UNIVERSITY OF CENTRAL FLORIDA

FRONTIERS IN INFORMATION TECHNOLOGY

COP 4910

CLASS FINAL REPORT

Abstract

This report brings together the final papers presented by the students in the Frontiers in Information Technology class, COP 4910 during the Summer-2015 semester. In addition, it is worth mentioning that this semester the students attended 56 talks and each student or team gave 4 presentations. In each talk they had to present the technical aspects of the selected topic along with its social impact, ethical aspects, and professional impact.

USB Rubber Ducky Analysis

Tyler Dever *(Author)*
COP 4910 – Frontiers in Information Technology
University of Central Florida

***Abstract*— The Universal Serial Bus (USB) is one of the most commonly used pieces of technology in today's world. But is it fundamentally secure? The USB Rubber Ducky takes advantage of the fact that computers trust human input. If computers trust human input, they also trust keyboards. Through the use of an easy to learn scripting language and open source platform, the USB Rubber Ducky demonstrates just how effective an attacker can be by plugging in a simple USB flash drive. With this knowledge, it is imperative that not just security professionals be aware of these risks. Individuals all around the world need to develop and implement security best practices in order to stay secure from these malicious cyber threats.**

I. INTRODUCTION

From keyboards and mice to gaming headsets and chargers, Universal Serial Bus (USB) technology has revolutionized the Plug-and-Play capability for computer systems and devices. Through utilization of standardized specifications, USB devices essentially speak the same language just with a different accent. By taking advantage of the concept of human interface devices (HID's) developed in the late 1990's, USB technology uses many of the same protocols no matter the purpose of the device being plugged in. In other words, there is an inherent trust between external input devices and the computer systems they are used on. The USB Rubber Ducky takes advantage of this concept. The small, USB flash drive is an open source security penetration testing platform that uses many of the same HID specifications in order to act as if it were a regular USB drive. If the device looks like keyboard, talks like a keyboard, then it must be a keyboard. Through scripting and automation, this innocent looking device quickly opens up a large number of attack vectors for the computer systems it is plugged into.

In the early 1990's there was a limited number of ways for humans to effectively communicate with computer systems. Although many external devices were being developed, keyboard and mouse served as the main source of input for humans to interact with computer technology. [1] Developing a standard at this point in time was not necessary since many of hardware manufacturers that developed input devices could take advantage of a limited pool of software drivers. As more diverse operating systems were developed and different hardware vendors began experimenting with newer human input methods, device manufacturers found themselves re-developing software drivers much more frequently. To allow for cross-platform support, each new input technology needed to be extensively tested with the latest software. In 1997 Mike Van Flandern and Manolito Adan conceptualized the idea of what a standard Human Interface Device (HID) specification would look like. This essentially would allow hardware to communicate in a specific way so that not as much time needed to be spent on software development and integration. That same year, Microsoft used this idea and implemented it into external input devices, more specifically, USB. [1] Jump ahead a few years and USB technology is now used as the primary form of communication between most external devices. But what can be said of USB's security? Developed in mid-2011, the USB Rubber Ducky was developed by Darren Kitchen as a way for the inherent trust between keyboards and computers to be exploited. As this paper will discuss, the ability to simulate a keyboard device though a small USB flash drive micro-computer is a very powerful technique for system exploitation.

The second section of this paper seeks to explain in detail the technical aspects of how the USB Rubber Ducky works. Hardware architecture and scripting language automation creates a device that is highly customizable and flexible for the environments it may be used in. In sections three and four, the social issues ethical issues currently surrounding this "hacking hardware" will be analyzed. Although security researchers make up a large portion of the user base for this device, no restrictions or policies are in place to limit good from bad use cases. Finally, in section five, the professional impact of hardware hacking will be discussed in order to outline and elaborate on the number of growing careers that exist in such a demanding industry. By the end of this paper, readers should be able to identify one of the major issues facing USB technology today as well as be aware of how USB Rubber Ducky and similar tools create a need for security best practices.

II. TECHNICAL ASPECTS

Even though the complexity of certain USB devices has increased over the past 10 years, it is important to understand there are standard building blocks that need to be satisfied first. For device communication to be successful with USB, special HID descriptors need to be agreed upon between the host system and the device. The host computer reads these descriptors to identify how the two entities will talk. For many devices, especially keyboards, the host can resort to using a "boot protocol" that host to use only the most basic of device features. This, for example, is why interacting with the keyboard at a system's BIOS works successfully. [2] Furthermore, with the establishment of Plug-and-Play (PnP) technology it is become much easier for generic device drivers to be loaded to interact with external devices such as keyboards and mice. This exemplifies how the HID infrastructure has been implemented and designed since its initial creation.

The USB Rubber Ducky is quite powerful for what it is intended to do. The device boasts an AT32UC3B1256 32-bit micro-controller with 256 KB of internal flash storage. For long-term storage, and perhaps one of the most important features, the USB has a 128 MB micro SD card to hold the desired script

payload. [3] When placing the USB drive into an open USB slot on a computer, the Rubber Ducky executes whichever script is loaded on the micro SD card. The execution time is very fast and the modular removable storage allows it to be upgraded in size as well.

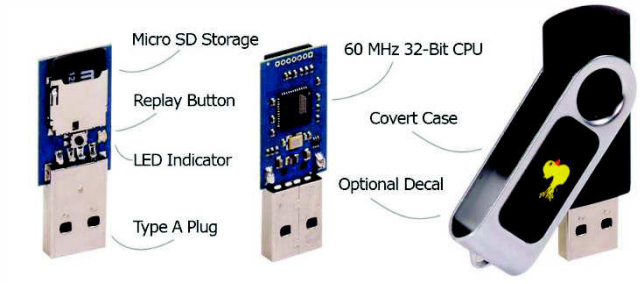

Figure 1: Rubber Ducky Architecture

Scripting plays an important role with the USB Rubber Ducky. It essentially defines what will run when the drive is plugged into a system. The commands used when developing Rubber Ducky scripts are very easy to learn and have high human readability. For example, if the attacker wants to press the Control, Alt, and Delete keys on the target system, they would simply type "CTRL SHIFT DEL" into the script. Figure 2, shows an example of a script developed for the Rubber Ducky.

Once the script has been developed in a text editor and saved with the ".txt" extension it needs to be run through the Duck Encoder. [4] This Java encoded compiler turns the plain-text commands into a language the Rubber Ducky can understand using the ".bin" file extension. Once the file has been created and placed on the micro SD card, the Rubber Ducky can be inserted into the target system for use. It is important to understand that because keyboards and mice are trusted and allowed on most all operating systems, cross-platform capabilities are possible. Essentially, different variations of a script that perform the same functions can be run on Linux, Windows, Mac, or even mobile devices. Figure 2 shows an example of a script developed for the Rubber Ducky.

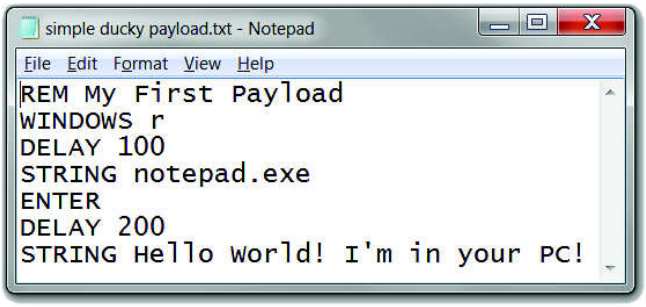

Figure 2: Simple Rubber Ducky Script

In terms of the different attack vectors, the list is quite extensive. It is important to note that once a malicious user has physical access to a computer system, the attack surface and possibility for exploitation increases two-fold. For instance, since the USB Rubber Ducky can type keyboard commands, it quite literally can write and compile scripts in real-time on a target machine without the user being notified. [5] What this means is that attacks such as DNS poisoning, anti-virus bypass, and reverse system shell creation are all possible with little effort on the attackers end.

III. Social Issues

Perhaps one of the biggest social issues with regards to information security and hardware exploitation is the term "hacker". This term generally draws a negative connotation against individuals who find vulnerabilities in the information security field. Instead of viewing hacking in a negative view, a new definition needs to be defined for "hackers". Yes, a good handful of individuals who engage in information security can be malicious but the term describes those who have taken the time to understand the device, software, or technology better than the actual creator or manufacturer of the product. Not all hackers should be viewed as malicious. Quite commonly "bug bounty" programs are held by large companies so that individuals can find vulnerabilities before they reach the headlines in the next large-scale data breach. For example, in the early months of 2015, United Airlines posted a bug bounty program for its public, web facing systems [10]. Independent security researchers around the world are encouraged to put their skills to the test in order to be rewarded. Not only do the researchers who rightfully disclose vulnerabilities benefit, but the systems hosted and managed by United Airlines become much more hardened and secure.

Another social issue in the world today that faces these USB devices and computer security in general is that many people just are not aware of current security best practices and procedures. At least 85% of organizations that are affected by security exploitation and infection have it arise from inexperienced users not being aware of the computer environment they are in. [9] The number one threat to any organization are the people that inhabit it. No amount of specially automated tools or security systems exist that can totally eliminate the risk that's associated with people working with computer systems. Educating users in an enterprise environment is mandatory in order to keep data secure. In fact, the USB Rubber Ducky is just one example of a device most users would have no problem plugging into their computer just to see what was on it. Ultimately, what led to the temporary ban of USB devices in the US military in 2008 stemmed from users not following standard policy with unknown external devices. Educating people around the world about computer security principles is the best way to foster an information aware society.

IV. Ethical Issues

In today's world, people can purchase just about whatever they want on the internet. It is no different with the USB Rubber Ducky. For just $45, anyone can purchase one of these devices and have it shipped to their address. The problem here being that people's intentions are unknown. Weather an individual plans on using it for security research or plans on using it to actively infect unsuspecting users systems, there is no way of telling. This is why many state laws and regulations have been placed on usage of these types of automated devices in the real world. [8] Unless someone has been given written or verbal permission to use one of these devices on a system, it is illegal to run exploits or payloads on intended target systems.

V. PROFESSIONAL IMPACT

Information security jobs are currently in high demand both within the United States and across the globe. Organizations spanning hundreds of countries are constantly facing advanced attacks that can cause millions of dollars in financial damages. From now until 2022, the expected growth for professionals within the information security field is expected to increase 37%. [6] This high number shows just how important defending organizations from cyber-attacks has become. Organizations such as the United States Department of Personnel Management and even Major League baseball are just some of the large organizations facing harmful attacks that have been in the news recently.

One of the most common positions in the information security field for professionals to achieve today is that of an Information Security Analyst. This type of work requires individuals to be well diverse in the operating systems and scripting languages that they know. Understanding key vulnerabilities in specific protocols and networking implementations is a heavy requirement as well. The median salary for individuals working in this area is about $86,170. [6]

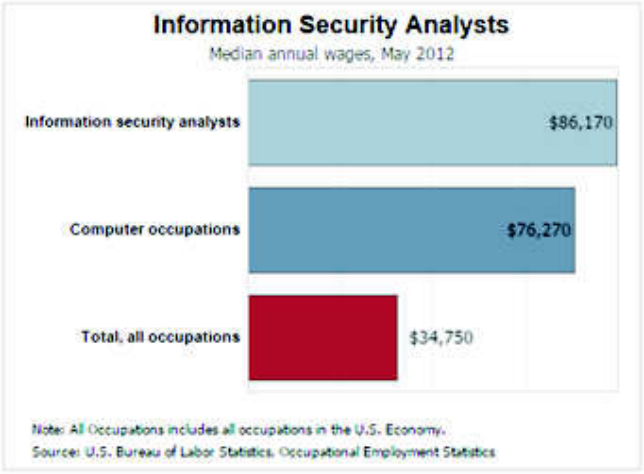

Figure 3: Information Security Analyst Salary

Information security is a very fast paced and ever changing field which means staying up to date on certifications and current exploitation techniques is a must. Having an understanding of how an attacker can break into a system is just as important as implementing defenses. On the other side of the spectrum, penetration testing takes a more offensive approach. In this field it would be more than likely that a USB Rubber Ducky would be actively used. Penetration testers audit and examine the defenses of an organization to find security holes or vulnerabilities in the infrastructure. The median salary for this type of position is about the same as that of an Information Security Analyst.

In terms of dealing with hardware, an Embedded Systems Engineer would focus more on the design and implementation of certain components within computer systems. Designing and testing firmware/BIOS configurations and working with different system architectures such as x86/x65 and ARM are just some of the duties associated with this line of work. This position pays well with the median salary being close to $100,000. [7] It is important to note that security plays an important role in hardware design as well as software.

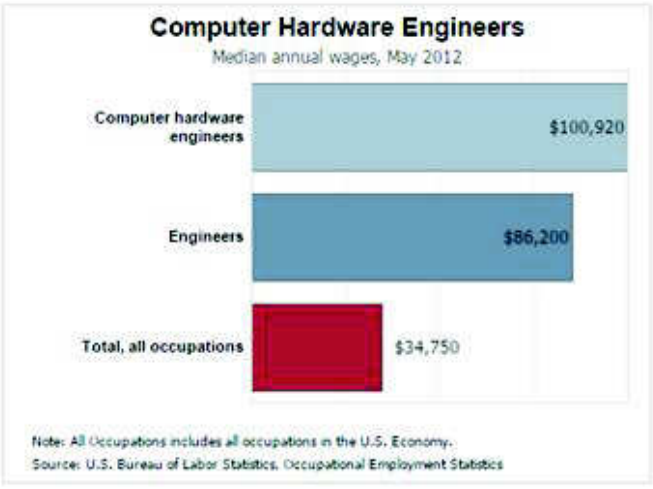

Figure 4: Hardware Engineer Salary Information

Weather it is defending systems or actively exploiting them, positions within the information security field are expanding each and every day. Educational degrees can play an important factor in how far a career path can lead, but it's the hands on experience that many employers are looking for. Having passion, dedication, and obsession creates security professionals that will be successful down the road. Actively pursuing side projects and industry certifications is a great way to land an entry-level position early in a career. Furthermore, there is no one person in the field that has extensive knowledge of every single topic. Having a general knowledge of specific topics and terminologies is important but specializing within a specific area is what many researchers and professionals find most rewarding.

Table 1: Common Security Careers

Position/Job Title	Median Salary	Background & Skills
Information Security Analyst	$86,170	• Windows and Linux mastery • Comon scripting language experience • Extensive networking protocol knowledge
Embedded Systems Engineer	$100,920	• Experience buiding and testing firmware • Understanding of x86 and x64 architectures • Ability to troubleshoot firmware and hardware
Vulnerability Researcher	$102,750	• Strong programming skills with low-level language • Familiarity with different hardware architectures • Ability to reverse engineer malware and binaries

VI. CONCLUSION

As technology has developed over the years, computer attack vectors have developed exponentially. Gaining physical access to a computer system now a days means that an attacker has access to just about anything on the system. The USB Rubber Ducky proves that exploitation is possible with literally the press of a button. Hardware hacking and exploitation is just

one aspect of information security that affects thousands of people each and every day. If the world is to become more effective in stopping cyber-crimes and exploitation, it is imperative that information security be taught just not to the ones interested in pursuing a career in the field, but to everyone that interacts with technology.

REFERENCES

[1] Arie, Benjamin, and Shereen Skola. WiseGeek. Conjecture, 2013. Web. 18 June 2015.<http://www.wisegeek.com/what-is-a-human- interface-device.htm>.

[2] "Functional Characteristics." Device Class Definition for Human Interface Devices (HID): Firmware Specification – Final 1/30/97. Version 1.0 / ed. Place of Publication Not Identified: USB Implementer's Forum, 1997. 7-11. Print.

[3] Midnitesnake. "The USB Rubber Ducky: Definitive Guide to the Quack Attack." Hak5 Community. 2013. 16 June 2015.

[4] Anderson, Brian. "USB Hacksaw." Seven Deadliest USB Attacks. Burlington, MA: Syngress, 2010. 1-5. Print.

[5] Anderson, Brian. "USB Switchblade." Seven Deadliest USB Attacks. Burlington, MA: Syngress, 2010. 27. Print.

[6] "Information Security Analysts." U.S. Bureau of Labor Statistics. U.S. Bureau of Labor Statistics, 8 Jan. 2014. Web. 18 June 2015. <http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm>.

[7] "Computer Hardware Engineers." U.S. Bureau oSf Labor Statistics. U.S. Bureau of Labor Statistics, 8 Jan. 2014. Web. 15 June 2015. hardware-engineers.htm#tab-5>.

[8] Rasch, Mark. "Legal Issues in Penetration Testing." SecurityCurrent.com. 26 Nov. 2013. Web. 18 June 2015. <http://www.securitycurrent.com/en/analysis/ac_analysis/legal-issues-in-penetration-testing>.

[9] "Secure USB Flash Drives." Sandisk. 2008. Enisa 17 June 2015 <http://www.sandisk.com/media/226716/enisa-whitepaper.pdf>.

[10] "United Airlines Bug Bounty Program." Bug Bounty Program. 2015. Web. 3 Aug. 2015. <http://www.united.com/web/en-US/content/Contact/bugbounty.aspx>.