

**ASSIGNMENT (15%)**

Instructions:

1. 2 students/group
2. You have to choose any ONE from the FIVE main topics below:

* Bring your own device (BYOD)
* Email
* USB
* Public wireless access / hotspots
* Internet of Things (IOT)

Discuss security issues related to usage of the above technology / services chosen. As a network and security administrator, suggest prevention strategies to overcome them. You may include figure or table if necessary. A template with suggested headings are shown as below:

1. Introduction
2. Security and privacy issues (minimum 5)
   1. Session Hijacking

Generally, when a user signs in to an online account, the server sends back a session cookie, a small piece of information allowing the user to access their account. The server will allow users to access the application if their device has that session token. When a user signs out, their session token is terminated, and the user must re-enter their credentials to access their account again.

Session hijacking or cookie hijacking works when the attacker acquires the user’s session token and uses it to access the user’s account. This allows the attacker to gain unauthorized access to the user account without requiring the user’s credentials while the user loses all control over the session. Unlike active session hijacking, which requires for the attacker to be in between the target and the server, passive hijacking is a lot easier as it only requires the attacker to be on the same network as the victim.

One of the types of session hijacking that happens over unsecured public Wi-Fi or hotspots is session-side jacking. An attacker can monitor the network traffic and intercept the user’s session cookies using a packet sniffer after authentication. This is more likely to happen on websites that encrypt their login pages using SSL (Secure Socket Layer) or TLS (Transport Layer Security), as the attacker can use the session key obtained from the packet sniffing to take control of the user’s session and act in their place while interacting with the web application.

One of the consequences of session hijacking is the theft of sensitive information, as the attacker may obtain the user’s login credentials or personal information. The attacker could also impersonate the user on the website and carry out unauthorised transactions or gain access to private content by taking control of the user’s session. Since the attacker can control the user’s session and perform actions on the user’s behalf, this could result in privacy violations or financial loss.

* 1. MITM attack

MITM attack or Man in The Middle attack occurs when the attacker intercepts or alters the communications between two parties by inserting themselves between them without the two parties’ acknowledgement. MITM attacks usually aim to eavesdrop on a conversation or steal credentials and personal information. Several types of Man in The Middle attacks include packet sniffing, ARP spoofing, DNS spoofing and Wi-Fi eavesdropping.

ARP spoofing allows the attacker to intercept, alter or block network traffic. ARP spoofing happens when an attacker sends fake ARPSS messages to link their MAC address to the IP address of a different device, typically the default gateway or another target. Traffic intended for the victim's device is diverted to the attacker’s computer. If the attacker is connected to the same network, ARP spoofing can happen over public Wi-Fi. The attacker can divert traffic from other users to their computer by altering ARP tables. The attacker can then execute session hijacking, intercept confidential data and carry out other attacks. The attacker could also set up a rogue Wi-Fi hotspot with a similar name to a legitimate hotspot name to fool users into joining the network.

DNS spoofing, another type of MITM attack, typically targets public Wi-Fi networks. DNS spoofing is an attack that modifies DNS server entries, causing a name server to return a malicious website rather than a legitimate IP address. Users are prompted to log into their accounts on the malicious websites. Users believe that they are on the official website, but when they log in, they end up sharing their credentials with the attacker. Additionally, malicious websites can leak confidential information or infect the user’s device with viruses.

Wi-Fi eavesdropping describes the unauthorised monitoring and interception of wireless network traffic, which enables the attacker to obtain sensitive data sent over a Wi-Fi network by taking advantage of the vulnerabilities in communication protocols. This attack could happen even towards networks secured using WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access) with weak passwords. Firstly, the attacker captures and analyses data packets sent over the Wi-Fi network using packet sniffing tools. The Standard tools used in this attack are Wireshark, tcpdump, and Aircrack-ng. This allows the attacker to intercept data packets and read their contents, including unencrypted data.

1. Prevention strategies
   1. Session Hijacking

One of the ways to prevent session hijacking is to enable Two-Factor Authentication (2FA). By requiring users to enter a second factor, such as code texted to their mobile device, in addition to their password, 2FA adds an extra layer of protection to the websites. Even if the attackers manage to obtain the login credentials from session cookies, 2FA can prevent them from getting access to the user’s account.

* 1. MITM attack

1. Conclusion

References

Submission:

Report should use 1.5 spacing, 12-point Times New Roman font. The minimum number of page is 15 pages. Sources should be cited according to APA method. Your submission will be checked for plagiarism in Turnitin. You need to submit in PDF format. Failure to adhere to these rules will incur a penalty.

Please submit your completed assignments by 12.59pm, 7th January 2024.