			
a) DBMS error message	**b) There will be no error message**	**c) ODBC error message**	**d) "access granted"**
2) Which of these is nota wildcard character in SQL query?			
a) %	**b) -**	**c) $**	**d) [!charlist]**

Wireless Hacking

- Wireless communication refers to the transmission of information over a distance, without the usage of cables or wires or any other electrical conductors.

The advantages that wireless technology offers

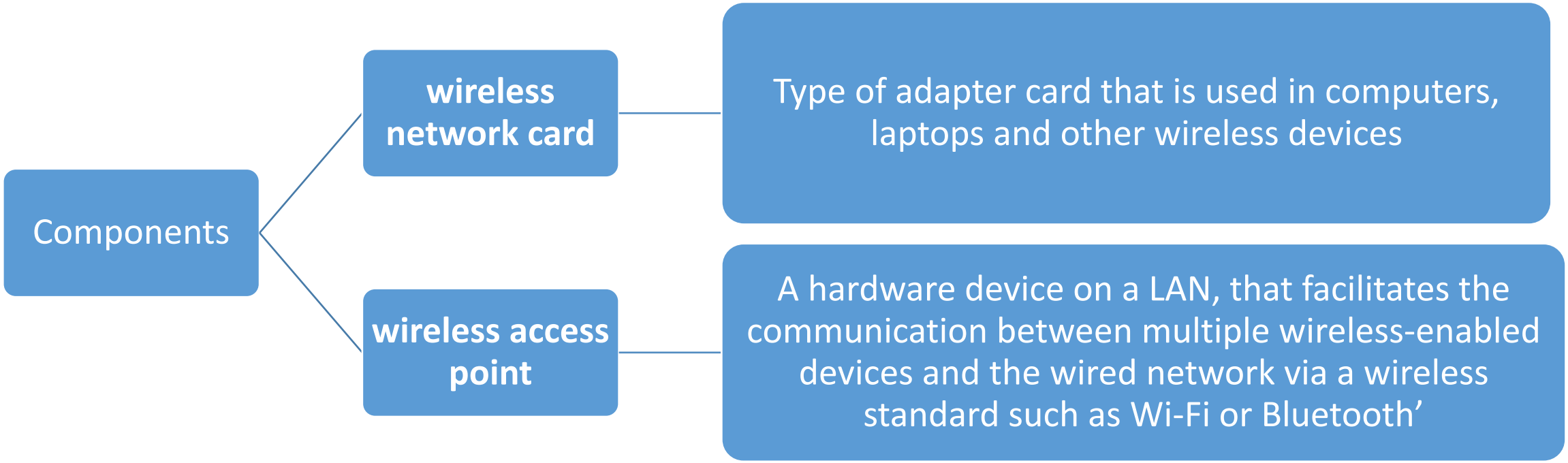
Easy to use

Flexibility:

Convenience:

Reliability

Wireless Network Components



Wireless Communication Methods

- Infrared communication or IR
- Satellite communication
- Broadcast radio
- Microwave radio
- Bluetooth
- Wi-Fi
- Mobile communication

Wireless Local Area Network or LAN

Security Protocols in Wireless Networks

Wired Equivalent Privacy

- **WEP** is a security protocol specified in the IEEE standard 802.11b

It is also known as **Wireless Encryption Protocol**

- It is the initial standard used for first generation wireless networking
- This protocol provides encryption to the data transmitted in a WLAN environment.
- This protocol operates at the data link layer and physical layer of the OSI model and suffers from vulnerabilities.
- By encrypting data at the data link layer, using an RC4 encryption, one can control the unauthorised access to data.

WEP and WPA—A Comparison

	WEP	WPA
Developed By	IEEE in 1999	Wi-Fi Alliance in 2003
Security Method	Via an encryption key	Via a password
Authentication	Open system or shared key	Using 64 digit hexadecimal key
Encryption	Using a static encryption key that uses plain text—RC4	AEP andTLIP with a message integrity check

Vulnerabilities in Wireless Communication

Unauthorised access points

- Unsecured or purely secured access points pose a threat to a wireless LAN environment.

SSID issues

- A service set identifier or SSID is an alphanumeric character that uniquely identifies a wireless LAN.
- This is programmed in wireless access points or clusters of it.

WEP vulnerabilities

- A wireless network administrator using the WEP encryption method can define a shared keyfor authenticating users. Only users with this shared key are allowed access the network.

MAC Address vulnerabilities

- MAC address sniffing and spoofing are the two most common methods by which a hacker can gain access to a WLAN.

Types of Wireless Attacks

Denial of Service or DoS Attacks

- A DoS attack maybe defined as '*an attack in which a hacker turns a network or a service unavailable to its legitimate users*'.

SSID Attacks

- This is another type of attack that occurs in wireless networks due to vulnerabilities that exist in SSIDssuch as functioning with a default value, black SSIDs or a value set to '*any*'

Rogue Access Points

- In this attack, the hacker installs his own access points that users assume is the original access point and connect to it.

MAC Spoofing

- MAC spoofing is a Wireless attack, in which a hacker will listen in on the network traffic and figures out the MAC address of the computer.

War Driving

- War Driving is defined as '*the act of sniffing WLANs by a hacker who is travelling in a vehicle, using his laptop and a wireless network adapter card*'.

The Broadcast Bubble

- A hacker may eavesdrop on network traffic or a perform packet analysis with the aid of a transceiver, sitting in a public place.

Wireless Hacking Tools

NetStumbler (Network Stumbler)	Aircrack	AirSnort	Kismet	Fern Wi-Fi Wireless Cracker
• Suitable for Windows OS • War Driving —click here • Verifies network configurations and detects rogue access points • Identifies the cause of network interference and poor signal-receiving areas	• Captures packets and analyses passwords • Used for 802.11 (WEP and WPA-PSK)	• A wireless LAN tool which can crack encryption keys on 802.11b WEP networks • It monitors packet transmissions and when enough packets are gathered, it starts computing an encryption key	• Used for 802.11a/b/g/n layer 2 standards of wireless networks • Based on client-server architecture and detects hidden packets	• Monitors real-time traffic • Capable of cracking WEP/WPA/WPS keys • Initiates other wireless attacks or Ethernet attacks

Countermeasures for Wireless Hacking

By Implementing Standards and Policies	MAC Address Filtering	Dynamic WEP Keys	Implementing SSID Issues
Countermeasures for DoS Attacks	Encryption	Anti-virus and Firewall Software	Disable Identifier Broadcasting

Quiz / Assessment

3) Wi-Fi Protected Access or WPA, which addresses vulnerability issues present in WEP, does so by implementing a/an _____.			
a) Pre-shared key	**b) Temporal Key Integrity Protocol or TKIP**	**c) Extensible Authentication Protocol**	**d) None of the above**
4) Silencing the wireless network by repeatedly transmitting RTS/CTS frames results in a _____ attack			
a) Parking lot	**b) SSID**	**c) DoS**	**d) WEP cracking**

Viruses and Worms

- Viruses and worms are a serious threat to information systems.
- They come in different forms and cause varying levels of damage to computers and networks.
- While some attacks only slow down a system's performance or deny access to a specific website or network resource,
- Some are more serious, bringing an entire system or network to a complete halt.
- A virus inflicts damage on the operating system by either replacing a program or by associating itself with a program
- Thereby modifying the way that program functions.
- On the other hand, worms are self-replicating, malicious computer programs or codes that spread to computers in a network by exploiting a weakness on the target system

Lifecycle of a Virus

Dormant Phase In this phase, the virus is seen as idle until it is activated upon an occurrence of an event like a specified date or at the execution of a specified program

Propagation Phase: The virus will infect a program or specific areas on the disk, with a clone of itself, which again propagates itself into many clones

Triggering Phase A system event will act as a trigger to activate the virus for performing the task it is intended for

Execution Phase This is the actual attack phase where the virus causes damage to computers and networks

Impact on Web Applications and Networks

- Vulnerabilities present in a website is a strong reason for a virus to attack a website. Once a virus infects a web application, it sends a specifically crafted message that is capable of:
    - Executing a malicious code on the target computer
    - Injecting codes into databases or
    - Can cause cache poisoning
- Some of the ways that viruses find their way to a web server are:
    - From the user's computer
    - Incorporating malicious software
    - Making an hidden visit

Some Examples of Viruses

Web Bugs	Blended Threat	ILOVEYOU	Storm Worm	Slammer
• IP address of the target • URL of the web page on which the web bug is located • The exact time the user clicked on the web bug source • The type and version of the browser on the target machine	• A blended threat combines elements of a virus and spyware infections. • Some examples of blended threats are Nimda, CodeRed, Bugbear and Conflicker.	• Known to be the most destructive of viruses till date. • Released in 2004, • It was delivered as an email message with the subject line "*I Love You*".	• This deadly virus appeared in inboxes with the subject line "230 Dead as Storm Batters Europe" and it is believed to have been sent to close to 200 million users.	• This was probably the *fastest replicating* virus, as it took just few seconds for this to double in number. • In the US, it was managed to crash ATMs owned by Bank of America and disrupted 911 services.

How to Protect your Website from Virus Attacks?

- Installing firewalls and anti-virus software
- Downloading the latest virus definition files
- Including external devices such as USB drives, hard disks and DVD drives in scans
- Using the right configurations and security features of any program in the way it is supposed to be used
- In case of a virus attack, immediately shut-down the computer or disconnect from the network in order to avoid further complications

Worms

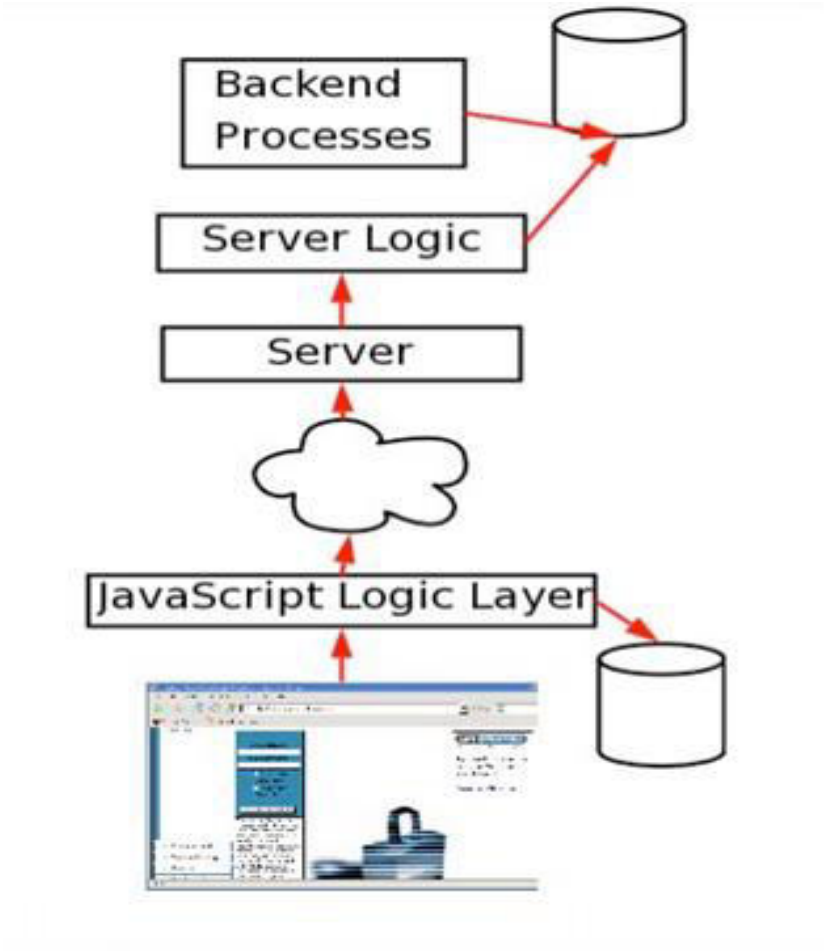
- Worms can be defined as ‘malicious and self-replicating computer programs’.
- They transmit from one computer to another via a network and unlike a virus a worm doesnot attach itself to a host program.
- Worms are designed to deliver damage to a payload.
- They spread havoc by destroying data, corrupting files and hindering a system’s performance on the computer or network.
- They can even install backdoors or Trojans and steal sensitive information.
- Worms often get inside your computer by exploiting a vulnerability in your software.

Some examples of worms are:

Explore.zip
Code Red Worm
My Doom

How to Secure your Web Applications from Viruses and Worms?

Securing websites and web applications is a harder task as they function in the open, hence bound to have many vulnerabilities, some of which come begin at the development stage.



Best Practices in Web programming

Implementing user identity for validation

Scrutinising every input

Implementing input validation at both ends

An application should be designed

Quiz / Assessment

5) What type of viruses hide the change in the file's date and time?

a) Macro viruses	b) Polymorphic viruses	c) Stealth viruses	d) Spyware

6) _____ is the name given to programs designed to collect email addresses from the Internet before they are made into a mailing list to be spammed.

a) Spyware	b) Spambots	c) Logic bomb	d) Web Bugs

Physical Security

- Physical security is a major concern faced by organisations, and it requires meticulous planning, design and the implementation of various components that together represent physical security.
- *Physical security is the protection of personnel, hardware, software, network and data from physical actions and events that could cause serious loss or damage due to an enterprise, agency or an individual. This may include protection from fire, natural disasters, burglary, vandalism and even terrorism.*

Components of Physical Security and its Importance

Administrative controls

- Site and Facility administration
- Facility plan
- Site location
- Environmental Crime prevention
- Securing data

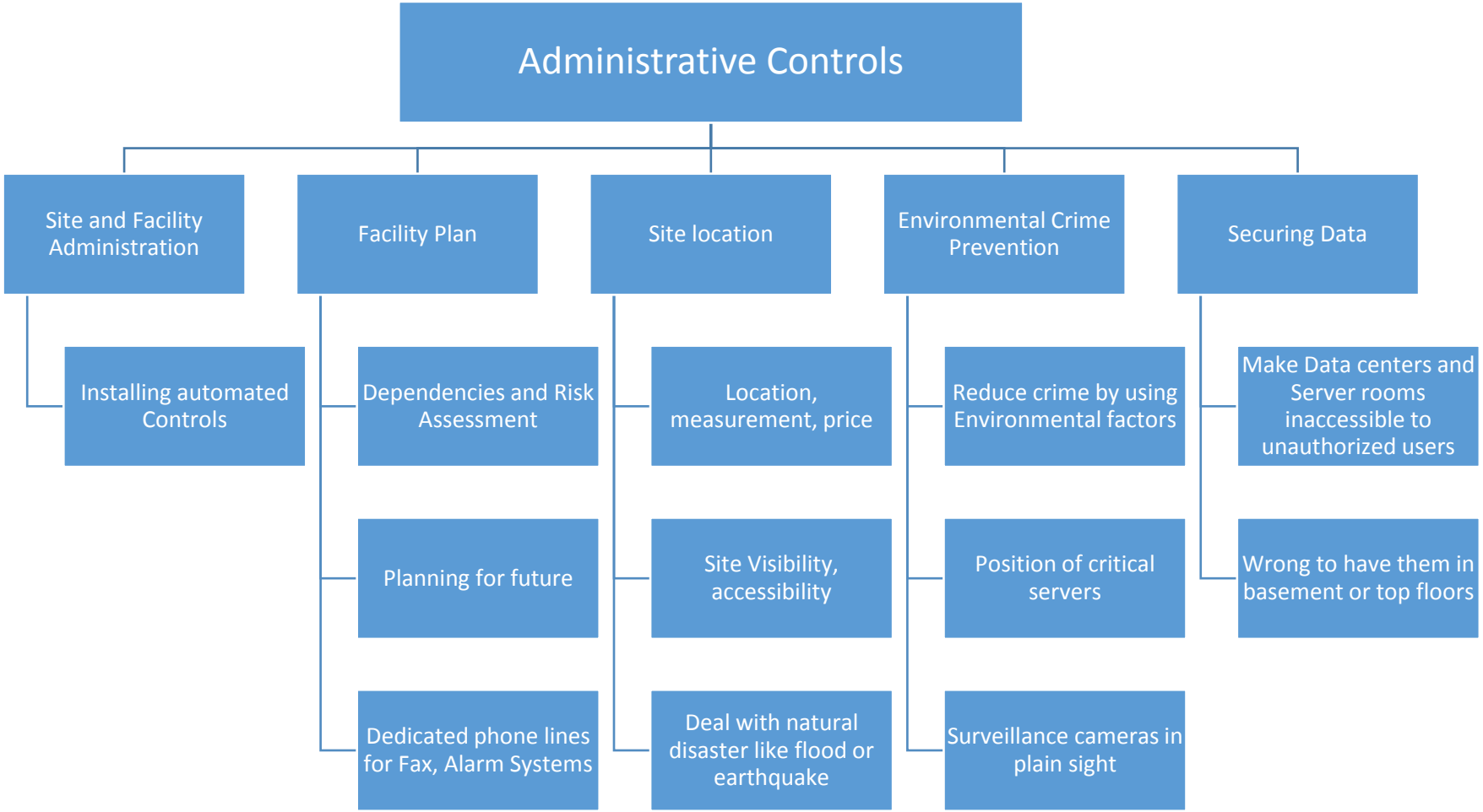
Physical controls

- Perimeter Security
- Badges
- Motion detectors
- Intrusion Alarms

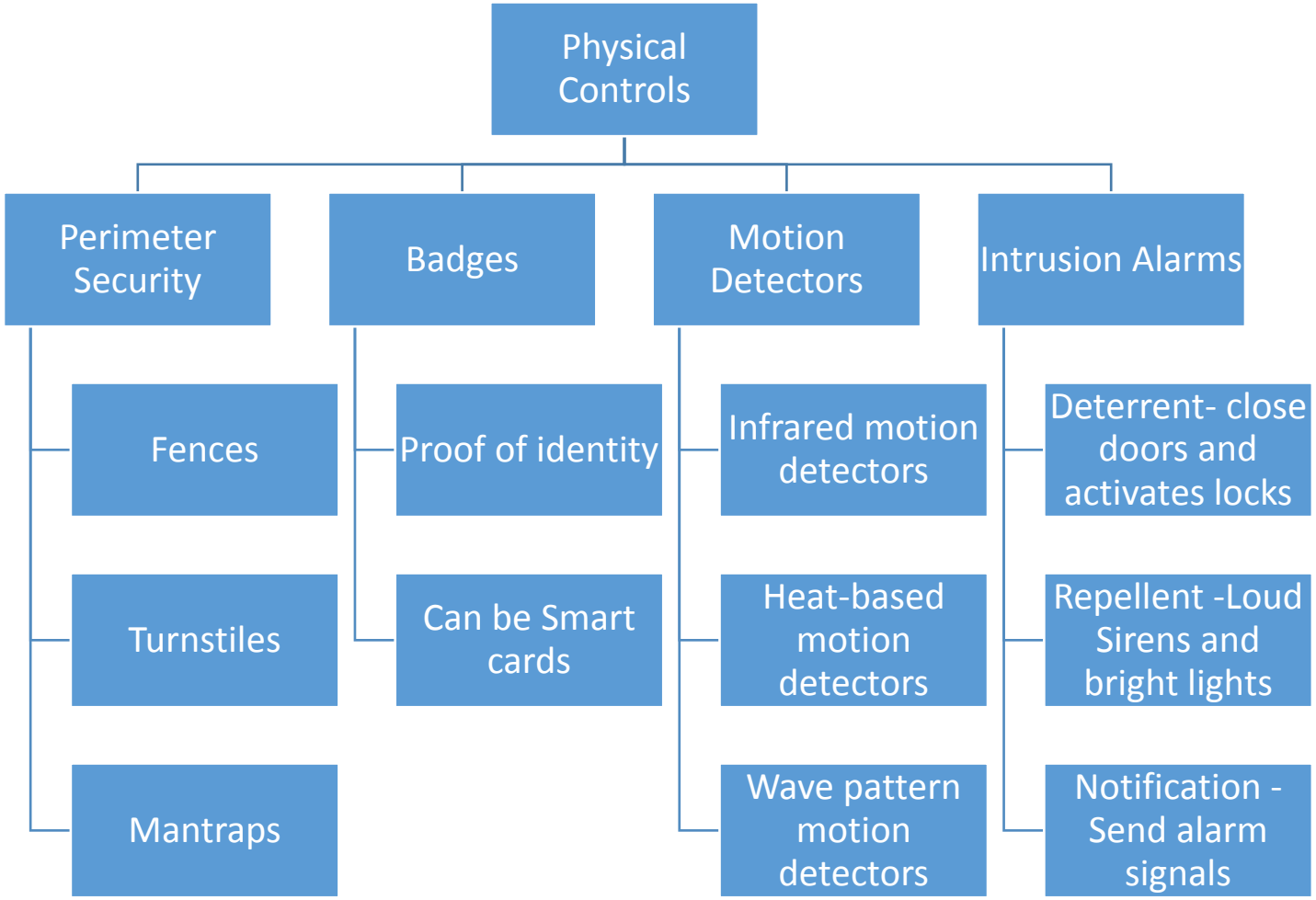
Technical Controls

- Smart Cards
- Proximity readers and RFID
- Intrusion detection, Guards, CCTV
- Physical access

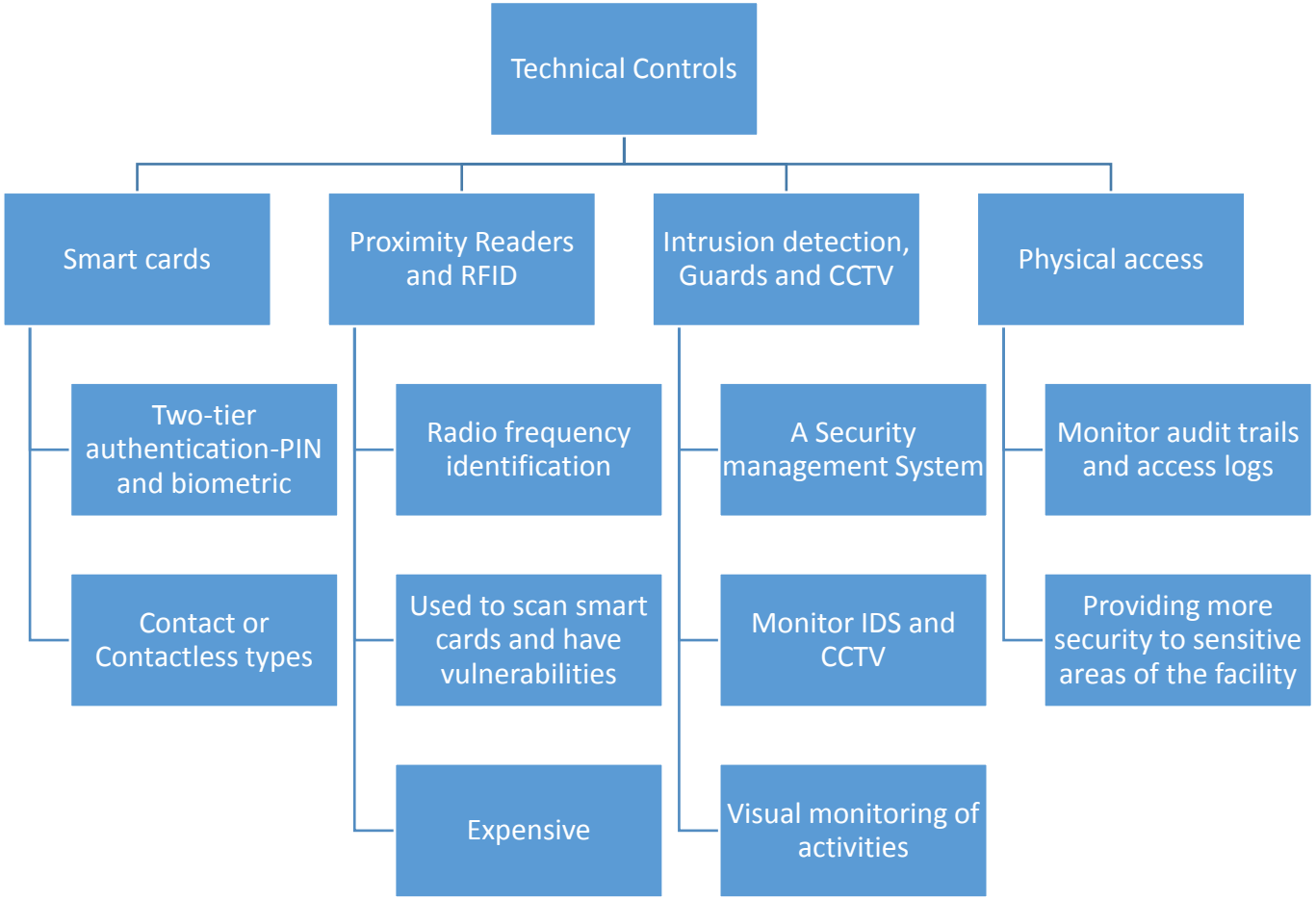
Various Components of Administrative Controls



Various Components of Physical Controls

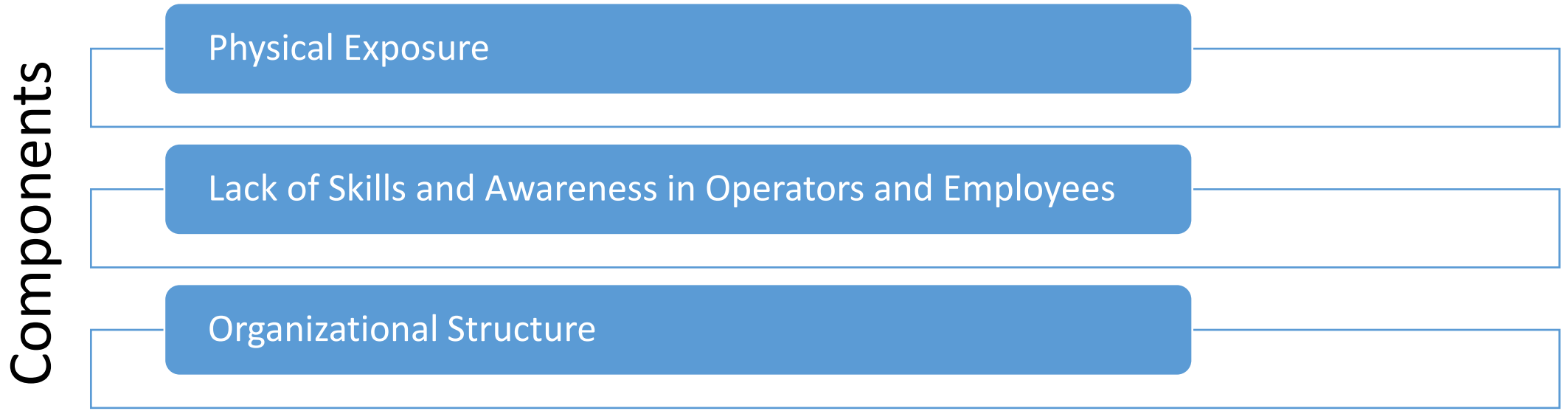


Various Components of Technical Controls



Attacks due to vulnerabilities in Physical security components

Physical attacks need not always come from a physical intrusion with the attacker present on the premises



Countermeasures

The mechanisms that can be used to countermeasure a physical attack, may vary depending on the nature of the target facility and the assets that are being stolen. It also varies on the nature of the damage caused. For example, consider the below situation:

- ✓ In a chemical manufacturing facility or a nuclear plant, acquisition of an asset by a hacker may lead to catastrophic incidences. Such facilities must install locked doors and vaults that can deny access to intruders
- ✓ If the loss of the asset has a high impact on the organisation, then containing it would be more suitable
- ✓ It may not be a financially viable option for some companies to have a robust and complete security solutionon their premises. They may view the recovery of the asset as a more convenient option

Quiz / Assessment

7) Which is 'not true' while describing the factors to be considered while choosing a physical facility for your company?

a) a) Checking visibility	b) Assessing transportation means	c) Inspecting options for installing access controls	d) Going over with the terms of joint tenancy, if any

8) Which of these is not an act to ensure physical security?

a) a) Defining a perimeter by putting up fences	b) Security guards manning the entry and exit points	c) Installing alarm systems	a) d) Segregating official documents as for private and general use

e-References & External Resources

- A white paper released from SANS ‘Physical Security and why it is so important?’ The report can be found at https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120
- *An article about ‘ Wireless Network Security, vulnerabilities, threats and countermeasures can be read at* http://www.sersc.org/journals/IJMUE/vol3_no3_2008/8.pdf
- *Read about 5D’s of perimeter security in the article* http://www.securitymagazine.com/articles/82833-the-5-d-s-of-outdoor-perimeter-security
- *An interesting article about how hackers combine Cyber threats and Physical security is given in* http://senstar.com/wp-content/uploads/2014/08/Cyber-Threats-in-Physical-Security-Whitepaper-2015.pdf
- Here is a good PPT about Viruses and Worms ; http://www.slideshare.net/hoangnamnguyen1694/ceh-v5-module-16-virus-and-worms
- Analysis of Web Application Worms and Viruses- http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Hoffman/BH-Fed-06-Hoffman-up.pdf by Billy Hoffman
- The 8 Most Famous Computer Viruses of All Time- https://uk.norton.com/norton-blog/2016/02/the_8_most_famousco.html

External Resources

1. John Kingsley-Hefty (Contributing Editor). *Physical Security Strategy and Process Playbook,* Elsevier
2. Ronald L.Krutz and Russel Dean Vines (2007), *The CEH Prep Guide,* Wiley Publications

Activity

Brief description of activity

Online Activity
(30min)

Description:
Visit a shopping mall and observe the physical security implemented atthe mall. Prepare a report reflecting your observations, categorising the various physical components into different categories.

Thank You