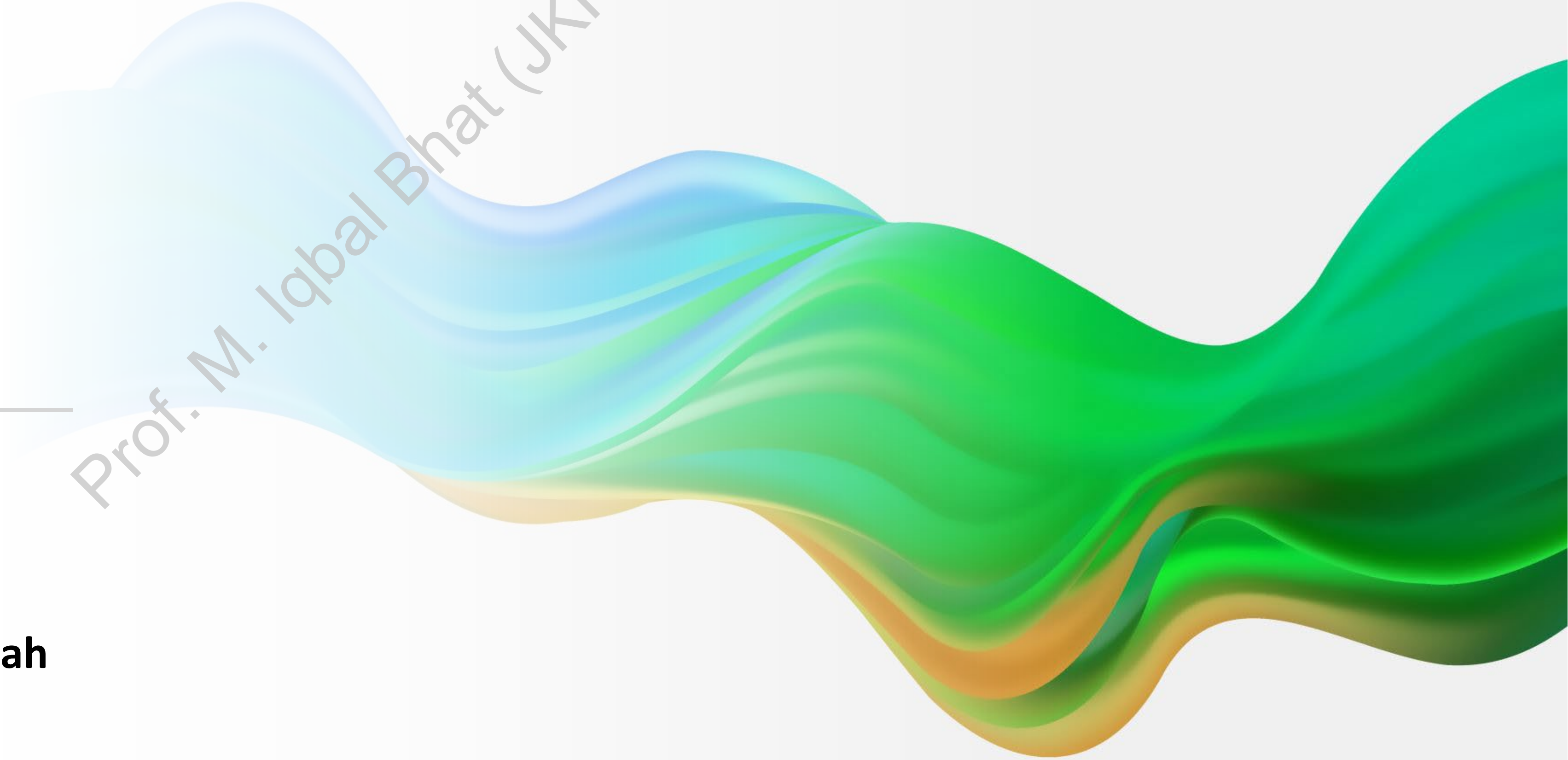
Trap Doors, Salami Attacks, Covert Channels, Control Against Program



By

Prof. Muhammad Iqbal Bhat

Government Degree College Beerwah

Topics

Trap Doors,

Salami Attacks,

Covert Channels,

Control Against Program

Trap Doors:

A trap door is a secret backdoor mechanism built into a system that allows an authorized person to access the system or specific functionality in a hidden way.

It is often added to software or hardware systems by the system designer or developer, and is not disclosed to the end user or system administrator.

The purpose of a trap door is to provide an emergency access mechanism that can be used by a system administrator to recover from a system failure or perform system maintenance activities.

Trap doors can also be exploited by attackers to gain unauthorized access or control over a system.

In some cases, a trap door may be intentionally added by an attacker during the development phase, enabling them to gain access to the system at a later time.

Trap Door examples:

1980: In the 1980s, the US National Security Agency (NSA) was accused of including a trap door in the Unix operating system that was distributed to foreign governments. The trap door was reportedly designed to allow the US government to gain access to the systems of foreign governments that were using the Unix operating system.

2004: In 2004, a researcher discovered a trap door in the Diebold Election Systems voting machines used in the US. The trap door was designed to allow election officials to update the software on the machines, but it was not disclosed to the public or election officials, making it a potential target for attackers.

2013: In 2013, it was reported that the NSA had a program called Bullrun, which involved inserting trap doors into commercial encryption products, such as virtual private network (VPN) software, to enable the NSA to bypass the encryption and gain access to the encrypted data.

Salami Attacks:

A salami attack is a type of financial crime that involves stealing small amounts of money or other resources from a large number of accounts or transactions over time.

The term "salami" refers to the idea of slicing off small pieces from a larger whole, in this case, stealing small amounts from multiple transactions or accounts.

Salami attacks are often carried out by insiders who have access to the systems or data they want to steal from. The stolen amounts are often small enough to avoid detection, but over time, the total amount stolen can be significant.

Examples of Salami Attacks:

In the 1990s, a programmer named Vladimir Levin used a salami attack to steal $10.7 million from Citibank. He gained access to the bank's computer systems and transferred small amounts of money from multiple accounts to a number of other accounts around the world, eventually stealing the total amount over a period of several months.

A common example of a salami attack is credit card fraud. Fraudsters steal small amounts from many credit card accounts, often by making small purchases or withdrawing small amounts of cash, and then repeating this process multiple times over a period of time.

Another example of a salami attack is the theft of computing power from a large number of computers over time. This can be done by installing malware that uses the victim's computer to mine cryptocurrency or perform other computational tasks, with the attacker taking a small portion of the processing power from each computer.

Covert Channels:

- A communication channel that is hidden from normal security measures, allowing unauthorized communication between two entities
- Purpose: to bypass security measures and exchange information without detection
- Risks: can be used for malicious purposes, such as stealing data or controlling a system
- Examples: using unused fields in network protocols to exchange data, using steganography to hide data within an image or audio file.

Examples of Covert Channels:

In the 1990s, researchers discovered a covert channel in the IP protocol that allowed an attacker to communicate with malware on a victim's computer without being detected by security software. The attacker could use unused fields in the IP header to transmit data to the malware, which would then respond by using other fields in the header to send data back to the attacker.

Another example of a covert channel is steganography, which involves hiding data within an image or audio file. The data can be extracted by someone who knows the secret key or algorithm used to hide the data.

Covert channels can also be used in social engineering attacks, where an attacker uses a seemingly innocent communication channel, such as email or instant messaging, to communicate with a victim and trick them into revealing sensitive information or performing a certain action.

Control Against Program:

Control against program attacks involve gaining control over a program or system and using it to carry out malicious actions.

These attacks can be carried out through vulnerabilities in the software or hardware, or through social engineering techniques that trick users into running malicious code.

Risks: can lead to data theft, system disruption, or other harmful consequences

Examples: gaining control over a web server and using it to launch DDoS attacks or steal data

Examples of Control Against Program:

A common example of a control against program attack is a distributed denial-of-service (DDoS) attack, where a large number of computers or devices are used to overwhelm a server or network with traffic, making it unavailable to legitimate users.

Another example of a control against program attack is ransomware, which is a type of malware that encrypts a victim's files and demands payment in exchange for the decryption key. Once the malware is installed on a victim's computer, the attacker can remotely control the malware and carry out the attack.

Control against program attacks can also be carried out through social engineering techniques, such as phishing emails or fake software updates that trick users into running malicious code or providing sensitive information.

Questions?