Christopher Dix
Prof. Rywalt
CMP-124
9 December 2019

<u>Executive Summary:</u>

Although our client appears to have an above-average knowledge of modern technology, their current education on security is still rather basic. As a result of our investigation, we have identified several vulnerabilities relating to the confidentiality, integrity, and availability of the client's electronic assets and residence in general. Most of the key vulnerabilities can be fixed with simple reconfigurations, and some of our findings reflect a past neglect to maintain good security.

Our investigation consisted of two site visits and two interviews with the client. During the visits to the client's residence, we scanned the network for vulnerabilities, checked the configuration of all in-scope devices, analyzed the passwords which are currently in use, and surveyed the residence for potential physical security vulnerabilities. Interviews with the client were also carried out to gather additional information and to clarify certain findings from the site visits.

As a result of the investigation, we were able to identify many vulnerabilities that leave our client at risk. These vulnerabilities can be categorized into network/wireless security, system security, authorization/authentication, backups/disaster recovery, physical security, and user education. Each vulnerability is detailed in this report, along with information on how to mitigate each. The five most important vulnerabilities are also listed, so that the client can prioritize implementing a solution for those. Some examples of discovered issues include poor wireless network configuration, poor security configurations on smartphones, systems which are not regularly updated, relatively insecure passwords, a poor backup procedure, and poor physical security practices.

Although one may have to give up some convenience to do so, it is important to follow good security practices to ensure that assets are protected. Assets can come in the form of anything that has monetary or intrinsic value; and, just as one would experience monetary loss if a physical belonging was stolen, the theft of personal information could pose an even greater burden. Since most sensitive information is now stored electronically, it is crucial that steps are taken to ensure that this information is kept safe from unauthorized access. Good information protection procedures involve layering security, limiting access to those who absolutely require it, using different methods of security (more than just passwords), keeping information within a barrier and making it difficult for outsiders to access it, and by making security procedures which are simple for clients to follow yet complex for others to breach. Recommendations that employ each of these methods are given in this report as each vulnerability is discussed.

<u>"Top-Five" List:</u>

Given below is a list of what we believe to be the top-five weaknesses in our client's security. These issues are detailed in later sections of this report, and we urge that the mitigations for these vulnerabilities be implemented as soon as possible.

1. The physical security of the client's residence should be improved before anything else. Here are the top two vulnerabilities:
    a. Not all entrances into the residence have door locks.
    b. Keys are often left in the door or doors are left unlocked.
2. Authentication methods used to access online accounts should be improved. Most notably:
    a. Currently-implemented passwords are relatively insecure.
    b. In some instances, the same password is used for multiple services.
    c. Passwords are all stored within a web browser.
    d. Two-factor authentication is not implemented.
3. The wireless network settings on the client's router should be reconfigured, to mitigate vulnerabilities such as:
    a. Poor choice of SSIDs
    b. A relatively insecure wireless passphrase
    c. Lack of implementation of a guest network or guest device authorization policy
    d. Ports unnecessarily being forwarded or left open
4. Automatic updates are not configured on device operating systems or anti-virus software, thus resulting in them not having the latest patches.
5. Automatic and off-site backups are not implemented, and not all devices are backed up.

Introduction

The client consists of two adults which reside in a two-bedroom condo and have a variety of wired and wireless devices. The condo is in close proximity to other condo units. This security analysis report will be used to find potential vulnerabilities in the client's residence and provide recommendations to correct those problems.

Project Scope

The following activities are within the scope of this project:

- Interviews with clients who use the Internet
- A Visual walk-through of the residence, rooms and ask who has access to the client's home and their devices
- A series of Port Scans to discover known and potentially unknown devices on the network. (These Scans will be conducted from within the client's residence and from outside the perimeter.)
- A configuration and security assessment of at most five key systems at each center.

The following activities are NOT part of this security assessment:

- Penetration Testing of systems, networks, and building
- Social Engineering to acquire sensitive information from guests and clients
- Testing Disaster Recovery Plans

Client Overview *(supplied by client)*:

The client is myself and my roommate. We are a residential client and use a home network for wireless and wired connections for our devices. We use our devices/network for peer 2 peer sharing, gaming, and streaming. There are others that visit this household that have access to the wireless network and the devices that are connected to it. We have 2 wired connections a desktop PC and Xbox 360. We also have several wireless connections like a desktop PC, Laptop, two cell phones, and a tablet. Our computer knowledge varies; one of the clients has basic knowledge while the other has limited knowledge on security standards. We have had viruses in the past and use p2p sites often. We also have frequent guests that connect to the network.

Devices in Scope:

Device Type	Device ID	Operating System	User	Description
PC1	TC	Windows 8.1	TC	Custom Build, Gigabyte MotherBoard
PC2	JL	Windows 8.1	JL	Custom Build, Gigabyte MotherBoard
Laptop	TC-Laptop	Windows 10	TC	Dell Inspiron i7 7000 Series 7746
Smartphone	TC	Android 5.0.2 version Kernel 3.4.0 Software D80130c	TC	LGG2 T-Mobile
Wireless Router	WNDR3400	V1.0.0.52_20.0.60		NETGEAR N600 Wireless Dual Band

Network & Wireless Security:

Vulnerability	Description	Recommendation
WPA Security Still Implemented	WPA is an older wireless security standard that, when enabled, introduces extra vulnerabilities into a network. Every device currently in use on the client's network supports WPA2, a newer and more secure authentication protocol.	The security on all wireless networks should be changed to "WPA2-PSK [AES]" (thus disabling WPA) to ensure that only the most secure authentication protocol is being used. This change would be made in the router's configuration settings.
Inappropriate SSIDs on Wireless Networks	Wireless networks should have a name which accurately depicts the network's owner(s) and purpose. The client's wireless networks have names which do not depict either and may entice attackers to target their network.	The SSIDs of each wireless network should be renamed to better depict the owner and purpose (ex. "[ClientLastName]" and "[ClientLastName]-Guest". This change would be made in the router's configuration settings.
WiFi Passphrase Could Use Improvement	The client's wireless password is of a moderate complexity but can be easily compromised since it consists of easy-to-obtain information about the client.	The wireless passphrase should be changed to a more-secure alternative. This change would be made in the router's configuration settings.
Guest Wireless Networks are configured but not enabled	Guest wireless networks allow for complete separation between personal devices and devices of others who are visiting a residence. This way, infected or malicious devices which guests bring into the residence would be completely isolated from the home network.	The guest network should be enabled in the router's configuration settings. The guest network's SSID should change (to meet the guidelines outlined above) and the passphrase should be made more complex and different than that of the main network.
Port forwarding unnecessarily enabled	Port forwarding opens routes for attackers to get into a network. The client's network currently has two ports forwarded for a game which is not played anymore.	The two currently-setup port forwarding services should be disabled (or deleted). This change would be made in the router's configuration settings.
Certain ports unnecessarily left open	Open ports give attackers routes into a network. It was observed that the client's network has extra ports left unnecessarily open.	Ports should be closed when not in use (either by permanently closing them or by only opening them during certain hours of the day to certain devices). This change would be made in the router's configuration settings.
Wireless signal range unnecessarily large	The client's 2.4GHz wireless signal currently extends far beyond the area where it is used (ex. into nearby parking lots), thus allowing attackers to reach the network from outside of the client's residence. Additionally, every device	The client's 2.4GHz wireless network should be disabled, thus making the network only operate in the 5GHz band. This change would be made in the router's configuration settings.

	on the client’s network supports wireless operation on the 5GHz band.	
Peer-to-Peer Sharing May Introduce Vulnerabilities	When peer-to-peer sharing is used on a network, ports must be opened, thus making the network more susceptible to attacks. It also puts devices at risk, since malicious files can be downloaded.	Unless absolutely necessary, we recommend that the client stop using peer-to-peer software. If required, then we recommend that device antivirus software is used (and updated) and that the network’s firewall be reconfigured accordingly.

System (PC/Device) Security:

Vulnerability	Description	Recommendation
Guest mode improperly configured on smartphones	The guest mode on smartphones is designed to let anyone use the device for basic needs without leaving history of the session on the device. Guests should be unable to alter the smartphone's settings or configuration in any way. It was found that one of the client's smartphones is configured to grant guests full Internet access and the ability to install software that is not in the Google Play Store.	The guest mode on all smartphones should be reconfigured to only allow guests the most basic access to smartphone features. If the client does not use the guest mode at all, then it should be disabled entirely.
Smartphones do not lock at frequent intervals	To prevent unauthorized access to sensitive information or device configurations, smartphones should remain locked when not in use and automatically lock after a short period of inactivity. It was found that one of the client's smartphones stays unlocked for long periods of time.	The screen lock settings should be changed so that the smartphone automatically locks after a very short period of inactivity (we recommend roughly 30 seconds).
Multiple devices share the same password	An increased threat is posed to a group of devices when they all share one common password. If this password were to be compromised, an attacker would then have access to every device, as opposed to just one machine.	The client should change passwords on certain devices to ensure that every device has a secure and unique password.
Antimalware Software Not Kept Up-to-Date	Antimalware software relies on updates to accurately detect new forms of malware. Antimalware software on the client's devices is not regularly updated.	Frequent, automatic updates should be configured in the antimalware software. If automatic updates are not supported, then the client should set a schedule to routinely do a manual update of the antimalware software.
Some Device Operating Systems Not Kept Up-to-Date	As vulnerabilities in device operating systems are discovered and patched, the fixes are distributed via system updates. Numerous devices on the client's network are running an out-of-date version of the operating system.	Automatic updates should be configured on the client's devices to ensure that the operating system obtains the latest security patches.

Authorization & Authentication:

Vulnerability	**Description**	**Recommendation**
Two-factor authentication is not implemented	Two-factor authentication provides an extra layer of security in an online account. In addition to a password, an attacker would need access to another account or device in order to get into the protected account.	Two-factor authentication should be enabled on all important online accounts.
Passwords are all stored in Chrome on local devices	When passwords are saved in a web browser, the protection of all online accounts is dependent on the security of that browser. In this case, an attacker would just have to get into the browser or the browser's synchronization account (ex. A Google account for Chrome) in order to gain access to all passwords.	Any passwords currently saved in Chrome or locally on any device should be removed, and passwords should not be stored in a similar manner in the future.
Some of the passwords are used in multiple locations	Using the same password for multiple services makes both more vulnerable to being breached. If an attacker obtains the password and associated email address from one site, he can then use it to gain access to the other accounts sharing the common credentials.	Any password that is shared amongst multiple sites should be changed to passwords which are secure and unique to only one account.
Smartphone uses a pattern passcode, and the pattern is a "common," recognizable symbol	Using a pattern to lock a smartphone is insecure compared to other options because of the relatively low number of unique patterns available. When a pattern is used, an easily recognizable letter or shape (which the client currently uses as a smartphone lock) is less secure since attackers will guess these first.	The screen lock on each of the client's smartphones should be set to a unique, secure PIN. If a fingerprint sensor is on the device, it is recommended that fingerprint sign-in be set up in addition to the PIN.
Passwords are not frequently changed	All passwords should be reset on a regular basis in order to restrict the use of stolen passwords. As a password is in use, it may be exposed or cracked, and regularly changing password is the best way to prevent unauthorized access to an account.	The client should set up a routine to regularly review their passwords and change them to different unique, secure options.
Guest devices do not require authorization to use the network	Guest devices should be checked for malicious software before being allowed to connect to a network.	The client should implement a new policy to isolate guest devices onto a separate network and to only allow devices onto this network if there is an absolute necessity.
The guest password is the same as that for the main network	If the guest WLAN password is the same as the main WLAN password, then guests would be able to connect unauthorized devices onto the private network.	Before the guest network is enabled, its passphrase should be changed to a unique and secure alternative.

Complexity of the passwords used can be improved	It was observed that many of the client’s currently-implemented passwords are relatively insecure.	The client should review each of their current passwords and change them to a more secure alternative.

Backups & Disaster Recovery:

Vulnerability	Description	Recommendation
Automatic backups are not configured	Automatic backups ensure that the most-recent copy of user data is safe and do not require the user to remember to manually run a backup.	We recommend that the client consider purchasing and implementing a cloud storage service to keep important data safe and accessible. If this is not possible, then we recommend that an offsite backup (with a NAS device) be set up to automatically backup data from every computer.
Some devices have never been backed up	Backing up data is essential to ensuring it is not lost if a crash or other issue would prevent the system from successfully booting.	
There are no off-site backups	If something were to happen to the client’s residence, all important data would be lost unless an off-site backup was in-place.	
UPS devices are not implemented on any part of the network	Running computers and network equipment off of uninterrupted power supplies would help to prevent system crashes (and, thus, data loss) if utility power is suddenly lost.	We recommend that UPS systems be purchased and installed for PC1 and PC2.

Physical Security:

Vulnerability	**Description**	**Recommendation**
Not all entrances into the residence have locks	Without locks on doors, anyone can access the client's residence to steal belongings or gain physical access to electronic systems.	Locks should be installed on any door in the residence which currently lacks one.
Keys are often kept in the door, or doors are left unlocked	The security of a door lock is completely removed when it is left unlocked or when keys are kept in the door. Leaving keys in the locks also would also make it easy for anyone to steal the key and, thus, gain access to the residence whenever they want.	Doors should remain locked at all times, and keys should never be kept in the locks.

User Education:

Vulnerability	Description	Recommendation
The client has basic knowledge of security but would benefit from further training	Any of the proposed security improvements will be ineffective unless the client understands how to maintain these policies. Education is the key to maintaining good security, since it would allow the client to make informed decisions in the future. The client also has to maintain a schedule to regularly assess their security and make necessary changes (such as changing passwords).	We recommend that the client work with us as we implement the proposed security changes. This would help to educate them on good security practices.

Action Plan:

The chart below outlines each vulnerability along with further information as to the process of mitigating them.

Category	Vulnerability	Priority (1-5)	Cost	Professional Needed?
Network & Wireless Security	WPA Security Still Implemented	1	Free	Y
	Inappropriate SSIDs on Wireless Networks	5	Free	Y
	Wi-Fi Passphrase Could Use Improvement	4	Free	Y
	Guest Wireless Networks are Configured but Not Enabled	5	Free	Y
	Port Forwarding Unnecessarily Enabled	4	Free	Y
	Certain Ports Left Open Unnecessarily	4	Free	Y
	Wireless Signal Range Unnecessarily Large	3	Free	Y
	Peer-to-Peer Sharing Introduces Vulnerabilities Into Network	3	Free	Y *(if client needs to continue using P2P)*
System (PC/Device) Security	Guest Mode Improperly Configured On Smartphones	4	Free	Y
	Smartphones Do Not Lock at Frequent Intervals	4	Free	N
	Multiple Devices Share The Same Password	3	Free	N
	Antimalware Software Not Kept Up-to-Date	4	Free	N
	Some Device Operating Systems Not Kept Up-to-Date	3	Free	N
Authorization & Authentication	Two-Factor Authentication Is Not Enabled	4	Free	Y
	Passwords Are Stored in Chrome on Local Devices	5	Free	N
	Some of the Passwords are Used in Multiple Locations	3	Free	N
	Smartphone Uses a Pattern Passcode Which is a Common, Recognizable Symbol	4	Free	N
	Passwords Are Not Frequently Changed	3	Free	N
	Guest Devices Do Not Require Authorization to Use the Network	5	Free	Y
	The Guest Password is the Same as that for Main Network	5	Free	Y
	Complexity of Passwords Used Can Be Improved	4	Free	Y
Backups & Disaster Recovery	Automatic Backups are Not Configured	3	Free	Y
	Some Devices Have Never Been Backed Up	4	Free	N
	There are No Off-Site Backups	2	Low	Y
	UPS Devices are Not Implemented on Any Part of the Network	1	High	N

Physical Security	Not all entrances into the residence have door locks	5	Low	N
	Keys are often kept in the door, or doors are left unlocked	5	Low	N
User Education	The client would benefit from further training in good information security practices	5	Low	Y