

**Measuring the Effectiveness of the USB Flash Drive as a Vector for Social
Engineering Attacks on Commercial and Residential Computer Systems**

by

Jeffrey Robert Jacobs

A Graduate Capstone Project
Submitted to ERAU Worldwide
in Partial Fulfillment of the Requirements of the Degree of
Master of Science in Technical Management

Embry-Riddle Aeronautical University
Worldwide
Hawaii Campus
February 2011

Measuring the Effectiveness of the USB Flash Drive as a Vector for Social Engineering Attacks on Commercial and Residential Computer Systems

by

Jeffrey Robert Jacobs

This Graduate Capstone Project was prepared under the direction of the candidate's Project Review Committee Member, Dr. Bobby L. McMasters, Associate Professor, ERAU Worldwide, and the candidate's Capstone Review Committee Chair, Dr. Wayne Harsha, Associate Professor, ERAU Worldwide, and has been approved by the Capstone Review Committee. It was submitted to ERAU Worldwide in partial fulfillment of the requirements for the degree of Master of Science in Technical Management.

Project Review Committee:

.....
Bobby L. McMasters, Ed.D, P.E.
Committee Member

.....
Wayne Harsha, Ed.D.
Committee Chair

Acknowledgements

I would like to thank my Embry-Riddle committee members for their assistance. Both Dr. Wayne Harsha and Dr. Bobby McMasters were tireless advisors who never failed to offer timely feedback and sound advice. I would like to thank my colleague Derek Terawaki for his help in reviewing the experiment system code. Many of Derek's recommendations made it into the final system and helped ensure a reliable experiment. Finally, I want thank my wife Rosie for her patience and optimism. Her kind encouragement was a significant benefit to me and this project.

Abstract

Researcher: Jeffrey Robert Jacobs

Title: Measuring the Effectiveness of the USB Flash Drive as a Vector for Social Engineering Attacks on Commercial and Residential Computer Systems

Institution: Embry-Riddle Aeronautical University

Degree: Master of Science in Technical Management

Year: 2011

This research project evaluated how readily a cyber attacker could perform an effective social engineering attack using USB flash drives to introduce malware into commercial and residential computer systems. The results of this research add to earlier work in two important ways: First, by exposing the ongoing vulnerability of commercial computer systems to this type of cyber attack; and second, by demonstrating that residential computer systems are just as vulnerable to this threat as their commercial counterparts.

A key component of this research was a simulated cyber attack that found that 91.67% of the 60 USB flash drives dropped in residential and commercial areas were discovered and picked up within 8 hours. Further, the research revealed that within 72 hours, 36.67% of the flash drives dropped in residential and commercial areas had had their contents opened using an Internet-connected computer, a clear measure of success in this experiment.

Table of Contents

	Page
Project Review Committee	ii
Acknowledgements	iii
Abstract	iv
List of Tables	viii
List of Figures	ix
Chapter	
I Introduction	1
Background of the Problem	1
Researcher's Work Setting and Role	2
Statement of the Problem	3
Significance of the Problem	3
Limitations	3
List of Definitions	4
List of Acronyms	6
II Review of the Relevant Literature	7
Prevalence of Broadband Access	7
Internet Connectivity	8
Safeguards Against Internet Threats	9
Threats From Workstation-Initiated Internet Communications	10
Social Engineering	10
USB Flash Drives	11
Security Threats Posed By USB Flash Drives	12

	Social Engineering Attacks Using USB Flash Drives	13
	Summary	14
	Statement of the Research Questions	14
III	Research Methodology	16
	Research Design	16
	Research Model	16
	Survey Population	19
	Experiment System and Instrumentation	20
	USB flash drive survey devices	20
	Internet data collection device	22
	Survey device preparation tool	23
	Data collection device monitoring tools	24
	System pretest	24
	Distribution method	25
	Instrument reliability	25
	Instrument validity	26
	Treatment of the Data	27
IV	Results	29
	Primary Results	29
	Secondary Results	30
	Summary	34

V	Discussion	35
VI	Conclusions	37
VII	Recommendations	38
	References	39
	Appendices	
A	Bibliography	43
B	Experiment System Code and Scripts	45
C	Survey Device Data	58

List of Tables

Table		Page
1	Survey Device Effectiveness by Population	29
2	Effective Survey Device Activation Lag by Population	30
3	Survey Device Effectiveness by Gender of Survey Device Label	31
4	Effective Survey Device Activation Lag by Gender of Survey Device Label	31
5	Survey Device Effectiveness by Weekday	32
6	Effective Survey Device Activation Lag by Weekday	32
7	Survey Device Effectiveness by Time of Day	33
8	Effective Survey Device Activation Lag by Time of Day	33

List of Figures

Figure		Page
1	Typical USB Flash Drives	2
2	The USB Flash Drive Survey Devices	21
3	A Screenshot of the PixelFoot.com Homepage	23
4	Distribution of Activation Lag Measurements for Effective Survey Devices	30

Chapter I

Introduction

Never before has the world been so connected. Today, the Internet has revolutionized information access, the way people do business, and the way they spend their free time. It has established the infrastructure for completely new industries and now plays a significant role in the world economy. Looking back, people were given less than a generation to grow comfortable with the capability of computer systems to store their information securely. Now, the Internet's rapid adoption has challenged the basic notions of what it means to protect individual privacy and security in a digital world (Gromov, 1995).

Americans have come to depend on systems that leverage the power of the Internet. While enjoying the benefits of this connectivity, people also maintain a strong desire to keep their personal information private and secure. This security is continually challenged by Internet-based threats; therefore the diligent application of appropriate safeguards must be employed. Further, as new threats to this security arise, the policies and mechanisms used to protect this information must continue to evolve. For those who are tasked with developing and implementing these information security protections, it is vital to continually assess the significance of potential threats to information security (Gromov, 1995).

Background of the Problem

As adoption of the Internet has spread, experts have offered increasingly better security technologies. With technical vulnerabilities becoming harder to exploit, cyber attackers have increasingly taken advantage of the human element of the security equation (Mitnick, 2002, p. 4). One avenue of attack is the introduction of malicious code via removable computer media such as USB flash drives. USB flash drives have become ubiquitous today due to their usefulness, durability, and low cost. Figure 1 shows two examples. Over a quarter billion will be sold in 2010 (SanDisk 2010, 2010).

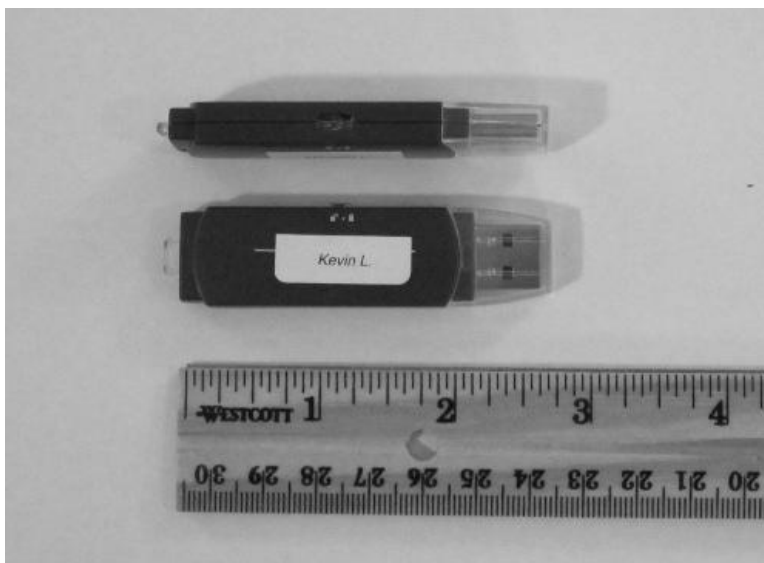


Figure 1. Typical USB flash drives.

Many of the qualities that make USB flash drives so beneficial also can be significant drawbacks when considering their threat to information security. The latest research shows that they are now a significant means of transmission, or vector, in the transmission of malware (Sirmer, 2010). Even more alarmingly, earlier research demonstrated that USB flash drives could be used as extremely effective vehicles for introducing Trojan software into a targeted commercial computer network. What makes this research particularly noteworthy is that the experiment relied on people finding "unknown" USB flash drives lying on the ground and plugging them into their office computers – an activity they proved to be very willing to do (Stasiukonis, 2006).

Researcher's Work Setting and Role

The researcher is a software engineer working in the domain of information assurance. His projects include work for US defense and intelligence agencies. He received a Bachelor of Science in Information Systems from the Sam M. Walton College of Business, University of Arkansas in 2001.

Statement of the Problem

A research experiment undertaken 4 years ago showed that USB flash drives could be used quite effectively in the nefarious introduction of malware (Stasiukonis, 2006). Since those findings were published, two things have happened that heighten the implications of this threat: The cost of USB flash drives has fallen, making them an attractive vector for cyber attack ("Amazon.com," n.d.); and the rate of residential broadband Internet adoption has increased to an all time high, rendering home computer systems potential targets ("Connecting America," 2010). However, one factor that might have mitigated this risk was an increased awareness of the threat posed by USB flash drives, and in particular, the danger associated with unknown drives.

The researcher believed a supplemental study; grounded on earlier research to determine whether individuals in commercial environments were still apt to facilitate the introduction of malware by inserting unknown USB flash drives into their computers was needed. Further, the researcher believed it was important to determine whether individuals in a residential environment were vulnerable to the same threat. The answers to these questions were found through the execution of this study.

Significance of the Problem

The findings of this research may be of interest to information security professionals and others who determine security policies. These professionals are primarily interested in the threat associated with commercial attacks. Additionally, the vulnerabilities exposed in a residential setting have clear implications for home users as well.

Limitations

This research relied on technical infrastructure including Internet access and a web server. The infrastructure was actively monitored during the experiment to safeguard against type II error, but a failure of these systems during the experiment might have led to irreclaimable survey instruments and other wasted experimental resources. Further,

survey instruments were unprotected when left outdoors and could have been damaged by natural environmental elements (e.g., rain). Thankfully neither of these scenarios occurred. However, one limitation still existed: The survey instrumentation operated differently than the instrumentation used in the previously referenced 2006 study. In this study, the instrument did not contain an automatically executing piece of software. Such an instrument would have been designed to automatically execute its software payload when it was plugged into a computer. While this would likely be an effective malware introduction strategy, the researcher found this technique particularly aggressive and not suitable for this study. The researcher instead designed and implemented a passive instrument which used a demonstratively harmless mechanism to signal the data collection device. This mechanism is discussed further in Chapter III.

List of Definitions

Broadband - an Internet connection that differs from dial-up in that it is usually "always on" and offers much higher communications speeds.

Cyber - an adjective used in this document to indicate either "Internet-based" or "Internet-borne."

Firewall - a communications gateway connecting two networks and capable of enforcing a security policy.

GB - Gigabyte. One billion bytes of data - equivalent to one billion characters of text.

HTML - HyperText Markup Language. The commonly used and human-readable document formatting language used on the Web.

IPv4 - IP version 4 - Internet Protocol version 4. The communications protocol in widespread use by today's Internet.

IPv6 - IP version 6 - Internet Protocol version 6. A new version of the Internet protocol supporting a significant increase in the number of addresses.

Malware - A kind of software that is designed to do malicious things.

MB - Megabyte. One million bytes of data - equivalent to one million characters of text.

NAT - Network Address Translator, or Network Address Translation. A device to, or the act of, actively modifying network packets to perform a translation between internal and external network addresses.

PHP – A programming language commonly used to develop web applications.

Social Engineering - The use of human deception rather than technical means to subvert security controls.

SQL - Structured Query Language. A language used to search and edit database information.

TCP/IP - Transmissions Control Protocol/Internet Protocol. The conventional name of the suite of protocols supporting Internet communications.

Trojan - Trojan Horse. A type of malware that uses a masquerade of authenticity or legitimacy to avoid detection.

USB - Universal Serial Bus. A common digital connector found on nearly all mainstream computers.

Vector - A method or instrument used in transmitting malware.

Virus - A type of malware. This term is typically used to describe malware that is encoded within the executable code of another program.

Worm - A type of malware. This term is typically used to describe malware that exhibits self-spreading behavior.

List of Acronyms

GB - Gigabyte

HTML - Hypertext Markup Language

IPv4 - IP version 4 - Internet Protocol version 4

IPv6 - IP version 6 - Internet Protocol version 6

MB - Megabyte

NAT - Network Address Translator

PHP – PHP: Hypertext Preprocessor

SQL - Structured Query Language

TCP/IP - Transmission Control Protocol/Internet Protocol

USB - Universal Serial Bus

Chapter II

Review of the Relevant Literature

In this chapter, the researcher reports background information necessary to understand the specific security threat being researched. The chapter begins with the latest figures outlining the adoption rates of broadband Internet connectivity for residential and business users. It then provides an overview of the technical underpinnings of Internet connectivity and the common safeguards employed to protect connected computers from cyber attack. The chapter then transitions from a purely technical focus to a more human-oriented one in discussing how social engineering can render the aforementioned safeguards ineffective. Narrowing the focus, USB flash drives are introduced and the threats posed by their use are described. Finally, the explained topics of USB flash drives, social engineering, and Internet security are combined to introduce the proposed research hypotheses.

Prevalence of Broadband Access

According to Aaron Smith of Pew Research (2010), the latest polls show that two thirds of Americans now have high-speed broadband Internet access at home. And with the signing of the American Reinvestment and Recovery Act in 2009, broadband Internet access for every American officially became a national priority (“Connecting America,” 2010). The billions allocated to this effort should provide many of the remaining third of Americans with home broadband Internet connections. According to the same plan, American businesses currently enjoy even higher rates of broadband Internet adoption; the vast majority (97%) use at least some of the basic features afforded by broadband access.

Although Americans do not enjoy the fastest broadband connections in the world, the average connection speed in 2010 was 4.6Mbps (Thompson, Gilmore, & Gideon, 2010). Or put another way, this connection speed would allow the contents of a CD-ROM to be downloaded in about 20 minutes.

Internet Connectivity

The Internet is composed largely of bidirectional communications carried via the TCP/IP protocol. TCP/IP has been around since the earliest incarnations of the Internet and while it has faced competition from other protocols in the past, it enjoys a prominent status as the underlying language of the Internet today. Communications are sent via TCP/IP for nearly all Internet transactions. It is convenient and mostly accurate to describe the conveyance of TCP/IP messages as coinciding one-to-one with each granular Internet transaction such as a web request or an email transmission (Kozierok, 2005).

According to Postel (1981), these TCP/IP connections are established using a procedure called a "three-way handshake." This procedure is normally initiated by one computer and responded to by another. User-initiated requests are largely responsible for the generation of TCP/IP connections. Therefore, from an Internet user's vantage point, TCP/IP connections are almost always initiated from their computer to a "server" on the Internet. This directionality of typical connection initiations has provided for and strongly influenced a practical solution of working around the Internet's scaling problems, which are discussed next.

With its reliance on TCP/IP, the Internet has and continues to struggle with scaling due to the limitations of the IP version 4, or IPv4, address space. This problem is caused by the use of a 32-bit address, which means there are only about 4 billion IPv4 addresses available. As the Internet has grown, it has become obvious that this finite number of addresses will become exhausted. This shortage is greatly aggravated by the fact that the IP address space was inefficiently allocated (3Com Corporation, 2001).

The long-term solution to the IPv4 addressing limitations can be found in the adoption of a new standard, IP version 6, or IPv6. However, this new standard requires a significant level of commitment due to the amount of software and hardware updates required and has yet to see wide deployment. The alternative and commonplace solution is one in which a private range of IP addresses is used on a local network and a Network

Address Translator, or NAT, is used to facilitate external Internet access (3Com Corporation, 2001).

Safeguards Against Internet Threats

In the Internet's infancy, it supported a small community of largely academic users who valued openness and sharing. Security was not viewed as a priority. It did not take long before the first malicious viruses and worms challenged this view in the late 1980s and early 1990s. It became clear that not everybody could be trusted, and when networks were connected together, a mechanism to enforce security boundaries had to be implemented. This mechanism is known as a firewall. Firewalls have existed since about 1987 and today they are so predominant that their use is implied with when Internet connectivity is established (Ingham & Forrest, 2002).

As previously discussed, because of the limited number of valid Internet IP Addresses, Network Address Translation has become so common that few people use the Internet without using NAT. By its very nature, NAT requires that Internet communications be initiated from local, or private network interfaces. This has the convenient side effect of eliminating Internet-initiated connections. In practical terms, it means that implementing NAT automatically creates a firewall between the internal network and the Internet ("How NAT Works," 2006).

Modern firewalls incorporate features such as dynamic inspection of network packets that can ensure Internet connections are initiated only from the internal network. When the firewall is also acting as the network address translator, it will often incorporate the NAT information in its processing engine. Stateful packet inspection and the use of NAT support the easily implemented, and what has become the standard, policy of blocking all inbound connections, and allowing outbound connections via known application protocols (e.g. HTTP) (Scarfone & Hoffman, 2009).

Firewalls and NAT devices can effectively block external Internet threats, but they offer little protection from internal ones. These threats might be insiders who would use

the Internet to knowingly or unknowingly disseminate protected information. Or more likely, these threats can be comprised of computers infected with malware or under the control of an external attacker (Scarfone & Hoffman, 2009).

Threats From Workstation-Initiated Internet Communications

The year 1999 was a turning point for malicious software. Although malware that automatically spreads via email was not new, 1999 was the first year that email-borne malware infected a sizeable percentage of the Internet. Furthermore, according to Schneier in *Secrets and Lies* (2000, p. 157), "This strain of malware ignores corporate defenses and tunnels right through firewalls. This is a really big deal."

Email propagation changed the game for individuals with malicious intent. It provided an avenue into users' computers by exploiting the rules allowing authorized services such as email. The year 1999 gave us the Microsoft Word virus "Melissa," and 2000 gave us the infamous "ILOVEYOU" worm. These two pieces of malware arrived via email and used the email functionality nested within users' software to replicate across the Internet (Schneier, 2000, p. 158).

When people use programs written by others, they are exposed to a certain degree of risk. They trust that that programmers are not malicious and that programs are doing what they are supposed to do and nothing else. While this is a fairly safe assumption when dealing with traditional "shrink wrapped" software, many elements of popular Internet use leverage mobile code – elements of which having almost untraceable origins. The most obvious examples include the many popular web browser plug-ins. But even software like utility programs and printer drivers can be considered risky. Networks, and especially the Internet, provide obvious benefits, but make malicious code even more dangerous due to the increased danger associated with information release (Schneier, 2000, p. 164).

Social Engineering

Companies and individuals may possess the best security technologies available but

still be vulnerable to attack. Why? Because people are often a security system's weakest link. Many information technology experts believe they have made their company safe by deploying security products such as firewalls and intrusion detection systems. However, individuals who think that security products alone offer true security are settling for an illusion of security (Mitnick, 2002, pp. 3-4). Indeed, Mitnick provides many examples in "The Art of Deception" of security being thwarted not by technical means, but by preying on the natural inclinations of targeted users.

An attacker does not have to play a personal role in these types of attacks. Many modern viruses and worms have demonstrated automatic social engineering as part of their life cycle. For instance, the "ILOVEYOU" worm would show up in a person's email inbox disguised as a legitimate email from a person the recipient knew. It had a realistic subject line and a convincing request for the recipient to review the attachment. The worm disguised its attachment as a harmless text file when the attachment was actually the executable content necessary to infect the computer and further spread the worm (Schneier, 2000, p. 268).

As specialists design better security technologies, with less technical vulnerability, attackers will increasingly exploit the human element of the security equation. For these attackers, breaking through this "human firewall" requires minimal investment or risk (Mitnick, 2002, p. 4).

USB Flash Drives

According to Mark Casey of About.com (n.d.), even in this age of networked computers, people have a need for a portable data storage device to easily transfer and store data. He goes on to report that transferring files from one computer to another can often be more trouble than it would seem. With IBM's introduction of the USB flash drive to the commercial market in 2000, people gained a convenient method of transferring files. IBM's original model had a capacity of 8 megabytes, which at the time was best equated to the storage capacity of about six floppy disks ("8 MB USB Memory

Key,” 2005). Today, 10 years later, USB flash drives are available in capacities reaching 256 gigabytes, 32,000 times the capacity of the original IBM model (Kingston Technology Company, 2010). USB flash drives can be used on all mainstream computers and operating systems (Kingston Technology Company, 2010), and are relatively inexpensive, with 8 gigabyte models available for less than \$10 at the time of this writing (“Amazon.com,” n.d.). Demand for these drives has increased every year since their introduction, and over 250 million USB flash drives will be sold globally in 2010 (SanDisk 2010, 2010).

Security Threats Posed By USB Flash Drives

The security-conscious U S. Department of Defense suffered its most serious publicized breach of network security in history after a foreign spy agency used a USB flash drive to introduce a worm into defense networks in 2008. According to Deputy Defense Secretary William J. Lynn, malicious code from the flash drive spread undetected through classified and unclassified Pentagon networks, ”establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control” (Jelinek, 2010, p. 1).

In November 2008, following the significant Pentagon network breach, the Department of Defense completely banned the use of USB flash drives on government computers. When asked about the ban in 2009, Admiral Mike Mullen, chairman of the Joint Chiefs of Staff, said he had no intention of reversing the prohibition of USB flash drives (Schogol, 2009). However, by early 2010, the drives’ usefulness allowed them be deemed worth the risk. The military’s restrictions were eased to allow limited use of the devices (Jelinek, 2010).

Americans are not the only ones who have experienced troubles with USB flash drives. In May 2010, IBM Australia embarrassed itself at a Queensland security conference by handing out complimentary USB flash drives inadvertently infected with not one, but two pieces of malware (Cluley, 2010).

These USB flash drives security mishaps are not rare, isolated incidents. According to security researcher Jan Sirmer of Avast Software (2010), during a one-week period in October 2010, malware attacks originating from USB flash drives represented 13.5% of all attacks reported by their collection network.

Social Engineering Attacks Using USB Flash Drives

A notable 2006 study revealed the surprising propensity of individuals to pick up and connect an unknown USB flash drive to their computers. The study, conducted by Steve Stasiukonis and his colleagues, was part of a network security assessment his company was hired to perform. The subject of the assessment was a credit union. As part of their research, Mr. Stasiukonis dropped 20 USB flash drives in the credit union's parking lot before the employees arrived to work. The drives were loaded with a custom-developed Trojan software that when activated would capture sensitive information and email it to the security assessment team. Of the 20 flash drives dropped in the parking lot, 15 were found and picked up. Of the drives picked up, all 15 were connected to bank computer systems. This was measured by the successful activation of the Trojan software and collection of sensitive information by the security team (Stasiukonis, 2006).

The United States Computer Emergency Readiness Team, US-CERT, advises individuals to "not plug an unknown USB drive into your computer" (McDowell, 2008, p. 1). But for those who would elect to do so, even cautious individuals may be fooled into facilitating the execution of flash-drive-borne malware. There are several proven techniques by which malware might disguise itself or bypass "autorun" restrictions. The "Conficker" worm exploited a Windows vulnerability by passively modifying the "AutoPlay" window such that the icon and label to open Windows Explorer to view the files on the drive actually activated the worm's executable code (Zdrnja, 2009). U3, a mainstream technology that allows individuals to keep a portable set of applications stored on their flash drive, actually fools the Operating System into running its launcher application by pretending to be a different kind of USB device. This capability can be

exploited with malicious intent (Johansson, 2008).

Summary

America's adoption of the Internet is widespread and growing. Two thirds of Americans now have high-speed Internet in their homes and an even greater percentage of them in their businesses. Owing to the culture of the Internet's heritage and the technical aspects of its communications, security mechanisms designed to protect information security have largely focused on blocking inbound Internet connections, exerting little control over outbound connections. As the traditional security mechanisms have gotten better, cyber attackers have increasingly turned to human deception, or social engineering, to achieve their aims. One such aim is exploiting the weak outbound security of traditional Internet security mechanisms by planting malware that leaks information or opens a back door from an internal system out to one on the Internet. An earlier study showed that USB flash drives could be used effectively as a social engineering vector to introduce such malware into a commercial computer system.

Statement of the Research Questions

By exploiting two vulnerabilities commonly found in today's computing environments, a cyber attacker may establish a high-speed, bi-directional communication back door to a computer through the Internet. The first of these weaknesses is a networked environment in which outbound Internet connections are either completely unrestricted or restricted in ways that do little to control the release of information. The second of these weaknesses is the relative ease by which human deception, or social engineering, may be employed by an attacker. Such deception allows an attacker to capitalize on the system access granted to an authorized person and completely bypass otherwise effective security mechanisms. The goal of such an effort in this case would be the execution of a back door software program on an internal system. USB flash drives were shown by Stasiukonis to be a very effective social-engineering vector for introducing malicious software into a targeted network.

Although Stasiukonis' study revealed 4 years ago that commercial computer systems were vulnerable to the social-engineering threat constituted by USB flash drives, the researcher believed that a new study would reveal a continued lack of awareness regarding this threat. Therefore, two research questions were posited for this study.

Research Question One: Do USB flash drives remain an effective social-engineering vector for cyber attacks targeting commercial computer systems?

Further, the researcher believed that high adoption rates of high-speed "always on" Internet have likely made home users vulnerable to the same threat:

Research Question Two: Are USB flash drives an effective social-engineering vector for cyber attacks targeting residential computer systems?

Chapter III

Research Methodology

Research Design

The researcher conducted an experiment to determine whether USB flash drives constitute an effective means for the introduction of malware into residential and commercial computer systems. This experiment was modeled after the aforementioned 2006 study and is described fully in the following sections of this chapter.

The quantitative results of this experiment were collected by the experiment system and its instrumentation. This system, described in-depth below, included USB flash drive survey devices and an Internet-based data collection mechanism. The gathered results have been used to answer the following questions:

Research Question One: Do USB flash drives remain an effective social-engineering vector for cyber attacks targeting commercial computer systems?

Research Question Two: Are USB flash drives an effective social-engineering vector for cyber attacks targeting residential computer systems?

Research Model

At the core of this research project was an experimental model designed to simulate the following scenario, in a safe and ethical way: Suppose that a skilled cyber criminal is motivated to commit espionage, identity theft, blackmail, or perhaps more simply, the destruction of computer records. It is a relatively straightforward task for such an individual to design software to facilitate this dirty work. However, introducing this software into a targeted computer system is a much more difficult proposition. The obvious vector, the target's Internet connection, is fortified against such types of attack. However, the attacker might leverage a bit of social engineering to accomplish his aim. The following steps outline a successful attack scenario:

1. The attacker prepares a USB flash drive by loading it with malicious software.

2. The attacker places the flash drive in a public, outdoor place where it's likely to be found by a targeted passerby.
3. A passerby sees the flash drive and is deceived into believing that he or she has discovered a misplaced USB flash drive.
4. The drive's discoverer picks up the device and takes it with them.
5. The discoverer connects the flash drive to their computer and unwittingly launches the malicious software.
6. The malicious software opens a back door for the attacker to use, or otherwise carries out the attacker's scripted plan.

While this method of attack would be perpetrated by a technology-savvy criminal, its success hinges on the non-technical involvement of the USB flash drive's unwitting discoverer. It was the aim of this research to measure and characterize the effectiveness of USB flash drives when employed as a social engineering vector. Thus, the research experiment modeled the necessary elements of this type of cyber attack to measure the following:

1. The percentage of discovered drives - the staged USB flash drives which have been discovered and picked up by a passerby, and of these:
2. The percentage of effective drives - the drives which have been discovered by an individual who subsequently opens one or more of the files contained on the drive, which simulates the execution of malicious software by triggering a detectable request from the Internet data collection device.

Of these measurements, only the percentage of effective drives was directly consequential in evaluating the research questions. However, the measurement of discovered drives is interesting and was valuable in supporting the experimental findings.

Briefly, the experimental procedure consisted of the following: First, the researcher prepared and distributed a number of USB flash drives (survey devices) as described below. Each of these flash drive survey devices contained a unique set of HTML files,

with each file containing an HTML image reference tag. This tag referenced a valid Internet address, such as <http://pixelfoot.com/mstm/getimage?id=3&key=abcd1234>. When the HTML file was loaded, the computer's web browser automatically requested each image specified within an image tag. In this experiment, each HTML image tag contained a unique identifier, and this identifier was passed along when the web browser made the Internet request. The Internet address referenced by the HTML image tag was the address of the Internet data collection device (detailed below), which responded appropriately to each image request and also noted the event by storing the relevant details in a database. In this way, the researcher used the Internet data collection device and the instrument monitoring tools (detailed below) to gather relevant data on requests originating from the survey devices. Following the predetermined measurement window, the researcher processed the gathered data in accordance with the Treatment of Data and Procedures section.

In designing the experiment, the researcher took special care in addressing the ethical concerns that might be raised due to the nature of the research. It was the researcher's primary goal to ensure that the experiment posed no risk to the surveyed population. Therefore, the experiment was carefully designed to eliminate this risk by meeting the following requirements:

1. The experiment could not spread malware, intentionally or otherwise. The researcher therefore:
 - a. Carefully prepared the USB flash drive survey devices by performing the following actions: Used a freshly-installed, trustworthy operating system (Ubuntu Linux) when configuring the USB flash drive survey devices; freshly formatted each USB flash drive survey device prior to use; and populated the survey devices using only plain HTML files produced by the researcher.

- b. Ensured the Internet data collection device did not host malware by performing the following actions: Used a website and domain solely dedicated to this experiment and containing no extraneous content; used strong passwords to protect the device code and database; and used code written by the researcher and reviewed by another programmer.
2. The research could not identify potential or measured at-risk targets by name. The researcher therefore: Did not record or report specific residential or commercial places of interest (e.g. specific businesses or offices); and did not collect IP addresses or other identifying information via the Internet data collection device or by any other means.
3. The experiment avoided panicking individuals who might be worried they were being targeted for cyber-attack. The researcher therefore: Used only human-readable HTML files (no scripts or binary content) on the USB flash drive survey devices; did not leverage any USB flash drive auto-run technology; and disguised the Internet data collection device as a legitimate, but possibly defunct, image hosting website.
4. In general, the researcher sought to minimize any negative impact on the surveyed population. The researcher therefore: Used a number of sample devices not significantly larger than necessary; and gathered undiscovered survey instruments after a predetermined time period in order to avoid littering.

Survey Population

Sixty (60) survey devices were separated into two groups of 30, with each group of devices surveying a designated subpopulation of Maui, Hawaii. These two subpopulations consisted of the individuals within either the residentially or commercially-zoned areas of Maui. The physical boundaries of each zone, as defined geographically by the Maui County Planning Commission, were used in differentiating the two subpopulations. The

combined subpopulations represent the vast majority of targets that a cyber-attacker would likely be interested in; therefore, the experimental data collected for each have been combined to produce meaningful results for the population of Maui as a whole.

For each of the two surveyed subpopulations, a sample size of 30 allowed the researcher to claim with slightly greater than 95% certainty that an effective survey device would be detected by the data collection device if the survey devices were 10% effective. This contrasts with the less than 5% chance that no device would have been effective given an equivalent sample size and effectiveness level [i.e., $(1-.10)^{30} = \sim .042$].

By combining the subpopulations, the larger sample size of 60 allowed a more certain claim (greater than 99%) that an effective survey device would have been detected if the devices were 10% effective. If the devices were 5% effective, the larger sample size allowed about a 95% certainty of detecting an effective device.

Experiment System and Instrumentation

Much of the experiment's design was captured in the engineering of the experiment system. Both the functional aspects of the experiment as well as the instrumentation necessary to measure and collect the desired data is embodied in this design. The system is best understood as the following collection of components:

USB flash drive survey devices. These 60 devices were typical USB flash drives (see Figure 1), all the same brand and model (Memorex brand 128 MB). They were not identical however; they were variously blue, gray, or white. Each device had a printed label bearing a person's name.

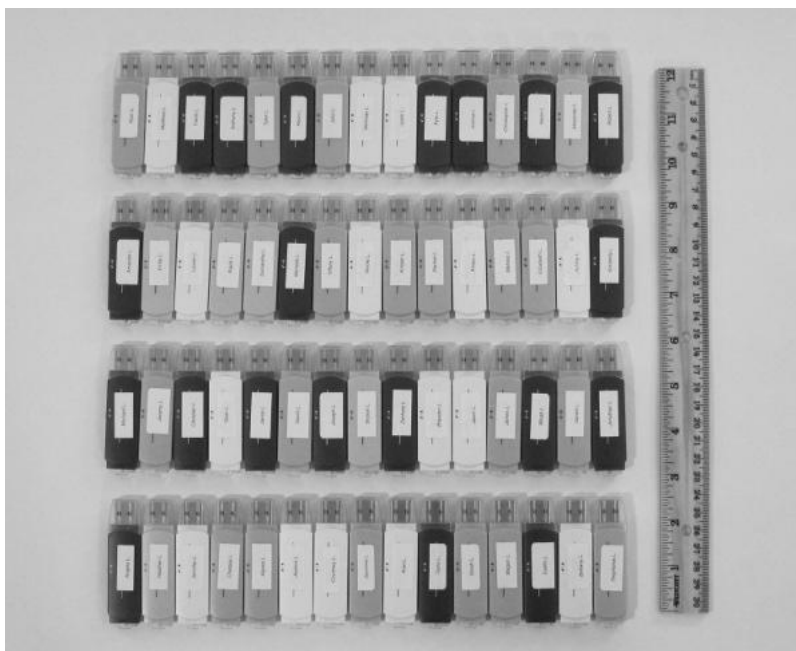


Figure 2. The USB flash drive survey devices.

The printed name labels were not just for show. They allowed the devices to be easily identified prior to and during the experiment. The printed labels included a unique first name and last initial. Half the devices had male names and the other half had female names. The names selected were those from an official list of most common baby names in Hawaii in the year 1990. Before the list of names was used, gender neutral names were removed.

Each device carried a payload of five uniquely generated HTML files. These files had the following names: gallery.html, resume.html, budget.html, bookmarks.html, and slideshow.html. Each of these files contained simple, but realistic, content. This content was similar to what one would expect to be produced as part of a web page creation assignment in an introductory computer course. For realism, each file contained within it the same name as printed on the device's printed label (e.g. "Resume of Michael Lee" was contained within the resume.html file on the device labeled "Michael L.").

Perhaps most significantly, each HTML file contained an HTML image or background image tag that referenced the Internet data collection device. This tag also

included a unique identifier and security code. When this HTML file was opened using a web browser (the application usually configured to load HTML files), the image request made to the Internet data collection device uniquely identified which file and survey device the request originated from.

Internet data collection device. The researcher developed the Internet data collection device as a web application running on the Internet domain `pixelfoot.com`. This domain and application were dedicated solely to this research experiment. The application was written in PHP and leveraged a MySQL database. The Internet data collection device served image files when they were requested using a valid identifier and security code. The device was able to validate each request by checking the identifier and security code using the values stored in the database. When a valid request was made, three pieces of information were recorded in the database:

1. The originating survey device's unique identifier
2. The originating HTML file (e.g. "resume")
3. The date and time

Because the Internet data collection device was publicly accessible (as was required to perform its duty), it was subject to scrutiny. To give it an authentic appearance, the researcher disguised the website with a small "Web 2.0" logo (see Figure 2) and a status message evocative of a semi-defunct image hosting service. This was done to minimize the risk associated with an overzealous and curiosity-driven individual by giving credibility to the notion that `pixelfoot.com` had once been a going concern. This topic is addressed further in the System Reliability and System Validity sections.



Figure 3. A screenshot of the PixelFoot.com homepage.

Survey device preparation tool. The 60 USB flash drive survey devices each stored five unique HTML files. It would have been tedious and error prone to generate all 300 of these files manually. The survey device preparation tool automated this process by generating the file sets for all the survey devices in one step. This tool executed in the same web server environment where the Internet data collection device was housed. During the execution of the preparation tool, it read the security device identifier, security code, and label name for each device from the Internet data collection device's MySQL database. The tool then generated and wrote each device's file set to a named directory on the web server. These names corresponded to the devices' printed labels. The researcher then used the "rsync" program to transfer these file sets from the web server to his workstation where he individually prepared each survey device.

Data collection device monitoring tools. The researcher developed a simple tool that allowed the real-time viewing of experiment results. This tool resided on the web server alongside the Internet data collection device and performed a query of the MySQL database each time the tool was executed. Using this tool, the researcher monitored the collection of data remotely. Another monitoring tool was developed and run in a background process on the researcher's workstation. This monitoring tool simulated the action of a valid survey device in making requests to the Internet data collection device. These queries were executed every 3 minutes for the entire duration of the experiment.

System pretest. Several tests were made to ensure the experiment system worked as designed:

First, the survey device preparation tool was tested by scrutinizing its output. A sampling of the generated file sets revealed that the script was working correctly.

Second, the Internet data collection device was evaluated. The device's interface was checked using manually specified inputs entered through a web browser. This testing revealed that the program was working correctly. It both recorded the transaction to the database correctly and generated the image file as designed.

Third, one of the file sets was copied to a USB flash drive to check that the entire system worked as designed. The researcher left the device at an assistant's desk. The assistant connected the flash drive, opened each of the files, and returned the drive to the researcher. The anticipated entries resulting from the assistant's opening of the files were found in the database. This revealed that the experiment system worked as designed.

Finally, to ensure broad compatibility, the USB flash drive survey devices were tested on several operating systems. These included: Windows Vista, Mac OS X, and Ubuntu Linux. Several common web browsers were tested, including Internet Explorer, Safari, Firefox, and Opera. There were no incompatibilities found.

Prior to the initiation of the experiment, the random security codes were updated in the database and the survey device files sets were generated. After the survey devices had been prepared, several of the devices were selected at random. These devices were tested by opening each HTML file on each drive. The Internet data collection device's database was checked to ensure that the appropriate data was captured. When this test was found to be successful, the database's response table was be cleared of all data and the research experiment commenced.

Distribution method. The 60 USB flash drive survey devices were distributed by the researcher over a period of 3 days, from January 25 through January 27, 2011. These dates coincided with typical workdays: Tuesday, Wednesday, and Thursday. On each day, 20 survey devices were distributed. The devices were evenly distributed between the surveyed subpopulations, with 10 devices targeting commercial areas and 10 devices targeting residential areas. Each survey device was placed on the ground in a public sidewalk or parking area where a passerby was likely to find it. The researcher placed each survey device inconspicuously to avoid drawing extra attention to the device. The location and time were recorded so the device could be retrieved at a later time if it had not been discovered and collected by a passerby.

Instrument reliability. Much care was put into the design of the experiment system. By opting for simple and proven technology such as the PHP scripting language and HTML, a great deal of technical risk has been avoided. A reliable Internet hosting provider (Dreamhost.com) was selected for web serving needs. The domain name of the Internet data collection device, pixelfoot.com, had an active registration throughout the experiment timeframe. Strong passwords were used for all server and database accounts. And the data collection device code was peer-reviewed in an effort to eliminate bugs.

The Internet data collection device relied on having a dependable Internet connection. An Internet or web hosting failure during the experiment could have gravely damaged the experiment. An important component of the experiment system was a

monitoring tool that continuously tested the health of the Internet data collection device by verifying its correct functioning every 3 minutes. While this monitoring tool could not make the system more functionally reliable, in the event of an Internet data collection device failure, the monitoring tool's logged output could have been used to determine the magnitude of the failure as measured by the length of time the data collection device was out of service. The monitoring tool did however, make the system more instrumentally reliable. It helped guard against the type II error of falsely regarding the absence of collected data as an indication of no effective flash drive survey devices.

Instrument validity. The experiment system was designed with the understanding that many of its components would be exposed to the Internet. Being an Internet-exposed service, security was taken very seriously. Standard web application development practices were used, such as treating data input with care by sanitizing and escaping the content appropriately before it was stored in the database. The Internet data collection code was reviewed by another programmer in an effort to eliminate bugs.

Requests to the Internet data collection device were validated with a unique identifier and a randomly generated security code. Each identifier/code pair was specific to a particular HTML file. Because there were five HTML files on each of the 60 survey devices, there were 300 valid identifier/code pairs. Each security code was 100 characters in length, with each character being one of 36 values. A code of this length offers $\sim 4.26 \times 10^{155}$ possible security codes, a number sufficiently large for ensuring the security codes were un-guessable. Adopting the necessary security practices to ensure a secure Internet presence for the experiment system significantly aided in ensuring the validity of the experiment system. Properly ensuring that only valid requests were recorded as such allowed the researcher to ensure that the possibility for false a false positive to be inserted was eliminated, thus guarding against type I error.

Treatment of the Data

The researcher used the following timelines in running the experiment and interpreting the results:

1. Ten (10) survey devices were placed per subpopulation per day, totaling 20 devices per day.
2. At the time a survey device was placed, its label, location and the time of the placement was noted. The time was accurate to the nearest second using a coordinated timepiece.
3. Each survey device was collected approximately 8 hours after it was placed, if it had not already been discovered and picked up. Survey devices that were collected in this manner were not reused during the experiment.
4. The Internet data collection device was started before the first survey device was placed and operated continuously for 3 days (72 hours) after the last survey device was placed. For each survey device, a measurement window of 3 days (72 hours) was used, starting at the moment it is placed. Data generated from survey devices recorded after this window were stored in the database, but excluded from reporting.

Any data captured for a surveyed sub-population was evidence of device effectiveness. A single device's activation was all that was required to demonstrate the presence of the vulnerability within that sub-population.

When a number of survey devices were found to be effective, the researcher could derive even more information. When that occurred, the researcher used a combination of tools to process the data. The data existed in its raw state within the relational database used by the Internet data capture device. SQL queries could be used in this environment. The researcher used these queries to process the data as well as export the data so it could be used in OpenOffice Spreadsheet and Microsoft Excel.

The Internet data collection device was designed to capture details for every request, even duplicate ones. When a survey device was effective, the discoverer of the drive often opened more than one of the HTML files, and there was a corresponding number of data points stored in the data collection database. The earliest recorded response for each survey device was used to calculate that device's "response lag."

If it was found that device effectiveness rates for each sub-population approached 50% and the responses appeared to form a normal distribution, descriptive statistics of the response lag (distribution, central tendency, dispersion) could have been reported. Because of careful experimental control, the statistical values derived for the two sub-populations could be compared and contrasted. Additionally, if the device effectiveness rates had allowed, effect sizes comparing the sub-populations for the recorded independent and dependent variables could be calculated. These calculations included the following independent variables:

1. Number of survey devices placed
2. Sub-population targeted
3. Time of day
4. Day of week
5. Gender of the name on the survey device's label

And the following dependent variables:

1. Effectiveness
2. Response lag (time between drop and to the first response)
3. Number of responses

It should be noted that the sample sizes and measured effectiveness rates measured during the experiment did not allow the application of some of these statistical tools without caveat.

Chapter IV

Results

Primary Results

A key aim of this research involved simulating and measuring the effectiveness of USB flash drives as a malware vector in the Commercial and Residential populations of Maui, Hawaii. Data relevant to this aspect of the research are summarized in Table 1 and are detailed in Appendix C. Figure 1 identifies the distribution of measured times for each survey device's first activation, also referred to as its lag.

Table 1
Survey Device Effectiveness by Population

Survey Devices	Commercial	Residential	Combined
Dropped by researcher	30	30	60
Recovered by researcher (after 8 hours)	1	4	5
Found and picked up by unidentified party	29	26	55
Effective (activated by unidentified party)	11	11	22
Effective Rate (percentage of found)	37.93%	42.31%	40.00%
Effective Rate (percentage of dropped)	36.67%	36.67%	36.67%

The length of time between a survey device's drop and its first activation was calculated and defined as its lag. Only effective survey devices have associated lag measurements. These values are detailed in Appendix C. The mean and median lags are grouped by population in Table 2.

Table 2

Effective Survey Device Activation Lag by Population

Effective Survey Devices	Commercial	Residential	Combined
Mean Lag (hours)	7.30	14.10	10.70
Median Lag (hours)	2.69	4.33	3.33

The distribution of survey device lags is shown in Figure 4. In this figure, the lags for both populations are combined and the results are grouped into 4-hour intervals.

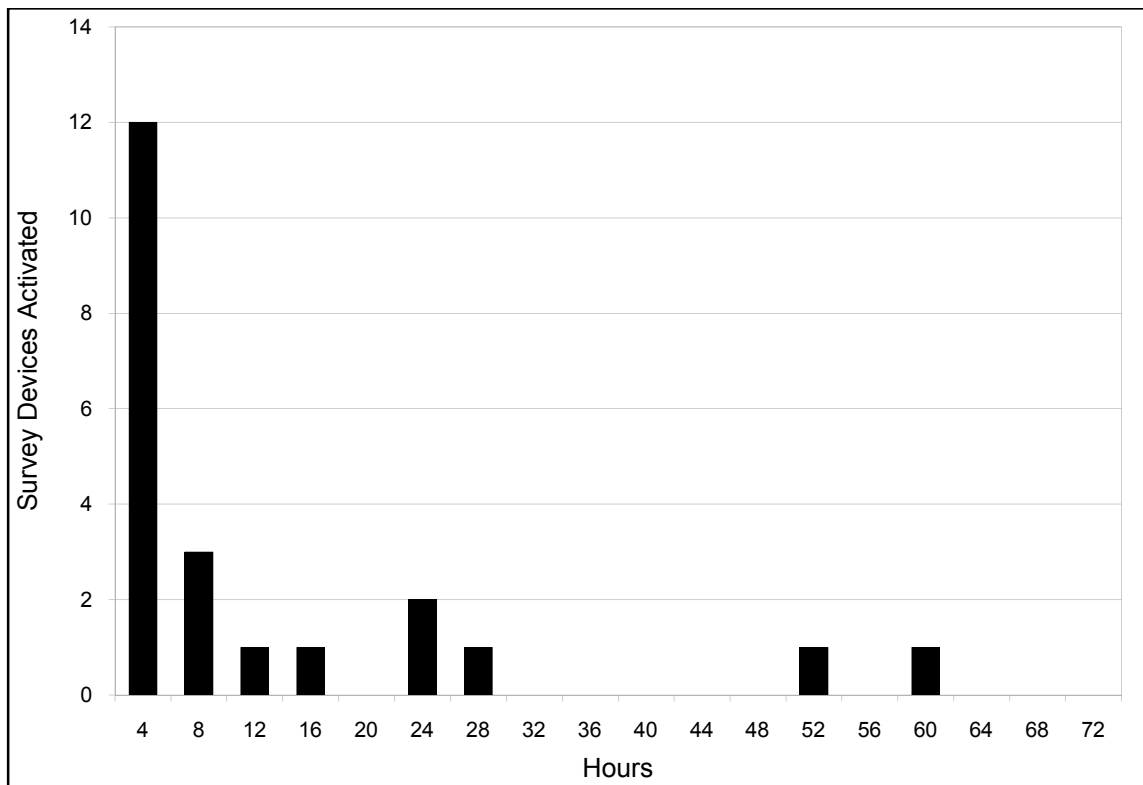


Figure 4. Distribution of activation lag measurements for effective survey devices.

Secondary Results

A secondary endeavor of this research was to execute the experiment in such a way that other non-primary, yet quantifiable, aspects were captured and reported. These variables include the following: The gender of the name on the survey device label; the

weekday the survey device was dropped; and the time of day (morning or midday) the device was dropped. These elements are summarized in Tables 3, 4, 5, 6, 7, and 8. The full data are detailed in Appendix C.

Table 3

Survey Device Effectiveness by Gender of Survey Device Label

Survey Devices	Male	Female	Combined
Dropped by researcher	30	30	60
Recovered by researcher (after 8 hours)	2	3	5
Recovered up by unidentified party	28	27	55
Effective (activated by unidentified party)	11	11	22
Effective Rate (percentage of found)	39.29%	40.74%	40.00%
Effective Rate (percentage of dropped)	36.67%	36.67%	36.67%

Table 4

Effective Survey Device Activation Lag by Gender of Survey Device Label

Effective Survey Devices	Male	Female	Combined
Mean Lag (hours)	9.10	12.29	10.70
Median Lag (hours)	1.76	3.83	3.33

Table 5

Survey Device Effectiveness by Weekday

Survey Devices	Tuesday	Wednesday	Thursday	Combined
Dropped by researcher	20	20	20	60
Recovered by researcher (after 8 hours)	2	0	3	5
Recovered up by unidentified party	18	20	17	55
Effective (activated by unident. party)	9	5	8	22
Effective Rate (percentage of found)	50.00%	25.00%	47.06%	40.00%
Effective Rate (percentage of dropped)	45.00%	25.00%	40.00%	36.67%

Table 6

Effective Survey Device Activation Lag by Weekday

Survey Devices	Tuesday	Wednesday	Thursday	Combined
Mean Lag (hours)	8.65	23.06	5.27	10.70
Median Lag (hours)	1.37	4.33	3.33	3.33

Table 7

Survey Device Effectiveness by Time of Day

Survey Devices	Morning (7:00-11:00)	Midday (11:00-15:00)	Combined
Dropped by researcher	30	30	60
Recovered by researcher (after 8 hours)	2	3	5
Recovered up by unidentified party	28	27	55
Effective (activated by unident. party)	13	9	22
Effective Rate (percentage of found)	46.43%	33.33%	40.00%
Effective Rate (percentage of dropped)	43.33%	30.00%	36.67%

Table 8

Effective Survey Device Activation Lag by Time of Day

Survey Devices	Morning (7:00-11:00)	Midday (11:00-15:00)	Combined
Mean Lag (hours)	11.15	10.04	10.70
Median Lag (hours)	3.83	2.69	3.33

Summary

Table 1 contains the answers to the two research questions posed in Chapter III. The first was “Do USB flash drives remain an effective social-engineering vector for cyber attacks targeting commercial computer systems?” The required evidence to answer Yes was one or more effective drives. The number of effective drives in the commercial population was 11.

The second research question can also be answered by the results identified in Table 1. The second question was “Are USB flash drives an effective social-engineering vector for cyber attacks targeting residential computer systems?” The required evidence to answer Yes was one or more effective drives. The number of effective drives in the residential population was 11, the same number as found in the commercial population.

Chapter V

Discussion

Before discussing the quantitative results generated in the experiment, a quick synopsis of what is known about how and why these results were generated is warranted.

The experiment was modeled after a realistic cyber-attack attack scenario and was designed to study the social-engineering aspect of this type of attack by measuring the propensity of individuals to explore the contents of an unknown USB flash drive after finding it lying on a public sidewalk. The USB flash drives used as survey devices in the experiment were deemed to be effective if they were activated, an event occurring when one or more of the files on each drive was opened from an Internet-connected computer. The opportunity for false positives to be introduced in the collected data was eliminated through the careful use of unique identifiers and security codes embedded within the files of each flash drive survey device. For an activation to occur, the contents of the flash drive must have been read, with the only practical way of doing so through connecting it to a computer and examining the contained files. Therefore, each activation was generated as a consequence of action by the party with physical control of the flash drive. Survey device effectiveness is defined as one or more activations per device, and every effective device represents irrefutable proof that an individual actively connected an unknown USB flash drive to their computer and opened the contents.

The experiment was primarily aimed to explore the effectiveness of the USB flash drive as a malware vector within two sub-populations, the commercial and residential populations of Maui. As depicted in Table 1, 11 of the 30 survey devices targeting the commercial sub-population were found to be effective. Also depicted in Table 1, 11 of the 30 survey devices targeting the residential sub-population were found to be effective. The number of samples was chosen to afford a 95% chance of witnessing an effective flash drive within each surveyed population if the drives were 10% effective (an arbitrary selection). As seen in Table 1, the drives were found to be 36.67% effective in each

population. The activation lag of effective flash drives as depicted in Table 2 shows that the median lag for the commercial population was 2.69 hours and the median lag for the residential population was 4.33 hours.

Also captured in the experiment were other quantitative data that while outside the primary scope, warrant discussion. The gender of the label on each flash drive was a controlled variable and the drives bearing male and female names were distributing in an alternating fashion so as to minimize the affect of confounding factors such as location and time of day. As seen in Table 3, the effective rates were identical for the two sexes at 36.67% each. There were however, different lag times associated with each sex. The median lag time associated with male labels was 1.76 hours, and the median lag time associated with female labels was 3.83 hours. Because of the relatively small sample size and non-normal distribution of response lag measurements, statistical measures of confidence associated with these average lag times are not available.

The effective rates and lag times are summarized for two other secondary factors in Chapter V. These factors are weekday and time of day. These variables were not well controlled as their distributions were heavily influenced by the logistical demands of distributing the survey devices by a single researcher. The most significant limitation is a non-uniform geographic distribution over the 3 distribution days. Specifically, survey devices were distributed in one or two towns per day, with different town on each day. Almost certainly there are differences between towns and their populations that affected effectiveness rates, and these differences are confounding factors in the weekday and time of day summaries. With that caveat, Table 5 depicts the weekday effective rates. These range from a high of 45.00% on Tuesday to a low of 25.00% on Wednesday. Thursday's effective rate was 40.00%. As depicted in Table 7, the time of day effective rates show that flash drives dropped in the morning (between 7:00 and 11:00) were 43.33% effective. Flash drives dropped midday (between 11:00 and 15:00) were 30.00% effective.

Chapter VI

Conclusions

This research project evaluated how readily a cyber attacker could perform an effective social engineering attack using USB flash drives to introduce malware into commercial and residential computer systems. While it is scientifically impossible to prove the absence of a security vulnerability in a computer system using only evidence collected through failed security attacks, the presence of a vulnerability can be demonstrated with a single successful attack. In this research project, the detection of a single effective USB flash drive survey device within each population would have signified the presence of this security vulnerability within that population.

With over one-third of the USB flash drive survey devices being effective, the experiment embodied within this research project demonstrated the very real and continuing vulnerability of commercial systems to this type of cyber attack. Further, the experiment showed that residential systems are just as vulnerable to this threat as their commercial counterparts.

Chapter VII

Recommendations

Each security breach carries with it some value to a cyber-attacker. Because commercial and residential computer systems possess different incentives, the risk to each due to this threat may vary radically. However, residential targets are not free from danger. The falling prices of USB flash drives make them viable for even less-financially lucrative attacks. Further, other factors such as personal motives might influence a targeted attack in a residential setting. The strategies to protect computer systems from this vulnerability largely depend on the perceived likelihood and cost associated with this security risk.

At a minimum, both commercial and residential computer users should be aware of this threat. In a commercial environment, computer system acceptable use policies can reflect the danger associated with unknown media including USB flash drives. From a technical perspective, performing frequent software updates and maintaining updated virus scanning software is very important but is certainly not a complete defense. Operating system and application software bugs are routinely identified only after being exploited by cyber criminals. And virus scanning software has only a marginal ability to catch novel malware. Until the day that computer systems are designed to treat external media as untrustworthy, the threats associated with unknown media will continue. Until then, the best defense strategy for this vulnerability will remain an awareness of the risk involved with connecting unknown USB flash drives.

References

- 3Com Corporation. (2001). Understanding IP addressing: Everything you ever wanted to know (pp. 1-13, Tech.). Santa Clara, CA: 3Com Corporation.
- 8 MB USB Memory Key - Overview. (2005, June 27). IBM. Retrieved from ibm.com
- Amazon.com: 8 GB USB Flash Drive [Advertisement]. (n.d.). Retrieved from <http://www.amazon.com/>
- Casey, M. (n.d.). Frequently asked questions about USB flash drives. About.com. Retrieved from <http://peripherals.about.com/od/removablestorage/f/USBFAQ.htm>
- Cluley, G. (2010, May 21). IBM distributes USB malware cocktail at AusCERT security conference. Sophos. Retrieved from <http://nakedsecurity.sophos.com/2010/05/21/ibm-distributes-usb-malware-cocktail-auscert-security-conference/>
- Connecting America: The national broadband plan. (2010). Washington, DC: Federal Communications Commission.
- Gromov, G. (1995). Roads and Crossroads of Internet History. Internet History, Web History, Silicon Valley, Computer Companies, Computer Magazines, Netvalley. Retrieved from <http://www.netvalley.com/intval.html>
- How NAT Works - Cisco Systems. (2006, January 24). Cisco Systems, Inc. Retrieved from <http://www.cisco.com/en/US/tech/tk648/tk361/technologies`tech`note09186a0080094831.shtml>
- Ingham, K., & Forrest, S. (2002). A history and survey of network firewalls (Rep.). Albuquerque, NM: Department of Computer Science, University of New Mexico.
- Jelinek, P. (2010, August 25). Pentagon: foreign spy agency flash drive caused worst computer breach in 2008 in Middle East. StarTribune.com. Retrieved from <http://www.startribune.com/nation/101492894.html>

Johansson, J. (2008, January). How flash drives and social engineering can compromise networks. Microsoft TechNet. Retrieved from <http://technet.microsoft.com/en-us/magazine/2008.01.securitywatch.aspx>

Kingston Technology Company. (2010, February 18). Kingston Digital ships first 256GB USB flash drive in the U.S. [Press release]. Retrieved from <http://www.kingston.com/press/2010/flash/02d.asp>

Kozierok, C. M. (2005). *The TCP/IP guide: A comprehensive, illustrated Internet protocols reference*. San Francisco: No Starch Press.

McDowell, M. (2008, November 3). US-CERT cyber security tip ST08-001 -- Using caution with USB Drives. United States Computer Emergency Readiness Team. Retrieved from <http://www.uscert.gov/cas/tips/ST08-001.html>

Mitnick, K. D. (2002). *The art of deception*. Indianapolis, IN: Wiley Publishing.

Postel, J. (Ed.). (1981). RFC: 793 Transmission Control Protocol (pp. 30-31) (United States, Defense Advanced Research Projects Agency, Information Processing Techniques Office). Arlington, VA: DARPA.

Popular names by State. (n.d.). The United States Social Security Administration. Retrieved from <http://www.ssa.gov/oact/babynames/state/index.html>

SanDisk 2010 Investor Day Meeting Presentation [PDF]. (2010, February 26). Milpitas, CA: SanDisk Corporation, Inc.

Scarfone, K., & Hoffman, P. (2009). Guidelines on firewalls and firewall policy (United States, National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory). Gaithersburg, MD: NIST.

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world*. New York, NY: John Wiley & Sons.

Schogol, J. (2009, February 20). Mullen: Thumb drive ban won't end soon. Stars and Stripes. Retrieved from <http://www.stripes.com/article.asp?section=104&article=60869>

- Sirmer, J. (2010, November 3). Malware running on AutoRun. Avast! blog. Retrieved from <http://blog.avast.com/2010/11/03/malware-running-on-autorun/#more-1280>
- Smith, A. (2010, August 11). Home Broadband 2010 (Rep.). Retrieved from Pew Research Center's Internet & American Life Project website: <http://pewinternet.org/Reports/2010/Home-Broadband-2010/>
- Stasiukonis, S. (2006, June 7). Social engineering, the USB way. Dark Reading. Retrieved from <http://www.darkreading.com/security/article/208803634/index.html>
- Thompson, J., Gilmore, P., & Gideon, A. (2010). The state of the internet, 2nd Quarter, 2010 Report (Rep.). Retrieved from Akamai Technologies, Inc. website: www.akamai.com/stateoftheinternet
- Zdrnja, B. (2009, January 15). Conficker's autorun and social engineering. SANS Internet Storm Center. Retrieved from <http://isc.sans.edu/diary.html?storyid=5695>

Appendices

- A Bibliography
- B Experiment System Code and Scripts
- C Survey Device Data

Appendix A
Bibliography

Bibliography

- American Psychological Association. (2010). Publication manual of the American Psychological Association (6th ed.). Washington, DC: Author.
- Cooper, D., R., & Schindler, P., S. (2003). Business research methods (8th ed.). New York: McGraw-Hill Irwin.
- Department of Business Administration capstone guide. (2010, February). Daytona Beach, FL: Embry-Riddle Aeronautical University, Department of Business Administration.
- Evans, J. R., & Lindsay, W. M. (2005). The management and control of quality (6th ed.). Eagan, MN: Thomson South-Western.
- Meredith, J. R., & Mantel, S. J. (2006). Project management a managerial approach (6th ed.). Hoboken, NJ: John Wiley & Sons.

Appendix B
Experiment System Code and Scripts

Experiment System Code and Scripts

Internet Data Collection Device

Database creation script:

```
-- Internet Data Collection Device Database Creation Script
--
SET SQL_MODE="NO_AUTO_VALUE_ON_ZERO";
--
-- Database: `drive_response_db`
--
-----
--
-- Table structure for table `drive`
--

CREATE TABLE IF NOT EXISTS `drive` (
  `drive_id` int(11) NOT NULL,
  `label` varchar(15) NOT NULL,
  `gender` varchar(1) NOT NULL,
  `business` varchar(1) NOT NULL,
  `drop_time` int(11) DEFAULT NULL,
  `retrieve_time` int(11) DEFAULT NULL,
  `resume_code` varchar(100) DEFAULT NULL,
  `budget_code` varchar(100) DEFAULT NULL,
  `gallery_code` varchar(100) DEFAULT NULL,
  `slideshow_code` varchar(100) DEFAULT NULL,
  `bookmarks_code` varchar(100) DEFAULT NULL,
  PRIMARY KEY (`drive_id`),
  UNIQUE KEY `label` (`label`)
) ENGINE=MyISAM DEFAULT CHARSET=utf8;

-----
--
-- Table structure for table `response`
--

CREATE TABLE IF NOT EXISTS `response` (
  `drive_id` int(11) NOT NULL,
  `response_time` int(11) NOT NULL,
  `originating_document` varchar(10) NOT NULL
) ENGINE=MyISAM DEFAULT CHARSET=utf8;
```

Database script to initialize survey device data ("Popular names by State," n.d.):

```
INSERT INTO `drive` (`drive_id`, `label`, `gender`, `business`,
`drop_time`, `resume_code`, `budget_code`, `gallery_code`,
`slideshow_code`, `bookmarks_code`) VALUES
(1, 'Joshua', 'M', 'Y', 1211443758, '', '', '', '', ''),
(2, 'Michael', 'M', 'N', 1211443758, '', '', '', '', ''),
(3, 'Christopher', 'M', 'Y', 1211443758, '', '', '', '', ''),
(4, 'Justin', 'M', 'N', 1211443758, '', '', '', '', ''),
(5, 'Matthew', 'M', 'Y', 1211443758, '', '', '', '', ''),
(6, 'Ryan', 'M', 'N', 1211443758, '', '', '', '', ''),
```

(7, 'Brandon', 'M', 'Y', 1211443758, '', '', '', '', ''),
(8, 'James', 'M', 'N', 1211443758, '', '', '', '', ''),
(9, 'Daniel', 'M', 'Y', 1211443758, '', '', '', '', ''),
(10, 'Andrew', 'M', 'N', 1211443758, '', '', '', '', ''),
(11, 'Kyle', 'M', 'Y', 1211443758, '', '', '', '', ''),
(12, 'Nicholas', 'M', 'N', 1211443758, '', '', '', '', ''),
(13, 'Joseph', 'M', 'Y', 1211443758, '', '', '', '', ''),
(14, 'Jonathan', 'M', 'N', 1211443758, '', '', '', '', ''),
(15, 'Robert', 'M', 'Y', 1211443758, '', '', '', '', ''),
(16, 'John', 'M', 'N', 1211443758, '', '', '', '', ''),
(17, 'David', 'M', 'Y', 1211443758, '', '', '', '', ''),
(18, 'Kevin', 'M', 'N', 1211443758, '', '', '', '', ''),
(19, 'Anthony', 'M', 'Y', 1211443758, '', '', '', '', ''),
(20, 'Sean', 'M', 'N', 1211443758, '', '', '', '', ''),
(21, 'Zachary', 'M', 'Y', 1211443758, '', '', '', '', ''),
(22, 'Tyler', 'M', 'N', 1211443758, '', '', '', '', ''),
(23, 'Jacob', 'M', 'Y', 1211443758, '', '', '', '', ''),
(24, 'William', 'M', 'N', 1211443758, '', '', '', '', ''),
(25, 'Aaron', 'M', 'Y', 1211443758, '', '', '', '', ''),
(26, 'Travis', 'M', 'N', 1211443758, '', '', '', '', ''),
(27, 'Alexander', 'M', 'Y', 1211443758, '', '', '', '', ''),
(28, 'Jason', 'M', 'N', 1211443758, '', '', '', '', ''),
(29, 'Christian', 'M', 'Y', 1211443758, '', '', '', '', ''),
(30, 'Micah', 'M', 'N', 1211443758, '', '', '', '', ''),
(31, 'Ashley', 'F', 'Y', 1211443758, '', '', '', '', ''),
(32, 'Jessica', 'F', 'N', 1211443758, '', '', '', '', ''),
(33, 'Nicole', 'F', 'Y', 1211443758, '', '', '', '', ''),
(34, 'Brittany', 'F', 'N', 1211443758, '', '', '', '', ''),
(35, 'Jennifer', 'F', 'Y', 1211443758, '', '', '', '', ''),
(36, 'Sarah', 'F', 'N', 1211443758, '', '', '', '', ''),
(37, 'Amanda', 'F', 'Y', 1211443758, '', '', '', '', ''),
(38, 'Michelle', 'F', 'N', 1211443758, '', '', '', '', ''),
(39, 'Chelsea', 'F', 'Y', 1211443758, '', '', '', '', ''),
(40, 'Lauren', 'F', 'N', 1211443758, '', '', '', '', ''),
(41, 'Samantha', 'F', 'Y', 1211443758, '', '', '', '', ''),
(42, 'Jasmine', 'F', 'N', 1211443758, '', '', '', '', ''),
(43, 'Amber', 'F', 'Y', 1211443758, '', '', '', '', ''),
(44, 'Tiffany', 'F', 'N', 1211443758, '', '', '', '', ''),
(45, 'Rachel', 'F', 'Y', 1211443758, '', '', '', '', ''),
(46, 'Alyssa', 'F', 'N', 1211443758, '', '', '', '', ''),
(47, 'Megan', 'F', 'Y', 1211443758, '', '', '', '', ''),
(48, 'Elizabeth', 'F', 'N', 1211443758, '', '', '', '', ''),
(49, 'Kayla', 'F', 'Y', 1211443758, '', '', '', '', ''),
(50, 'Kimberly', 'F', 'N', 1211443758, '', '', '', '', ''),
(51, 'Courtney', 'F', 'Y', 1211443758, '', '', '', '', ''),
(52, 'Melissa', 'F', 'N', 1211443758, '', '', '', '', ''),
(53, 'Ariel', 'F', 'Y', 1211443758, '', '', '', '', ''),
(54, 'Brittney', 'F', 'N', 1211443758, '', '', '', '', ''),
(55, 'Stephanie', 'F', 'Y', 1211443758, '', '', '', '', ''),
(56, 'Heather', 'F', 'N', 1211443758, '', '', '', '', ''),
(57, 'Kristen', 'F', 'Y', 1211443758, '', '', '', '', ''),
(58, 'Emily', 'F', 'N', 1211443758, '', '', '', '', ''),
(59, 'Sara', 'F', 'Y', 1211443758, '', '', '', '', ''),
(60, 'Tiana', 'F', 'N', 1211443758, '', '', '', '', ''),
(61, 'Monitor', 'X', 'X', 1211443758, '', '', '', '', '');

Primary data collection device program (handles requests and stores survey device data):

```
<?php
// get_image.php
// This program captures input parameters from a URL.  If they match
// the values in the database, a record of the event is taken and an
// image file is returned.  Otherwise, nothing is returned.

include 'config.php';
include 'opendb.php';

// Get input parameters from URL
$id=mysql_real_escape_string($_GET['i']);
$resume=mysql_real_escape_string($_GET['e']);
$budget=mysql_real_escape_string($_GET['u']);
$gallery=mysql_real_escape_string($_GET['a']);
$slideshow=mysql_real_escape_string($_GET['l']);
$bookmarks=mysql_real_escape_string($_GET['o']);
$response_time=time();

if ($id > 0 && $id < 62) { //Fits into the numerical range

if (strlen($resume)==100) {
    $column="resume_code";
    $code=$resume;
    $originating_document="resume";
}
if (strlen($budget)==100) {
    $column="budget_code";
    $code=$budget;
    $originating_document="budget";
}
if (strlen($gallery)==100) {
    $column="gallery_code";
    $code=$gallery;
    $originating_document="gallery";
}
if (strlen($slideshow)==100) {
    $column="slideshow_code";
    $code=$slideshow;
    $originating_document="slideshow";
}
if (strlen($bookmarks)==100) {
    $column="bookmarks_code";
    $code=$bookmarks;
    $originating_document="bookmarks";
}

// Check security code
$query = "SELECT $column from drive where drive_id='$id'";
$result = mysql_query($query);

if ($result > 0){
while ($row = mysql_fetch_assoc($result))
{
```

```

$db_code=$row[$column];
}

if ($db_code==$code) { // Success!
$success=1;
}

} // Result of DB Query is not > 0

if ($success==1) {

$query="INSERT INTO response
(drive_id,response_time,originating_document) values
('$id','$response_time','$originating_document')";

mysql_query($query) or die('Error, insert query failed');

// Event has been captured; serve image file
header ("Content-Type: image/png");
$image = imagecreate(10,10);
$gold = imagecolorallocate($image, 250, 250, 230);
imagepng($image);
imagedestroy($image);
}

} // End of result of ID query being in range

include 'closedb.php';
?>

```

Shared program module for specifying the database connection parameters:

```

<?php
// config.php
$dbhost = '[Redacted]';
$dbuser = '[Redacted]';
$dbpass = '[Redacted]';
$dbname = 'drive_response_db';
?>

```

Shared program module for opening a connection to the MySQL database:

```

<?php
// opendb.php
$conn = mysql_connect($dbhost, $dbuser, $dbpass) or die
('Error connecting to mysql');
mysql_select_db($dbname);
?>

```

Shared program module for closing the connection to the MySQL database:

```

<?php
// closedb.php
mysql_close($conn);
?>

```

Program to update survey device security codes:

```
<?php
// update_random_security_codes.php
include 'config.php';
include 'opendb.php';

function generatePassword() {
    $values =
'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890';

    $password = '';
    $valuesLength = strlen($values);

    for ($i = 0; $i < 100; $i++) {
        $password .= $values[(rand() % $valuesLength)];
    }
    return $password;
}

for ($i=1; $i<62; $i++) {

for ($j=0; $j<5; $j++) {
    if ($j==0) $col="resume_code";
    if ($j==1) $col="budget_code";
    if ($j==2) $col="gallery_code";
    if ($j==3) $col="slideshow_code";
    if ($j==4) $col="bookmarks_code";

    $code = generatePassword();
    $query = "update drive set $col='$code' where drive_id='$i'";

    mysql_query($query) or die('Error, insert query failed');
}
}

include 'closedb.php';
?>
```

USB Flash Drive Survey Devices

Survey device directory structure (output from Linux “tree” command):

```
.
|-- bookmarks.html
|-- budget.html
|-- gallery.html
|-- pictures
|   |-- slideshow.html
|-- resume.html

1 directory, 5 files
```

Representative sample of the survey device bookmarks.html file:

```
<!-- bookmarks.html -->
<html>
<head>
<title>
</title>
</head>
<body
background="http://pixelfoot.com/mstm/get_image.php?o=8rYuIwU3X1fQCZfmrn0SzX
JOBkIuf5NajAuRUeII3NouAuFRHEy5p6GQee9j7KhfaBVUDtsv7FNuXibsKxmYtSExVBERbLV0cG
TD&i=2">
Michael Lee's<br>
Bookmarks
<br>
</body>
</html>
```

Representative sample of the survey device budget.html file:

```
<!-- budget.html -->
<html>
<head>
<title>
</title>
</head>
<body
background="http://pixelfoot.com/mstm/get_image.php?u=5NYySc7V59DxbAhfWxXaUq
nf09ch9nB1looHqjsifTGgiLk5984QlgTkcUqa8R1W6dtjkLqptWvBxFttAk8JoRSrB9pyNekHhD
Qp&i=2">
Michael Lee's Budget
<br>
</body>
</html>
```

Representative sample of the survey device gallery.html file:

```
<!-- gallery.html -->
<html>
<head>
<title>
</title>
</head>
<body
background="http://pixelfoot.com/mstm/get_image.php?a=d7EuQXTbrcsPlqpz880w65
UI96ddwUsxOURtHAsWBJCMXRbUMQgFIYbGRfHeXZBzHhSeH0Z9IrIv7IdIohbU6cqNhXP3Keshla
jR&i=2">
Michael Lee's Gallery
<br>
</body>
</html>
```

Representative sample of the survey device slideshow.html file:

```
<!-- slideshow.html -->
<html>
<head>
<title>
</title>
</head>
<body
background="http://pixelfoot.com/mstm/get_image.php?l=09NFnk1jS4P59QO5R5FWPi
Pnm8sw6zb4yMyJWnTEewyddc8S5AEHIjUUeaeaAd4WQpvCCc6FztIAuDio4MUBUCjYDmY2pPL647
wt&i=2">
<br>
<br>
Back...Forward
<br>
(c) Michael Lee
</body>
</html>
```

Representative sample of the survey device resume.html file:

```
<!-- resume.html -->
<html>
<head>
<title>
</title>
</head>
<body
background="http://pixelfoot.com/mstm/get_image.php?e=vEcTilNbK
H6HCBq7CV8MNQ5gqRHPkgVDIwMRKXQksMRVd6PDQMesq9wGP5lXa6qJPAopm5AE
GhpId3bRFf0TewqRqzFouTV8k0nu&i=2">
Resume of Michael Lee
<br>
</body>
</html>
```

Survey Device Preparation Tool

Program to create survey device file sets:

```
<?
// make_drive_file_sets.php - Create survey device file sets
$startTime = time();
include 'config.php';
include 'opendb.php';

$mainDir="drive_files";
if (!file_exists($mainDir)) mkdir($mainDir);

for ($i=1;$i<62;$i++){
$query = "select drive id, label, resume code, gallery code, budget code,
```

```

slideshow_code, bookmarks_code  from drive where drive_id='$i';
$result=mysql_query($query);
while($row=mysql_fetch_assoc($result))
{
$label=$row['label'];
$drive_id=$row['drive_id'];
$resume_code=$row['resume_code'];
$gallery_code=$row['gallery_code'];
$slideshow_code=$row['slideshow_code'];
$bookmarks_code=$row['bookmarks_code'];
$budget_code=$row['budget_code'];
}
echo $label . "\n";

if (!file_exists($mainDir."/". $label)) mkdir($mainDir."/". $label);
if (!file_exists($mainDir."/". $label."/pictures")) mkdir
($mainDir."/". $label."/pictures");

//use: createFile(uniqueId, friendlyName, securityCode, securityIdentifier,
inFile, outFile);
createFile($drive_id, $label." Lee", $gallery_code, "a", "gallery.html",
$mainDir."/". $label."/gallery.html");
createFile($drive_id, $label." Lee", $resume_code, "e", "resume.html",
$mainDir."/". $label."/resume.html");
createFile($drive_id, $label." Lee", $budget_code, "u", "budget.html",
$mainDir."/". $label."/budget.html");
createFile($drive_id, $label." Lee", $bookmarks_code, "o", "bookmarks.html",
$mainDir."/". $label."/bookmarks.html");
createFile($drive_id, $label." Lee", $slideshow_code, "l", "slideshow.html",
$mainDir."/". $label."/pictures/slideshow.html");
}
include "closedb.php";
echo "Finished, took " . (time() - $startTime) . " seconds to complete.";

function createFile($uniqueId, $friendlyName, $securityCode,
$securityIdentifier, $inFile, $outFile){
$outHandle = @fopen($outFile, "w");
$inHandle = @fopen($inFile, "r");
if ($inHandle) {
while (!feof($inHandle)) {
$buffer = fgets($inHandle, 4096);
$buffer = str_replace("XxXxXxXx", $friendlyName, $buffer);
$buffer =
str_replace("YyYyYyYy", "http://pixelfoot.com/mstm/get_image.php?". $securityI
dentifier."=" . $securityCode."&i=" . $uniqueId, $buffer);
//echo $buffer;
fwrite($outHandle, $buffer);
}
fclose($inHandle);
fclose($outHandle);
}
} //end of createFile
?>

```

Bookmarks.html template file:

```
<!-- bookmarks.html -->
<html>
<head>
<title>
</title>
</head>
<body background="YyYyYyYy">
XxXxXxXx's<br>
Bookmarks
<br>
</body>
</html>
```

Budget.html template file:

```
<!-- budget.html -->
<html>
<head>
<title>
</title>
</head>
<body background="YyYyYyYy">
XxXxXxXx's Budget
<br>
</body>
</html>
```

Gallery.html template file:

```
<!-- gallery.html -->
<html>
<head>
<title>
</title>
</head>
<body background="YyYyYyYy">
XxXxXxXx's Gallery
<br>
</body>
</html>
```

Slideshow.html template file:

```
<!-- slideshow.html -->
<html>
<head>
<title>
</title>
</head>
<body background="YyYyYyYy">
<br>
<br>
Back...Forward
<br>
(c) XxXxXxXx
</body>
</html>
```

Resume.html template file:

```
<!-- resume.html -->
<html>
<head>
<title>
</title>
</head>
<body background="YyYyYyYy">
Resume of XxXxXxXx
<br>
</body>
</html>
```

Data Collection Device Monitoring Tools

Program that displays survey device database entries (IVs):

```
<?php
// view_drives.php
include 'config.php';
include 'opendb.php';

$query = "SELECT drive_id, label, gender, business, drop_time, resume_code,
budget_code, gallery_code, slideshow_code, bookmarks_code FROM drive order
by drive_id";

$result = mysql_query($query);

echo "<table border=1>";
echo "<tr><td>drive_id</td><td>label</td><td>gender</td><td>business</td><td>
drop_time</td><td>resume_code</td><td>budget_code</td><td>gallery_code</td><
td>slideshow_code</td><td>bookmarks_code</td></tr>";
while($row = mysql_fetch_assoc($result))
{
echo "<tr>";
echo "<td>{$row['drive_id']}</td>";
echo "<td>{$row['label']}</td>";
echo "<td>{$row['gender']}</td>";
echo "<td>{$row['business']}</td>";
echo "<td>{$row['drop_time']}</td>";
//echo "<td>{$row['resume_code']}</td>";
//echo "<td>{$row['budget_code']}</td>";
//echo "<td>{$row['gallery_code']}</td>";
//echo "<td>{$row['slideshow_code']}</td>";
//echo "<td>{$row['bookmarks_code']}</td>";
echo "</tr>";
}
echo "</table>";

include 'closedb.php';
?>
```

Program that allows real-time viewing of effective survey device data (DVs):

```
<?php
// view_responses.php
include 'config.php';
include 'opendb.php';

$query = "SELECT drive.drive_id, label, gender, business, drop_time,
response_time, (response_time - drop_time)/3600 AS latency_hrs,
originating_document FROM drive, response WHERE
drive.drive_id=response.drive_id ORDER BY drive_id";

$result = mysql_query($query);

echo "<table border=1>";
```

```

echo"<tr><td>drive_id</td><td>label</td><td>gender</td><td>business</td><td>
drop_time</td><td>response_time</td><td>latency_hrs</td><td>originating_docu
ment</td></tr>";
while($row = mysql_fetch_assoc($result))
{
echo "<tr>";
echo "<td>{$row['drive_id']}</td>";
echo "<td>{$row['label']}</td>";
echo "<td>{$row['gender']}</td>";
echo "<td>{$row['business']}</td>";
echo "<td>{$row['drop_time']}</td>";
echo "<td>{$row['response_time']}</td>";
echo "<td>{$row['latency_hrs']}</td>";
echo "<td>{$row['originating_document']}</td>";
echo "</tr>";
}
echo "</table>";

include 'closedb.php';
?>

```

Internet data collection device monitoring script:

```

### monitor.sh

#!/bin/bash
for i in `seq 4800` # 10 days * 24 hours * 20 times per hour
do
    wget -T 20 "http://pixelfoot.com/mstm/get_image.php?o=yyy&i=xxx"
    sleep 180 # Pause for 3 minutes
done

```

Appendix C
Survey Device Data

Survey Device Data

ID	Label	Sex	Bus.	Drop Time	Day	Time	Retrieve Time	Lag (hrs)
27	Jeremy	M	Y	2011-01-25 09:13:36	Tue	Morning	NULL	25.5889
51	Courtney	F	Y	2011-01-25 09:28:50	Tue	Morning	NULL	0.8075
25	Aaron	M	Y	2011-01-25 09:33:06	Tue	Morning	NULL	NULL
47	Megan	F	Y	2011-01-25 09:37:47	Tue	Morning	NULL	NULL
7	Brandon	M	Y	2011-01-25 09:42:17	Tue	Morning	NULL	0.2092
16	John	M	N	2011-01-25 09:48:50	Tue	Morning	NULL	NULL
56	Heather	F	N	2011-01-25 10:15:11	Tue	Morning	NULL	20.1017
26	Travis	M	N	2011-01-25 10:21:12	Tue	Morning	NULL	NULL
38	Michelle	F	N	2011-01-25 10:27:43	Tue	Morning	NULL	NULL
12	Nicholas	M	N	2011-01-25 10:43:18	Tue	Morning	NULL	0.1872
42	Jasmine	F	N	2011-01-25 11:21:30	Tue	Midday	NULL	NULL
20	Sean	M	N	2011-01-25 11:27:38	Tue	Midday	NULL	1.3678
32	Jessica	F	N	2011-01-25 11:33:30	Tue	Midday	2011-01-25 19:34:30	NULL
18	Kevin	M	N	2011-01-25 11:46:20	Tue	Midday	NULL	6.7831
36	Sarah	F	N	2011-01-25 11:49:14	Tue	Midday	NULL	NULL
41	Samantha	F	Y	2011-01-25 12:01:54	Tue	Midday	2011-01-25 19:51:30	NULL
29	Christian	M	Y	2011-01-25 12:15:45	Tue	Midday	NULL	1.1503
59	Angela	F	Y	2011-01-25 12:50:42	Tue	Midday	NULL	21.6772
11	Kyle	M	Y	2011-01-25 13:09:20	Tue	Midday	NULL	NULL
53	Ariel	F	Y	2011-01-25 13:13:30	Tue	Midday	NULL	NULL
19	Anthony	M	Y	2011-01-26 07:53:45	Wed	Morning	NULL	NULL
43	Amber	F	Y	2011-01-26 07:57:04	Wed	Morning	NULL	NULL
13	Joseph	M	Y	2011-01-26 08:00:24	Wed	Morning	NULL	NULL
54	Caitlin	F	N	2011-01-26 08:08:04	Wed	Morning	NULL	NULL
8	James	M	N	2011-01-26 08:16:30	Wed	Morning	NULL	NULL
57	Kristen	F	Y	2011-01-26 08:23:30	Wed	Morning	NULL	NULL
50	Kimberly	F	N	2011-01-26 08:25:30	Wed	Morning	NULL	58.0114
3	Christopher	M	Y	2011-01-26 08:32:40	Wed	Morning	NULL	1.7592
4	Justin	M	N	2011-01-26 08:39:40	Wed	Morning	NULL	NULL
46	Alyssa	F	N	2011-01-26 09:04:30	Wed	Morning	NULL	NULL
33	Nicole	F	Y	2011-01-26 13:21:15	Wed	Midday	NULL	NULL
24	Bryson	M	N	2011-01-26 13:26:33	Wed	Midday	NULL	NULL
17	David	M	Y	2011-01-26 13:30:00	Wed	Midday	NULL	NULL
37	Amanda	F	Y	2011-01-26 13:35:20	Wed	Midday	NULL	NULL
21	Zachary	M	Y	2011-01-26 13:40:50	Wed	Midday	NULL	NULL
39	Chelsea	F	Y	2011-01-26 13:45:50	Wed	Midday	NULL	2.685
40	Lauren	F	N	2011-01-26 13:48:52	Wed	Midday	NULL	NULL
6	Ryan	M	N	2011-01-26 13:59:22	Wed	Midday	NULL	4.3283
58	Emily	F	N	2011-01-26 14:02:35	Wed	Midday	NULL	NULL
30	Micah	M	N	2011-01-26 14:10:30	Wed	Midday	NULL	48.5208
1	Joshua	M	Y	2011-01-27 08:00:35	Thu	Morning	NULL	8.9531
55	Stephanie	F	Y	2011-01-27 08:02:50	Thu	Morning	NULL	13.3147
5	Matthew	M	Y	2011-01-27 08:06:10	Thu	Morning	NULL	NULL
45	Rachel	F	Y	2011-01-27 08:09:20	Thu	Morning	NULL	2.8278
48	Elizabeth	F	N	2011-01-27 08:12:30	Thu	Morning	NULL	7.1561
2	Michael	M	N	2011-01-27 08:17:53	Thu	Morning	2011-01-27 17:37:10	NULL

52	Melissa	F	N	2011-01-27 08:22:08	Thu	Morning	NULL	3.8264
10	Alexander	M	N	2011-01-27 08:27:08	Thu	Morning	2011-01-27 17:41:34	NULL
60	Tiana	F	N	2011-01-27 08:33:03	Thu	Morning	NULL	2.2311
9	Daniel	M	Y	2011-01-27 08:39:04	Thu	Morning	NULL	NULL
31	Ashley	F	Y	2011-01-27 11:39:04	Thu	Midday	NULL	NULL
23	Jacob	M	Y	2011-01-27 11:44:50	Thu	Midday	NULL	1.2792
49	Kayla	F	Y	2011-01-27 11:51:39	Thu	Midday	NULL	NULL
15	Robert	M	Y	2011-01-27 12:01:42	Thu	Midday	NULL	NULL
22	Tyler	M	N	2011-01-27 12:13:50	Thu	Midday	NULL	NULL
34	Brittany	F	N	2011-01-27 12:23:00	Thu	Midday	NULL	2.5853
28	Jason	M	N	2011-01-27 12:30:59	Thu	Midday	NULL	NULL
35	Jennifer	F	Y	2011-01-27 12:36:00	Thu	Midday	NULL	NULL
44	Tiffany	F	N	2011-01-27 12:45:07	Thu	Midday	2011-01-27 20:57:59	NULL
14	Jonathan	M	N	2011-01-27 12:50:05	Thu	Midday	NULL	NULL