**A logo of a university

Description automatically generated**

Western Governors University

**Emerging Technologies in Cybersecurity**

**C844**

**Greg Westmoreland**

**GRP1 Task 2: WLAN AND MOBILE SECURITY PLAN**

**A. WLAN Vulnerabilities**

**The first vulnerability for WLAN:**

The Alliah company utilizes a wireless local area network with a GB fully managed-switch, a wireless network controller, and several Wi-FI access terminals placed in various locations through out the office. Offering a Wireless network gives an opportunity for different types of vulnerabilities that could transpire known as insider threats. What if a disgruntled or malicious employee intentionally introduces a vulnerability to the company network? They can “…use privileged access to steal sensitive or valuable data for personal financial gain”([Froehlich 2](#Two))? One such example, is an Evil-Twin Access Point. “The definition of an Evil-Twin Access point, is a wireless access point with a duplicate service set identifier (SSID), set to the same name as the real access point. This fools unsuspecting users into connecting to the evil-twin instead of the real access point” ([Doherty 74](#One)). Once a user logs onto the evil-twin access point, their traffic can be sniffed and analyzed using a packet sniffer, such as Wireshark, potentially revealing sensitive data while connected to the fake access point.

**The second vulnerability for WLN:**

A threat can be unintentional when an employee will “…sometimes create vulnerabilities when they try to circumvent policies or device configurations” ([Doherty 73](#One)). One such example of a WLAN vulnerability would be when an employee hooks up a rogue-access point. This rogue-access point would be plugged into a wired network port and could potentially provide wireless access to attackers outside of Alliah’s internal network. Once an outside attacker has access to the internal network, they can begin to capture packets and ascertain which type of attack they can administer next.

**B Mobile Vulnerabilities**

**The first vulnerability for Mobile devices**

Alliah employs five account representatives who travel eighty percent of the time to different locations. As they travel, they use their mobile devices to stay connected to the office. With company-issued laptops, tablets, and smartphones, they are able to check work email, upload/download company documents, and schedule appointments with customers. While on the road traveling, they face different types of vulnerabilities that specifically target their mobile devices. The most common issue they face is the vulnerability of data theft. Once an attacker is able to access sensitive data that is obtained on a lost or stolen device, they can take that data and place it for sale on the dark web. By placing information for sale on the dark web, it can be very profitable to the highest bidder by illegall obtaining this information. Hackers can sell information that can contribute to identity theft. They will offer items for sale like social security numbers, credit card numbers, date of birth, and other personal information. “Often hackers bundle your personal information with other stolen data and sell it en masse to other criminals on the dark web, who can then use it in their own shady schemes” ([Mail.com Blog 3](#Three)).

**The second vulnerability for Mobile devices**

Another challenge the account representatives face while traveling on the road is device control threats. This vulnerability is often seen with near-field communication hacking. Near Field Communication, also known as NFC, is a close proximity connection between two pieces of technology that communicate with each other. If a hacker were able to successfully exploit a mobile device with a NFC hack, such as one of the account representative’s smartphones, they could potentially take full control of that device.

**C. Mitigation**

**First Mitigation for WLAN**

Companies are safely able to offer WiFi for their employees with wireless intrusion prevention systems, also known as WIPS. This detection software is able to determine if their is a bad activity happening on the wireless network. One such example would be that the WIPS is able “to determine if there is a duplicate, evil twin access point. The WIPS would then attempt to keep employees from connecting to it by mistake” ([Orsi 4](#Four)). The IT staff of Alliah could implement another wireless instruction prevention system called Watch Guard. "This Intrusion Prevention Service, also known as an ’IPS’, will use common trace signatures to provide real-time protection against corporate network attacks" ([Intrusion Prevention Service 5](#Five)).

**Second Mitigation WLAN**

Alliah IT staff can “…scan all card data environment locations for known wireless access devices and maintain an up-to-date inventory” ([Glover 6](#Six)). This up-to-date inventory could also document the firmware that is installed on all wireless assets used by the company. Anytime a new firmare is released by the vendor, this inventory could keep track of which devices need to be patched and updated with the latest security software updates. Other tools to utilize by Alliah would be scanning and vulnerability tools. One tool available on the market for enterprise companies, is the SolarWinds Security Event Manager (SEM) IDS/IPS. This software is able to “take logs from firewalls, switches, routers, and various production nodes and be able to make decisions to mitigate any attacks that are occurring on a company’s network” ([SolarWinds 7](#Seven)).

**First Mitigation for Mobile devices**

When dealing with data theft on mobile devices, strong encryption is the key to protecting Alliah’s data. "Encryption is useful for laptops and other smaller devices that can be physically lost or stolen. This ensures that should a laptop, phone, USB, etc. is stolen or lost, the data is still secured" ([Securing Mobile Devices with Mobile Encryption 8](#Eight)). One mobile security solution that is available to businesses like Alliah, is the MaaS360 by IBM. This software Is able to provide mobile device management to keep a close control on Alliah’s mobile devices, laptops, tables, and smartphones. “IBM Security® MaaS360® protects devices, apps, content and data by building a zero trust strategy with modern device management” ([Manage and protect your mobile workforce 9](#Nine)).

**Second Mitigation for Mobile devices**

To protect the account representative’s mobile devices from Near Field Communication (NFC) hacking, Alliah's IT staff could require that the company-issued devices, specifically smartphones, will have their NFC communication disabled, by default. The account representatives will not be able to utilize Apple Pay. This feature will be disabled by default and management software installed on the phone will not allow it to be enabled. One such tool that could be used by Alliah is JamfPro. This device management software allows full management of company-issued smartphones "...by leveraging native security features. Manage device settings and configurations, restrict malicious software, and patch all of your Apple devices without user interaction" ([Jamf Pro for Apple Device Management 10](#Ten)).

**D. Preventative Measures**

**Supply A Plan of Action To Combat WLAN Attacks**

One way to combat attacks on wireless local area networks, is to allow the IT department to install special software-based controls that permit or deny WLAN access for employees based on the devices mac address. “By controlling the mobile devices on the operating system level, such as specific wireless drivers or even specialized software from a particular vendor can help control these connections in a safe manner” ([Souppaya and Scarfone 6](#Eleven)). These mandatory controls should be an essential part of the operating system upon setup for the company-owned laptops, tablets, and smart phones that are distributed to all Alliah employees that will have access to the wireless network.

**Supply A Plan of Action To Combat Mobile Environment Attacks**

A second way to combat attacks on mobile enviornments is to allow the IT department at Alliah to be able to install Zimperium management device software on all company-issued tablets. “Zimperium MTD, used to be known by the name of zIPS, is a mobile threat defense solution for entprise level companies. Zimperium MTD is able to detect network threats issue kill commands that minimize phishing, malicious activity, and application attacks” ([Zimperium zIPS | Mobile Intrusion Prevention System 12](#Twelve)). The Zimperium software will give the IT staff the ability to perform regular scans on the tablets for any harmful applications.

**Reference federal, state, or industry regulations that justify these measures.**

Alliah’s CEO, Jennifer, plans on becoming a public traded company with the next year or so. With this cautious approach and implementation of these measurements on company-issued equipment, Alliah is protecting its network, assets, and financial reputation. When they go public and begin trading on the New York Stock Exchange, Alliah will be in full compliance with The Sarbanes-Oxley Act (SOX) of 2002. The SOX Act is a federally regulated law for all publically traded companies. Alliah’s investors will be able to have full confidence in the company because this regulation requires absolute adherence to reputable “…corporate governance and the integrity of financial reporting” [(Doherty 84](#One)).

**E. Recommended BYOD Approach**

**Recommendation:**

After doing some extensive research on “Bring Your Own Device”, also known as BYOD, Alliah has decided to take the specified approach for personally owned devices on the company’s wireless LAN. Most of the research was done from the NIST SP 1800-22 Mobile Device Security: Bring Your Own Device (BYOD) paper, published by the National Institute of Standards and Technology (NIST). “The goal of the Mobile Device Security: Bring Your Own Device practice guide is to provide an example solution that helps organizations use both a standards-based approach and commercially available technologies to help meet their security and privacy needs when permitting personally-owned mobile devices to access enterprise resources” ([NIST SP 1800-22 13](#Thirteen)).   
  
Alliah will allow a flexible work environment that will permit its employees to utilize their personal devices at the office for business-related tasks. We remain committed to maintaining the highest standard of security and integrity for our information systems and company data. By adhering to the NIST Special Publication 1800-22, we can minimize the risk of introducing malicious code and viruses to our internal network.

Effective immediately, Alliah will permit employees to use their personal devices, including but not limited to, smartphones, tablets, and laptops. These devices will be allowed access to the internal network to process business-related tasks. Any devices that will be used on the company’s internal network will be subject to security measures agreed to by the employee prior to use.

All personal devices that are intended to be used for business-related tasks must be presented to the IT department to be registered. This will document the device type, name, serial number, and mac address. All devices will be verified to have all of the up-to-date software and operating system’s latest security patches. All devices will have McAfee antivirus or another vendor-approved ant-viirus/anti-malware software installed on them.

All devices must be password protected and adhere to the company’s password complexity standards. All devices will be installed with management device software allowing for remote data wipe, in case an item is lost or stolen. Alliah reserves the right to visually inspect a device at any time for additional auditing and monitoring.

All employees must agree to these measurements prior to a BYOD use on the internal company network. Any violations of such policy will forfeit the employee’s use of their device on the company network. Questions and concerns can be brought to the compliance department in writing.

**References**

1. Doherty, Jim *Wireless and Mobile Device Security*, 2nd ed., Jones & Bartlett Learning, 2022.
2. Froehlich, Andrew. “Insider Threat” <https://www.techtarget.com/searchsecurity/definition/insider-threat> September 25, 2023.
3. Mail.com Blog "What happens when data is hacked? What hackers do with personal data" <https://www.mail.com/blog/posts/why-do-hackers-steal-data/178/> July 3, 2023.
4. Orsi, Ryan. "Understanding Evil Twin AP Attacks and How to Prevent Them" <https://www.darkreading.com/attacks-breaches/understanding-evil-twin-ap-attacks-and-how-to-prevent-them> November 14, 2018.
5. "Intrusion Prevention Service" <https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/services/ips/ips_intro_c.html> September 25, 2023.
6. Glover, Gary. "Wireless Access Point Protection: 5 Steps to Find Rogue Wi-Fi Networks and Comply with PCI DSS Requirement 11.1" <https://www.securitymetrics.com/blog/wireless-access-point-protection-finding-rogue-wi-fi-networks> September 25, 2023.
7. "SolarWinds Security Event Manager Datasheet" <https://www.solarwinds.com/assets/solarwinds/swdcv2/licensed-products/security-event-manager/resources/datasheet/sem-datasheet.pdf> September 25, 2023.
8. "Securing Mobile Devices with Mobile Encryption" <https://www.securitymetrics.com/blog/securing-mobile-devices-mobile-encryption> September 25, 2023.
9. "Manage and protect your mobile workforce" <https://www.ibm.com/products/maas360> September 25, 2023.
10. "Jamf Pro for Apple Device Management" <https://www.jamf.com/lp/jamf-pro-2/#security> September 25, 2023.
11. Souppaya Murugiah and Scarfone Karen. "Guidelines for Securing Wireless Local Area Networks (WLANs) Recommendations of the National Institute of Standards and Technology" [https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf February 2012](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf%20February%202012).
12. "Zimperium zIPS | Mobile Intrusion Prevention System" <https://www.zimperium.com/zips-mobile-ips/#:~:text=Zimperium%20MTD%20(formerly%20zIPS)%20is,%2C%20phishing%2C%20and%20app%20attacks> September 25, 2023.
13. "NIST SP 1800-22 (2nd Public Draft) Mobile Device Security: Bring Your Own Device (BYOD)" <https://csrc.nist.gov/pubs/sp/1800/22/2pd> November 29, 2022.