CSG3308 Wireless security

Assignment 2 – Wireless Network Audit

Family Name: David Selvam

Given Name: Visahl Samson

Student Number: 10498743

Name of Lecturer: : Loh Kah Yee

Campus: PSB Academy, Singapore

Due Date: 06th April 2020

Contents

[**Introduction** 2](#_Toc36819646)

[**Wireless Security threats in the given network design** 2](#_Toc36819647)

[WEP Shared Key 3](#_Toc36819648)

[Wireless Temperature Sensor 3](#_Toc36819649)

[Cisco ASA 5585-X firewall 4](#_Toc36819650)

[Unmanaged switch 4](#_Toc36819651)

[**Attack Scenario** 4](#_Toc36819652)

[An actual attack based on WEP 5](#_Toc36819653)

[An attack based on IoT temperature sensor 5](#_Toc36819654)

[Cisco ASA 5585-X firewall 5](#_Toc36819655)

[Unmanaged Switch 6](#_Toc36819656)

[**Wireless network policy** 6](#_Toc36819657)

[Scope 6](#_Toc36819658)

[Policies 6](#_Toc36819659)

[**Countermeasures for the threats identified** 6](#_Toc36819660)

[WEP Encryption (Wireless) 6](#_Toc36819661)

[IoT devices 7](#_Toc36819662)

[Gateway firewall 8](#_Toc36819663)

[Unmanaged switch 8](#_Toc36819664)

[**Conclusion 8**](#_Toc36819665)

[**References 9**](#_Toc36819666)

# Introduction

In modern times Wireless Networks have become popular everywhere from business organizations to individuals. We can point out the significant growth in the use of wireless networks everywhere. Regardless of size and type of organization, all the sectors are using the wireless network for its affordability, flexibility, easy to configure function. But when comes to security there is no single technology with no vulnerability. The same thing applies to wireless networks also. As technology grows the security threat also grows along with it. So, it’s important to develop strategies to combat the threats against wireless networks.

# Wireless Security threats in the given network design

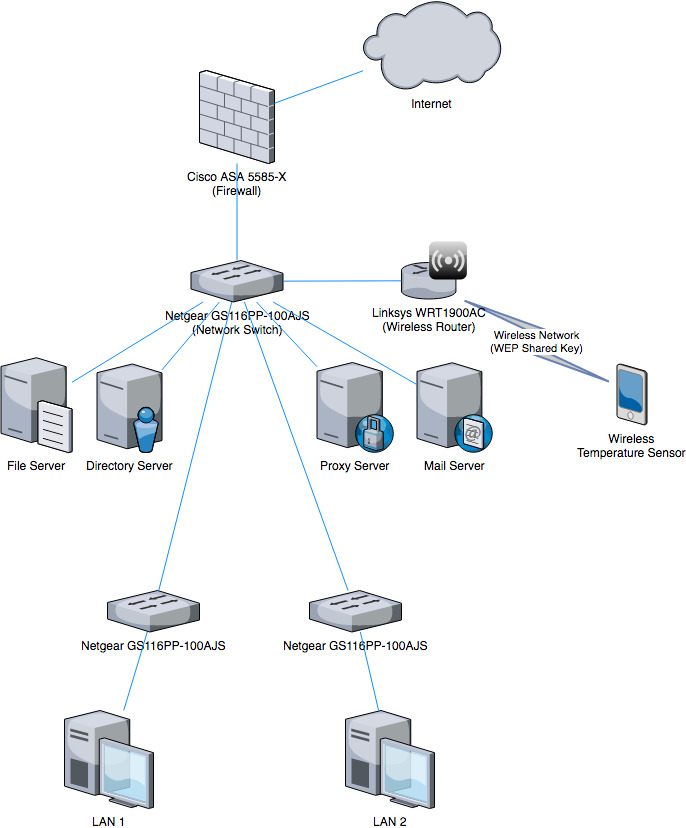


Figure 1 Given Network Design

The given wireless network design consists of several threats that increase security risks. Since it's for wireless the top 3 wireless security threats associated with the wireless network are WEP Shared Key, Wireless Temperature sensor, Cisco ASA 5585-X firewall.

## WEP Shared Key

WEP stands for Wired Equitant Privacy. WEP is a security protocol comes under IEEE 802.11 standards (Margaret, 2006). It was originally introduced in 1997. WEP aimed to secure the wireless network as secure as wired networks. WEP has several security flows and it can be compromised for several attacks. Some of the attacks are (Issac, n.d.) active attacks to decrypt the traffic, active attack to inject the packet, and table-based attack (typically uses a decryption table). Apart from those primary attacks, few other attacks are (Packt, 2015) FMS attacks (**Fluhrer, Mantin, and Shamir) in 2001, PTW attacks (Pyshkin, Tews, and Weinmann) in 2007, and ARP requested relay attacks.** Also, the router model that is in place has been reported (Tom, 2017) that it’s vulnerable for several kinds of attacks including DOS, Authentication bypass.

According to NIST standards 2016 Revision 1, (Paulsen & Toth, 2016) WEP is no longer considered as a trusted encryption protocol due to its vulnerabilities. So, NIST advised not to use WEP anymore.

## Wireless Temperature Sensor

In recent days usage of sensors has been increased. These sensor devices connected to a network are called IoT devices (Internet Of Things). These IoT sensors can be used for several different purposes such as temperature, humidity calculation, vacuum, etc... But these IoT devices consist of high-security issues which makes them easy to compromise. According to Netscout’s threat intelligence report (NETSCOUT, 2019), it takes only five minutes to attack/compromise an IoT device once it is connected to the internet. Also, privacy in IoT devices is another reason to consider here. So, if an IoT device that is connected to the internet is compromised then it might lead to the exploitation of the entire network that the device is connected to.

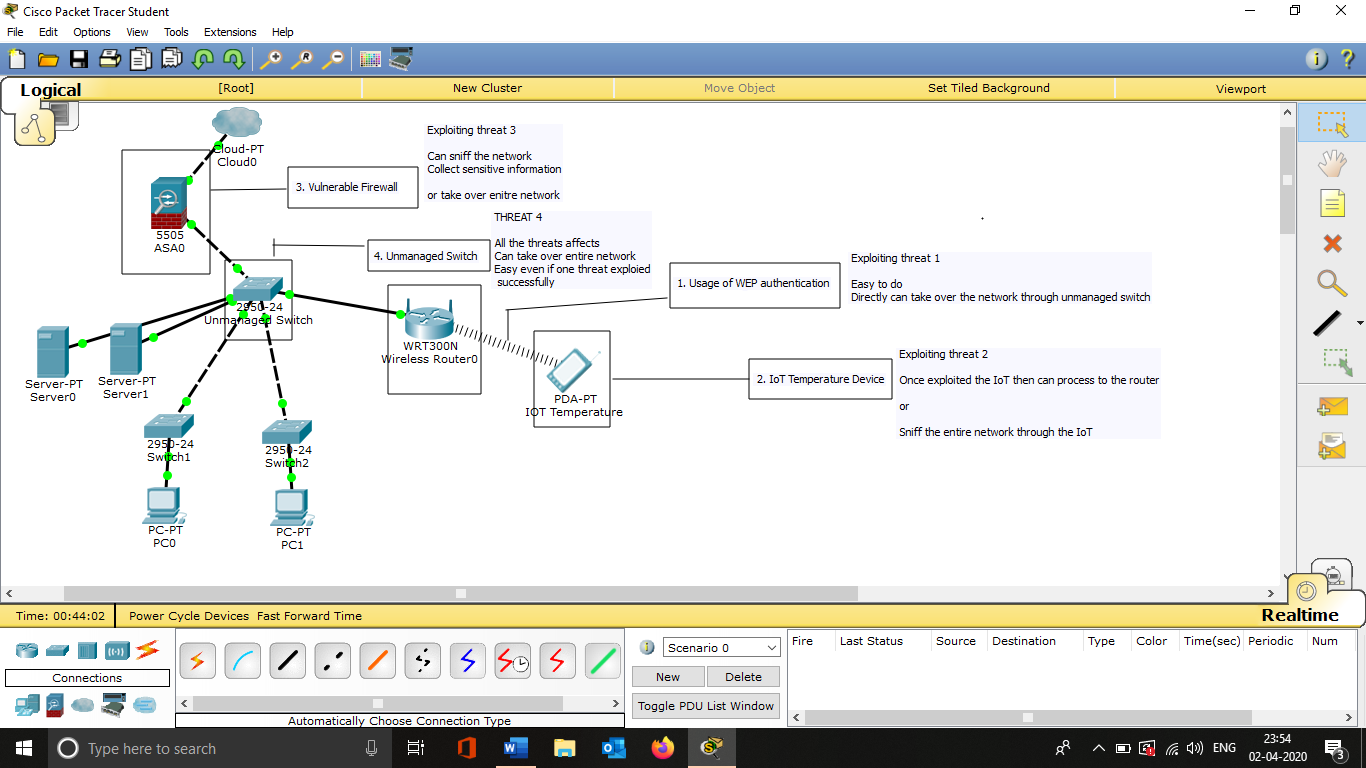
## Cisco ASA 5585-X firewall

The given Cisco ASA 5585-X firewall has several security vulnerabilities reported. According to the United States Computer Emergency Readiness Team (CISA Cyber + Infrastructure, 2016), exploitation of these vulnerabilities possible allows a remote attacker to take over the entire affected system. After the announcement, Cisco has issued several patches for several products. Since it’s stated that the firmware update date is unknown for their company’s Cisco ASA 5585-X firewall it’s possible to compromise it.

## Unmanaged switch

Unmanaged switches always need careful handling. Because exploiting these switches can be done easily and will cause severe impact to the organization. Apart from security issues, these switches cause an impact in the quality of service because unmanaged switches cannot balance (Scot, 2016) the network traffic properly since no configurations are in place.

# Attack Scenario



Screenshot Attack Scenario Diagram

Screenshot 1 shows the attack vectors that are identified. At this point even if anyone point has been compromised it will impact the entire network. Because all the vectors are connected at a single center point which is the unmanaged switch.

## An actual attack based on WEP

In 2007 TK Maxx security breach was a sensational and well-known one. This breach also is known as the world’s largest commercial security breach back in time. During this data breach, the attackers stole 45 million customer records (Espiner, 2007) which include their credit and debit card details. This data breach led TK Maxx to offer 40.9 Million USD as a settlement (Espiner, 2007) . When the analysis was done by the organizations the root cause of this data breach was using WEP. It is reported (Simon, 2007) that Tk Maxx was using WEP and attackers successfully cracked that and installed the credit harvester software on the company’s systems.

This breach clearly shows how much impact that using WEP can cause to an organization.

## An attack based on IoT temperature sensor

IoT based malware campaigns are increasing day by day. A unique breach that suits for the IoT temperature sensor that is given in this case study happened in 2017. According to the Dark Trace global threat report 2017 (Dark Trace, 2017) it is stated that hackers exploited a casino’s fish tank temperature sensor to breach the security. During the data breach 10GB size of data has been transferred to out of the company’s network. The name and other details of the casino associated with this incident are not disclosed.

Apart from that specific incident, one more emerging threat that targets the IoT devices is Mirai It’s (Cloudflare, n.d.) a malware that affects the IoT devices connected through the internet and turns them into botnets that cybercriminals can utilize. In 2016 October a massive DDoS attack made the internet not accessible on the USA east coast (Fruhlinger, 2018). Researches revealed that the DDoS attack caused due to IoT botnet i.e. Mirai. So, securing IoT devices in a network is crucial to avoid security incidents.

## Cisco ASA 5585-X firewall

There are no specific real-world security incidents that happened due to this specific product but there are a huge amount of vulnerabilities that have been reported for it. According to NIST’s NVD (National Vulnerability Database) (NVD, n.d.) records, there are 56 CVE’s are published for this particular product. And the majority of these vulnerabilities allows the external attacker to perform privilege escalation and take control over it.

## Unmanaged Switch

Same as the previous threat there is no specific real-world security incident that happened only because of an unmanaged switch. Because switches cannot be compromised directly unless other parts of the infrastructure compromised and then only it is possible to compromise the switches.

In the given scenario the multiple several vulnerabilities are easy to exploit and then the unmanaged switch can be compromised easily. Also, due to the nature of the unmanaged switches, attackers can exploit it very easily.

# Wireless network policy

## Scope

The wireless policy applies to all areas of wireless connection across the company network infrastructure and consists of all wireless devices operating within the company IP range, on any of the company premises, or any remote location connected to the company network directly.

## Policies

* All-access points must stand by all national guidelines concerning to wireless devices. (National guidelines are the one regulated by the country that the company operates in. Also, other guidelines such as ISO27001, NIST can be followed)
* Users will be authenticated on the wireless network for each session that they’re connecting in.
* It is users responsibility that their devices containing up to date antivirus software and operating system is fully patched.

# Countermeasures for the threats identified

## WEP Encryption (Wireless)

According to NIST 800-153 (Murugiah & Karen, 2012), the following are some recommended guidelines for wireless networks that can be act as suitable counter measures,

* Replacing the WEP authentication mechanism with a more advanced security algorithm such as WPA2.
* Following standardized security configurations for common WLAN components such as client devices and Access points. (this includes changing default wireless AP/admin passwords).
* Drafting a clear wireless usage policy across the organization.
* Performing attack monitoring, vulnerability monitoring at the same time to support security.
* Conducting periodic review/audits on the wireless network.

## IoT devices

Since IoT is emerging organizations like NIST haven’t compiled a structured standard for it. But some other government bodies around the world made some guidelines on IoT devices. The following are the guidelines made by IMDA Singapore (IMDA, 2020) that can be act as suitable counter measures,

* Implementing strong cryptography with following specifications
  + Usage of approved algorithms
  + Sufficient key length
  + Recommended crypto period
* All sensitive communications from/to IoT devices must be encrypted.
* Threat modeling should be conducted at the beginning of the implementation stage.
* Roof-of-trust (Provides tamper protected module to establish security mechanisms) should be established to components like IoT gateways, and IoT platforms.
* Implementation of a secure version of transport protocols. Like usage of TLS while using MQTT.
* Disabling non authenticated Bluetooth pairing measures.
* Segregating the IoT device if required
* Usage of proper access control with the following specifications
  + Changing all default passwords
  + Using multi-factor authentication for high impacted remote operations
  + Security measure to keep the physical access safe

## Gateway firewall

According to NIST 800-41 (Karen & Paul, 2009), the following guidelines are recommended,

* Keeping the hardware/software firewall up to date along with fully patched
* Firewall policy should specify how the firewall going to handle both the inbound and outbound traffic.
* Periodically reviewing the logs, security alerts and applying appropriate actions on them.

## Unmanaged switch

* Properly configuring the switch with security controls
* Applying VLAN control on a switch and segregating the IoT/wireless device.
* Properly updating the patches/firmware.

# Conclusion

In cybersecurity, there is no single solution for all the issues rather several protocols can be applied to reduce the security incidents. This same applies to wireless security also. Due to emerging and inevitable wireless network benefits, the threats also emerging and specifically emerging IoT technology comes with more security issues and introducing new vulnerabilities. Organizations like NIST are currently developing standard strategies to combat the threats and it’s expected that in the upcoming era the issues can be reduced.

# References

CISA Cyber + Infrastructure. (2016). Cisco Releases Security Updates | CISA. Retrieved from <https://www.us-cert.gov/ncas/current-activity/2016/05/04/Cisco-Releases-Security-Updates>

Cloudflare. What is the Mirai Botnet?. Retrieved from <https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/>

Dark Trace. (2017). Global Threat Report 2017 Selected Case Studies (p. 8). Dark Trace. Retrieved from <https://www.infosecuritynorthamerica.com/__novadocuments/504567?v=636718219701230000>

Espiner, T. (2007). TJX offers US$40.9M settlement over breach | ZDNet. Retrieved from <https://www.zdnet.com/article/tjx-offers-us40-9m-settlement-over-breach/>

Espiner, T. (2007). Wi-Fi hack caused TK Maxx security breach | ZDNet. Retrieved from <https://www.zdnet.com/article/wi-fi-hack-caused-tk-maxx-security-breach/>

Fruhlinger, J. (2018). The Mirai botnet explained: How IoT devices almost brought down the internet. Retrieved from <https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html>

IMDA. (2020). Guidelines Internet of Things (IoT) Cyber Security Guide. *IMDA Iot Cyber Security Guide V1*, *V1*. Retrieved from <https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/Reference-Spec/IMDA-IoT-Cyber-Security-Guide.pdf>

Issac, B. (In)Security of the WEP algorithm. Retrieved from <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>

Karen, S., & Paul, H. (2009). Guidelines on Firewalls and Firewall Policy. *National Institute Of Standards And Technology Special Publication 800-41 Revision 1*, *Revision 1*. Retrieved from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf>

Margaret, R. (2006). What is Wired Equivalent Privacy (WEP)? - Definition from WhatIs.com. Retrieved from <https://searchsecurity.techtarget.com/definition/Wired-Equivalent-Privacy>

Murugiah, S., & Karen, S. (2012). Guidelines for Securing Wireless Local Area Networks (WLANs). *Recommendations Of The National Institute Of Standards And Technology*. Retrieved from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf>

NETSCOUT. (2019). DAWN OF THE TERRORBIT ERA. doi: SECR\_001\_EN-1901

NVD. NVD - Results. Retrieved from <https://nvd.nist.gov/vuln/search/results?adv_search=true&cves=on&cpe_version=cpe:/a:cisco:adaptive_security_appliance_software:7.2.3.1>

Packt. (2015). What we can learn from attacks on the WEP Protocol | Packt Hub. Retrieved from <https://hub.packtpub.com/what-we-can-learn-attacks-wep-protocol/>

Paulsen, C., & Toth, P. (2016). Small Business Information Security: The Fundamentals. doi: 10.6028/nist.ir.7621r1

Scot, W. (2016). The top 5 reasons to avoid unmanaged switches on your machines [Blog]. Retrieved from <https://blogs.cisco.com/manufacturing/the-top-5-reasons-to-avoid-unmanaged-switches-on-your-machines>

Simon, A. (2007). Poor Wi-Fi controls and security enabled TK Maxx data theft. Retrieved from <https://www.itpro.co.uk/112465/poor-wi-fi-controls-and-security-enabled-tk-maxx-data-theft>

Tom, S. (2017). 20 Linksys Router Models Vulnerable To Attack. Retrieved from <https://threatpost.com/20-linksys-router-models-vulnerable-to-attack/125085/>