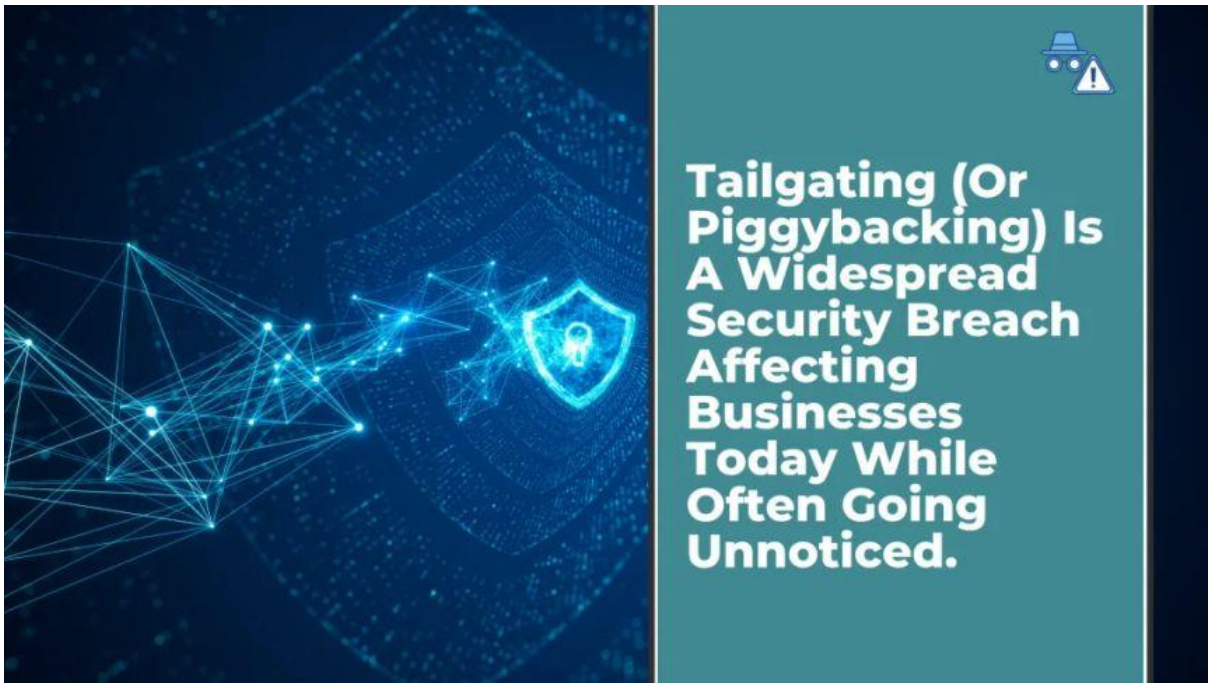
Fall Semester 2024-25
BCSE319L

Penetration Testing and Vulnerability Analysis
Faculty - Siva Shanmugham

Digital Assignment 1

Kruthardh Tirunahari

21BCI0400



Piggybacking

Piggybacking in cyber security refers to unauthorized access to a wireless network or a restricted area by “tagging along” with an authorized individual.

This can occur through various means, including:

- **Wireless Network Piggybacking**: Connecting to an unsecured or unprotected Wi-Fi network without permission, allowing unauthorized access to the network and potentially compromising sensitive data.

- **Physical Piggybacking**: Accompanying an authorized person to gain entry into a restricted area or bypass security checkpoints, which can be legal or illegal depending on the circumstances.

Types of Piggybacking

1. **Electronic Piggybacking**: Attaching acknowledgement to a data packet sent by another device, instead of using a separate transmission.
2. **In-Person Piggybacking**: Social engineering tactics used to gain physical access to restricted areas.

Here are the key characteristics of a piggybacking attack:

1. **Unauthorized Access**: The attacker does not have permission to enter the system but uses someone else's credentials or connection to get in.
2. **Relying on Trust**: The attack depends on exploiting the trust between the system and the legitimate user. This often happens when a user unknowingly allows the attacker to follow them in or share their access.
3. **Physical or Digital**: Piggybacking can happen in both real-world and online settings. In a physical setting, an attacker might follow someone through a secure door. In a digital setting, they might use someone's login session to access data or resources.
4. **Difficult to Detect**: Since the attacker is using legitimate credentials or access, it can be hard to spot unless someone is actively monitoring for unusual behavior.
5. **Exploiting Weak Security Practices**: Piggybacking often takes advantage of weak security habits, such as leaving a computer unlocked, sharing passwords, or not enforcing two-factor authentication.

Evolution of Piggybacking attack

The evolution of piggybacking attacks in cybersecurity reflects how attackers have adapted their techniques over time as security measures have improved.

1. Physical Piggybacking

- **Early Forms**: Initially, piggybacking was mostly a physical attack. For example, unauthorized individuals would follow employees into secure buildings or restricted areas without proper identification.
- **Increased Awareness**: As awareness grew, organizations started using security guards, keycards, and surveillance systems to prevent unauthorized physical entry.
- **Advanced Physical Security**: Today, more sophisticated systems like biometric scanners and multi-step authentication processes help guard against physical piggybacking. However, attackers still exploit moments of human error, like employees holding doors open for others.

2. Digital Piggybacking

- **Basic Digital Attacks**: With the rise of computer systems, piggybacking evolved into a digital issue. Early forms of digital piggybacking involved attackers physically using unattended or logged-in computers to gain access to sensitive data.
- **Session Hijacking**: As online systems became more common, attackers started focusing on session hijacking, where they would piggyback on an active session. This allowed them to bypass login credentials by exploiting open connections.
- **Malware and Phishing**: Over time, attackers began using malware, phishing attacks, or social engineering to trick users into giving them access or leaving their sessions open. This allowed attackers to "ride along" on active user sessions without the need for physical presence.

3. Modern Piggybacking Techniques

- **Cloud and Remote Access**: In today's world, where cloud services and remote work are common, piggybacking has evolved further. Attackers target unsecured Wi-Fi networks, poorly protected remote desktops, or shared cloud accounts to piggyback into systems from anywhere in the world.
- **Exploiting IoT (Internet of Things)**: With the explosion of IoT devices, attackers have started piggybacking through connected devices, such as smart home systems or business sensors, to gain network access.
- **Advanced Persistent Threats (APTs)**: In modern, highly targeted attacks, cybercriminals use piggybacking as part of larger strategies, like Advanced Persistent Threats, where they gain and maintain unauthorized access over extended periods without being detected.

Vulnerabilities Created by Piggybacking Attacks

1. **Unauthorized Access**: Piggybacking allows attackers to enter systems, networks, or physical locations without proper permission. This could lead to sensitive information being stolen, changed, or deleted.
2. **Data Breaches**: Once inside, attackers can access confidential data, such as personal information, business secrets, or financial records. This can lead to large data breaches, harming both companies and individuals.
3. **System Disruption**: The attacker might mess with system settings, delete important files, or install harmful software (malware), disrupting operations and causing downtime.
4. **Loss of Trust**: If customers’ or employees’ data is compromised, the organization can lose the trust of its users or clients. This can hurt the business and lead to legal consequences.
5. **Risk to Other Systems**: In connected environments, gaining access to one system through piggybacking can allow attackers to jump to other systems. This can spread damage across an entire network.

How to Prevent Piggybacking Attacks

1. **Strong Authentication Methods**: Use multi-factor authentication (MFA), which requires users to provide two or more verification methods (like passwords and a fingerprint). This makes it harder for attackers to piggyback on someone's access.
2. **Log Out and Lock Devices**: Always log out of systems or lock devices when stepping away, even for a short time. This prevents unauthorized people from using open sessions.
3. **Regular Session Monitoring**: Monitor active sessions and look for unusual behavior, such as accessing restricted areas. If anything strange happens, the system should alert administrators or automatically log out users.
4. **Secure Physical Access**: In buildings, use keycards, biometric systems, or security guards to prevent unauthorized people from entering. Train employees to avoid letting anyone follow them through secure doors.
5. **Education and Training**: Teach employees and users about piggybacking risks and how to recognize them. Encourage them to report any suspicious activity or behaviors.
6. **Use Zero Trust Security**: In a zero trust model, no one is trusted automatically, even if they are inside the system. Every access request is verified, which reduces the risk of piggybacking.