Use Authorization

In presenting this thesis in partial fulfillment of the requirements for an advanced degree at Idaho State University, I agree that the Library shall make it freely available for inspection. I further state that permission to download and/or print my thesis for scholarly purposes may be granted by the Dean of the Graduate School, Dean of my academic division, or by the University Librarian. It is understood that any copying or publication of this thesis for financial gain shall not be allowed without my written permission.

Signature _____

Date _____

Covert Transmission Malware System

Marshall Steel Smith

A thesis

submitted in partial fulfillment

of the requirements of the degree of

Master of Business Administration in the College of Business

Idaho State University

Spring 2014

To the Graduate Faculty:

The members of the committee appointed to examine the thesis of Marshall Smith find it satisfactory and recommend that it be accepted.

_____

Dr. Corey Schou,

Major Advisor

_____

Dr. David Beard,

Committee Member

_____

Dr. Jonathan Lawson,

Graduate Faculty Representative

Table of Contents

List of Figures vi
Glossary vii
Abstract viii
Chapter 1: Introduction 1
Chapter 2: Literature Review 3
Malware 3
Espionage 4
Chapter 3: Current State of the World: A Global Mobile Perspective 9
Networking 11
Unstructured Peer-to-Peer Network 11
Star Network 12
Mobile Networks 13
Chapter 4: Espionage 14
State Espionage 14
Industrial Espionage 15
Dead Drops 17
Covert Communication 19
Covert Countermeasures 22
Chapter 5: Malware 25
What is Malware? 25
Protection from Malware 26
Mobile Platforms and Malware 30
Malware into the Future 32
Chapter 6: Covert Transmission Malware System 34
Overview 34
Application Scenario 34
Components of the Covert Transmission Malware System 36
Covert Transmission Malware 37
Infected Device 39
Passive Devices 41
Chapter 7: Future Research 44

Chapter 8: Conclusion 46
Bibliography 48
Appendices 55
Passive Camera System 55
System Setup 55
Raspberry PI Setup 58
Wi-Fi Setup 59
Motion Setup 60
Raspbian Email Setup 63
SSMTP Setup 63
Mutt Setup 64
Auto Zip and Mail 68

List of Figures

Figure 1 Mobile broadband Internet subscriptions in 2012 as a percentage of a country's population (Mobile Broadband 2014) 9
Figure 2: Mobile Cellular Subscriptions in relation to Population (Information Telecommunication Union 2013) 10
Figure 3: Unstructured Peer-to-Peer Network (Peer-to-peer 2014) 12
Figure 4: Star Network (Network Topology n.d.) 13
Figure 5: Hollowed Out Rock (Rynolds 2006) 18
Figure 6: 1948 Alger Hiss Hollowed out Pumpkin (Finin 2006) 18
Figure 7: McCumber Cube 22
Figure 8: Malware Attack Goals 25
Figure 9: Versions of Android's Operating systems 31
Figure 10: Top Threat Type Distribution (Trend Micro 2013) 32
Figure 11: Covert Transmission System. 35
Figure 12: Passive Device 43
Figure 13: Raspberry Pi Model B 55
Figure 14: Raspberry Pi Camera 5 Megapixels 55
Figure 15: TP-Link TL-WN823N 300 Mbps Wireless Mini USB Adapter 56
Figure 16: Anker Astro 3 56
Figure 17: Passive Camera System 57
Figure 18: Mutt Configuration File 64
Figure 19: Zip and Mail Bash Script 68

Glossary

Anonymity Sets: The set of total individual subjects that can be used in transmission or reception of a covert message.

Bot Net: A collection of Internet-connected programs communicating with other similar programs in order to perform tasks.

Counterintelligence: Information gathered and activities conducted to protect against espionage.

Covert Channels: Communication channels that exists, contrary to its design.

Dead Drop: A “container” not easily found… that should be possible to approach and fill or empty but not easily observable.

Geocaching: An outdoor recreational activity, in which the participants use a Global Positioning System (GPS) receiver or mobile device and other navigational techniques to hide and seek containers.

Grey Markets: Third party markets that sell or offer free applications that are generally from unsecure sources.

Malware: Malware is short for "malicious software." Malware is any kind of unwanted software that is installed without your adequate consent. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

Mobile Broadband: Broadband access in the cellular environment.

Networking: Enables communication between computing devices and other peripherals.

Passive Device: A device that collects data without using any detectible signals.

Signals Intelligence: is intelligence-gathering by interception of signals.

Unstructured Peer-to-Peer Network: Decentralized and distributed network architecture in which individual nodes in the network act as both suppliers and consumers of resources.

COVERT TRANSMISSION MALWARE SYSTEM

Thesis Abstract – Idaho State University - 2014

Mobile devices are becoming a mainstay in public life. Security for these devices is a relatively new industry and users are generally ignorant of the security issues. Covert channels using mobile devices with their varied communication abilities are a great risk to industry, government, and private sectors.

This paper addresses the possibility of using mobile devices infected with malware as a vector of covert data transfer. With the increased use of mobile devices, traditional and industrial espionage is a national concern. It is believed that a network of infected mobile devices could be used to transfer data from its collection point through mobile networks to its destination. Mobile malware transmission could leave the sender and receivers unidentifiable. Using such a covert transmission system would also make the covert channel extremely difficult to detect. This paper is intended to show a proof of concept and bring awareness of this issue to Academia, Cyber Security officials, and Government Agencies.

Chapter 1: Introduction

Problem:

Covert forms of communication continually threaten governments and industries. The mass acceptance and proliferation of smart mobile devices create a potential vector for covert communication. The purpose of this thesis paper is to determine the feasibility of covert communication by way of infected mobile device malware.

Mobile devices have become a mainstay in everyday lives. Many people have not just one but multiple mobile devices constantly on their person. The industry of smart mobile devices is in its infancy. Finding ways of securing and protecting those devices is also in its early stages. This thesis, "Covert Transmission Malware System," proposes that nation states, criminal organizations, terrorist organizations, and corporations could use malware infected mobile devices as a means to anonymously transfer covert data from one site to another.

Significant research on the topic of malware, both for mobile devices and computer systems, is available. This research usually centers on specific attack goals such as "sabotage, fraud, data theft, spam and service misuse" (Suarez-Tangil 2013) or specific types of malware. In this paper I will introduce the Covert Transmission Malware System as a new specific attack goal that could be employed on mobile devices.

The Covert Transmission Malware System will be discussed in the following manner:

- Literature Review
- Current State of the world: A short overview of smart mobile devices on a worldwide scale
- Networking and Mobile Networks: How networks operate, includinga more in-depth look at mobile networks
- Espionage: A historical look at dead drops and its technological progression
- Covert \Overt Communication: How types of communications can be accomplished in a secret manner
- Malware: The hidden enemy
- Covert Transmission Malware System: An anonymous transmission system
- Conclusion
- Proof of Concept: A simple dead drop example

Awareness of the potential exploitation of mobile devices as a means of covert communication is essential for security personnel. Governments and industries must begin to protect their data from this type of exploit.

Chapter 2: Literature Review

Malware

Suarez-Tangil, G. *Evolution, Detection and Analysis of Malware for Smart Devices.* March 22, 2013.

In the "Evolution, Detection and Analysis of Malware for Smart Devices" Guillermo Suarez-Tangil discusses types of malware that could potentially exploit mobile devices. Within his paper Suarez-Tangil breaks malware into attack goals and characteristics. He also goes into detail about how current security measures are inadequate.

Marforio, Claudio. "Analysis of the Communication between Colluding Applications on Modern Smartphones." (ACSAC), no. Dec (2012).

Claudio Marforio's article "Analysis of the Communication between Colluding Applications on Modern Smartphones" describes the threat of applications that cannot be trusted to behave according to its declared purpose. Mobile applications are supposed to be designed with no interaction between each other. This is described as sandboxing in industry. Marforio has discovered that not only are applications able to get around the sandboxing, but most security tools cannot detect all channels of communication.

Trend Micro. "Android Under Siege: Popularity Comes at a Price." *TrendLabs 3Q 2013 Security Roundup.* 10 01, 2012.

Trend Micro is a security company that researches current digital security issues. Each quarter it releases reports on digital security. The 2013 third quarter security roundup addressed the issues of the Android operating system. As an open source operating

system and a current market share of 81 percent it is the most targeted mobile operating system.

They addressed the issue of end-user license agreement that overstep the needs of the application. Many developers request permission for resources on the device that are not needed. As a common practice this type of agreement would be part of the Covert Transmission Malware System. Within the fine print it would allow the phone to be used to communicate data back to a development server.

Trend Micro. "Mobile threats Go Full Throttle." ***TrendLabs 2Q 2013 Security Roundup.*** **10 01, 2012.**

The 2013 second quarter security roundup addressed the issue of increased sophistication to bypass security measures. As mobile devices evolve and technological abilities increase malware will become more powerful. Mentioned in this issue is the fact that the Android master key is vulnerable to attacks and that 99 percent of mobile devices were affected by it.

Espionage

Office of the Director of National Intelligence. ***Worldwide Threat Assessment of the US Intelligence Community.*** **Washington DC: United States of America, 2014.**

Every year the Office of the Director of National Intelligence publishes a worldwide threat report against the US national security. This year Director James R. Clapper reported the following as the top four greatest threats: cyber security, counterintelligence, terrorism, weapons of mass destruction and proliferation. Of these top four, cyber security and counterintelligence are number one and two. This report

highlights the concerns the US Intelligence Community (IC) has in regards to threats directed at the US.

International Data Group. *How Mobility is Disrupting Technology and Information Consumption.* IDG Global Solutions, 2012.

Many industries are now allowing the use of private devices within their work environments. In this IDG study, of those surveyed, 50 percent owned or used a mobile device and half of them used their personal device for work. Organizations are struggling to enable the free use of devices without risking security.

Sbrusch, Raymond. "Network Covert Channels: Subversive Secrecy." *SANS.* 2006. SANS.org (accessed 03 27, 2014).

Raymond Sbrusch reports his research in "Network Covert Channels: Subversive Secrecy," which is an analysis of motives for covert network channels, methods of hiding data and countermeasures being employed to detect and prevent these types of channels. He is one of the first that identifies covert channels not as attack tools but systems to leech information away from organizations. He also introduces the concept of "anonymity sets."

Department of Defense. *Trusted Computer System Evaluation Criteria.* Washington DC: DoD USA, 1985.

The Department of Defense introduced the "Trusted Computer System Evaluation Criteria" as a method of securing their computer systems. Since 1985 there have been many updates to this work; however, guidelines on covert channels and its definition have not changed significantly. The only significant change is the potential amount of data loss and the speeds by which it can be lost.

Bidou, Renaud. "Covert Channels." ***iv2-technologies.*** **n.d.**

Renaud Bidou discusses how covert channels can be used to protect privacy. He also discusses techniques that are important in case of detection. Through his research he addresses the concepts of both using stealth channels or covert channels and also hidden information within them. The characteristics a covert channel shares with regular channels are also introduced.

Fisk, Gina. "Eliminating Steganography in Internet Traffic with Active Wardens." (accessed 02 28, 2014).

Eliminating Steganography in Internet Traffic with Active Wardens addresses a method of preventing hidden information from transmitting. Gina Fisk states that network security is one of the most pressing and difficult problems facing modern private organizations and governments. She also introduces an “active warden” that is constantly watching and preventing covert channels over internal networks. The methods she suggests to keep information secure are valid and show great potential.

However in relation to a Covert Transmission Malware System, methods mentioned by Gina Fisk could be circumvented by the use of mobile broadband and private mobile devices. A valid user could collect significant amounts of data within legitimate channels and then transmit it without the use of an internal network.

Zander, Sebastian. "A Survey of Covert Channels and Countermeasures in Computer (accessed 02 28, 2014).

In “A Survey of Covert Channels and Countermeasures in Computer Network Protocols,” Sebastian Zander introduces the difference between encryption and covert channels. He also gives an overview of common methods for detecting and eliminating covert channels as well as their limited of capacity. All of this information can be used to improve security in future computer networks. Included in his writing are application scenarios where these methods might be used and the different security models that would work best in a given scenario. One key chink in most network security is the lack of ability to control data that is transmitted through independent broadband mobile devices.

Hill, Raquel. "Quantifying and Classifying Covert Communications on Android." ***Springer Science+Business media*****, 2013: 79-87.**

Raquel Hill’s research into covert communications focuses on the ability to use mobile device hardware to enable communication between applications. Using the device’s volume and vibrations, Hill was able to sustainably transfer 80-100 bits per second. While this is not a significant amount of data, it could be enough to transmit credit card numbers, social-security numbers or GPS coordinates.

Smith, I. C. "The FBI and Chinese Espionage." ***Wikileaks.*** **n.d. (accessed May 05, 2014).**

The FBI and Chinese Espionage is a speech given during the Third Raleigh International Spy Conference. Within this take I. C. Smith gives an overview of Chinese espionage in the United States. While espionage against the United States government happens, the vast majority of it is done against industries. Not only are industries targeted but also universities and places of research. It is interesting to note that he also mentions that

content is not really important to the Chinese. They are trying to acquire as much research and technology as possible without any specific requirements.

W. Victor Maconachy, Corey D. Schou. "A Model for Information Assurance: An Integrated Approach." *BYU.net.* June 5, 2001. (accessed May 29, 2014).

W. Victore Maconachy and Dr. Corey D. Schou expand the McCumber model within this paper. Developed in 1991, the McCumber Model provides a brief depiction of the information systems security discipline. With the growth and advancement of technology the McCumber model needed to be expanded. In this paper two additional sections were added to the Security Services. The original McCumber Model featured Availability, Integrity and Confidentiality. Authentication and Non-repudiation were added with this article. This new model was named the Information Assurance Model.

Chapter 3: Current State of the World: A Global Mobile Perspective

From a global perspective, previously inaccessible mobile technology has started to become available to all people everywhere. Where there once was pure poverty, second-hand mobile devices are becoming readily available. In many parts of the world, wireless communication is the only financially viable method of communication. At little cost to the cellular companies, mobile broadband has been enabled on many of those cellular sites worldwide.

Mobile broadband is “broadband access in the cellular environment.” (Virginia Tech 2012) While both mobile broadband and Wi-Fi are wireless, Wi-Fi is still limited to a fairly confined area of about 200 feet around the access point. Mobile broadband, on

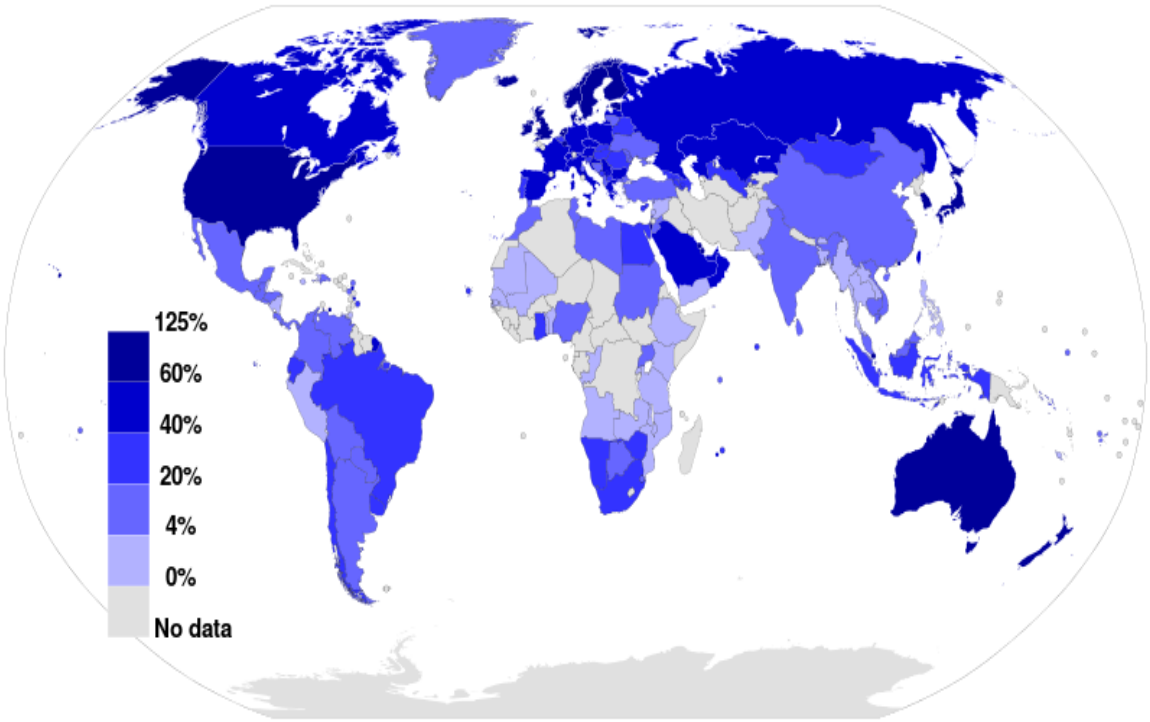

Figure 1 Mobile broadband Internet subscriptions in 2012 as a percentage of a country's population (Mobile Broadband 2014)

the other hand, extends that reach and provides high-speed Internet access within the range of 22 miles (Airwave Management LLC 2013) from the cell site.

Figure 1 shows the International Telecommunication Union (ITU) report on mobile broadband subscriptions worldwide. Mobile broadband is accepted throughout the world. While the United States overwhelmingly has the most broadband Internet subscriptions, Russia follows close behind and China below them, due largely to its vast population. Even countries with low mobile broadband are at risk of Covert Transmission Malware System attacks.

In addition to the 2012 mobile broadband study, ITU in 2013 reported on the continued growth and use of mobile devices worldwide. Figure 2 shows the estimated mobile-cellular subscriptions worldwide. In 2013 mobile cellular subscriptions would be within

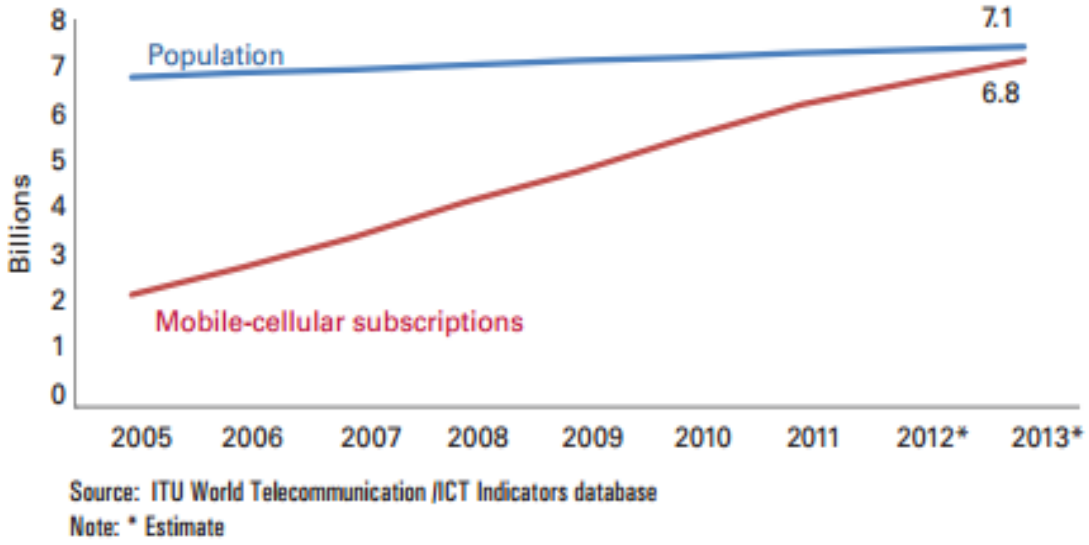

Figure 2: Mobile Cellular Subscriptions in relation to Population (Information Telecommunication Union 2013)

5 percent of the total worldwide population, and is expected to continue growing.

Networking

Networking, in relation to computing devices, enables communication between devices and other peripherals. With each computer connection, the size of the network increases. Computing devices connected to the Internet are part of one huge network. This network allows for instant communication, sharing of ideas, and the potential theft of data and information.

Networks can be set up in many different ways to enable efficient and secure communication. While there are many types of networks, the research for this paper, has been confined to a hybrid combination of unstructured peer-to-peer and star network topology. It is a combination of these two types of networks that best describe the Covert Transmission Malware System. In addition to these two network topologies, I will also discuss in depth mobile broadband networks.

Unstructured Peer-to-Peer Network

An unstructured network is a network without any particular structure that is used to communicate data from one device to the next. It is self-organized and decentralized and each device is equal. Each device attached to this network acts as a node that makes informal connections to other devices. As more devices connect to the network, each provides available data to the overall network. As seen in Figure 3, these networks

can be built from different devices, and connections can be made from any node in the network.

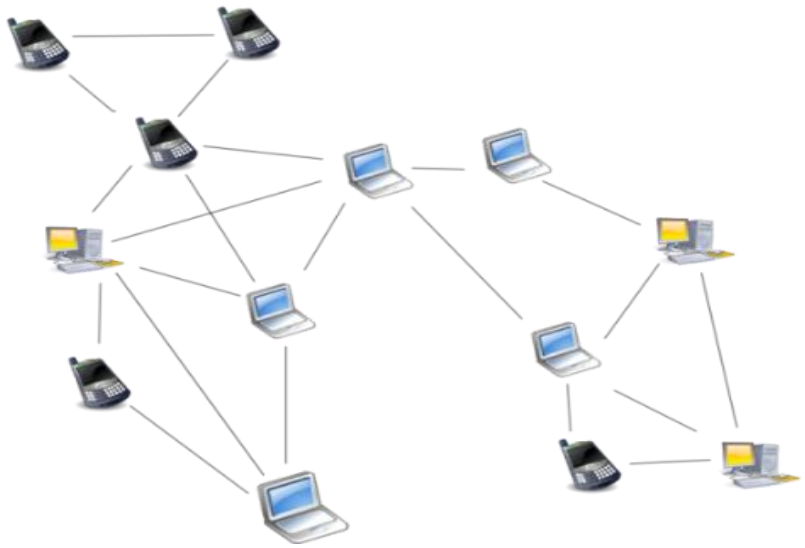

Figure 3: Unstructured Peer-to-Peer Network (Peer-to-peer 2014)

According to Microsoft (MSDN Microsoft 2014), some of the advantages of using an unstructured network include:

- No single point of failure
- Easy to set up
- All content shared
- No full-time administrator
- Low cost

This type of network has been growing significantly because of these advantages. Unstructured networks are often spoken of in a negative connotation, because of their frequent use for illegal purposes; however, legal and legitimate reasons exist for using them. For example, when an enterprise is reimaging computer systems peer-to-peer networking can be used to assist in the imaging process.

Star Network

A star network is built in the shape of a star as seen in Figure 4. The topology of a star network revolves around a central hub or switch that all other systems or nodes connect too. There is no limit to how many nodes can be connected to the hub. In the case of a star network, if any one

of the nodes fails the rest of the network continues; however, if the central hub fails, the whole network fails.

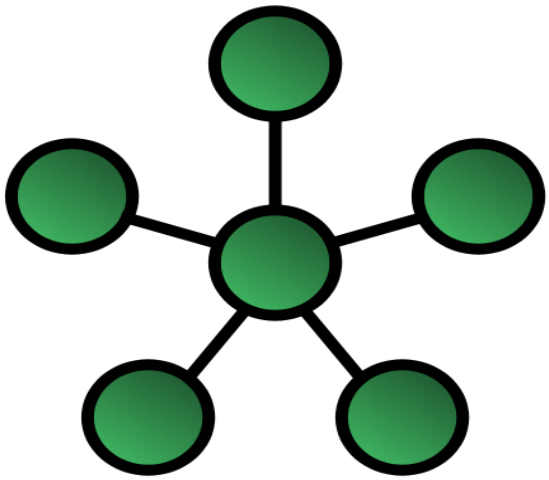

Figure 4: Star Network (Network Topology n.d.)

Mobile Networks

In 1991 a new form of network access became available for public use. Mobile access to data called 2G introduced the possibility of true mobile networks to ht world as a whole. With speeds of up to 144kbit/s, 2G became more practical for use on the go. As technology advanced, 3G allowed for speeds of up to 2Mbps, and later 4G bumped speeds up to 1Mbps. (Speedguide 2014) This has changed our dumb mobile devices into true communication marvels capable of transmitting significant amounts of data.

As mentioned earlier, there are 6.8 billion cellular subscriptions (Figure 2). Of those cellular subscriptions, an estimated 90 percent of them are within areas with 2G coverage. (Mobile Broadband 2014) Even at 144kbit/s significant amounts of data could be transmitted through a Covert Transmission Malware System. As technology continues to improve, even greater speeds can be expected. It is projected that by the end of 2018, there will be 9.3 billion mobile subscriptions (Ericsson 2012) that could be used as part of a Covert Transmission Malware System. This means that in 2018 there will a possible 9.3 billion mobile devices that could potentially be infected with malware.

Chapter 4: Espionage

According to Military Intelligence Section 5, espionage is “non-public information gathered through covert means.” (MI5 2013) When talking about espionage we need to address two types: traditional espionage against governments and industrial espionage against organizations. Both can use similar methods to ascertain information. Understanding how information is stolen is critical to successful counterintelligence or the protection against espionage.

State Espionage

Director of National Intelligence, James R. Clapper reports that in 2014 “cyber-attacks, cyber-espionage; and counterintelligence have surpassed Terrorism” (Office of the Director of National Intelligence 2014). This report highlights the concerns the US Intelligence Community (IC) has in regards to threats directed at the US. These threats and dangers grow progressively worse as more information is migrated to the Internet and digital media.

Currently the top three countries with the best signals intelligence are the United States, Russia, and China. Signals intelligence is the practice of collecting intelligence from communication and Information Systems. (National Security Agency 2014) In addition to the ability to collect data through signals intelligence, China is considered the FBI’s “highest counterintelligence problem.” (Smith n.d.)

As will be shown, the Covert Transmission Malware System has potential to be used for both traditional and industrial espionage. In the past one of the main concerns of espionage was getting that information out without revealing the spy or source of that information. Obviously "espionage is inherently clandestine … and, in many cases illegal and punishable by law". (Espionage n.d.) Using a Covert Transmission Malware System essentially allows for anonymous collection of stolen information.

Industrial Espionage

The idea of the Covert Transmission Malware System was initiated by the intelligence community. Its application and risk as part of industrial espionage is a real threat. It is estimated that theft of proprietary information and technology by the Chinese in the US alone costs US corporations close to $2 trillion. (InfraGard 2014) Worldwide "industrial espionage costs the US on average approximately $200 billion annually". (White n.d.) I. C. Smith, a retired agent of the Federal Bureau of Investigation, believes that "the Chinese are less interested in targeting the FBI, CIA, NSA, etc. for recruitment than they are in simply obtaining as much industrial and scientific information as possible to aid in developing their industrial and military capabilities." (Smith n.d.) The Chinese are not the only nation states practicing industrial espionage. Any country not allied to the US, acknowledging western law, practice industrial espionage.

One of the greatest risks to industries is what the Senate Select Committee calls Trusted Insiders. Studies have shown that "30 to 50 percent" (Anderson 2012) of security

breach incidents are caused by Trusted Insiders. There are two main types: ignorant or misinformed and malicious.

The first group, ignorant or misinformed insiders, consists of individuals who simply are "moving, sharing, and exposing sensitive data in order to do their daily jobs." (Symantec 2013) With the current trend of "Bring Your Own Device" (BYOD), industries are struggling to implement security on all these private devices. A recent article by the International Data Group reported that over 55 percent of respondents used private devices to view work related information. (International Data Group 2012) Many of these insiders are simply ignorant of the risks related to the sensitive data and technology they are using. They have no true intent to do harm to the company or organization. It is commonly known that the greatest risks to information security are the human resources that access them.

Malicious individuals, the second group, are those who intend to "exploit their access to compromise vast amounts of sensitive and classified information." (Office of the Director of National Intelligence 2014) Usually this malicious group also can be further broken down into two sub groups. The first are those who will receive financial gain by stealing industrial information. The second are those who have a social agenda that will be furthered by the stolen information.

A Covert Transmission Malware System could be used to transfer any digital data collected, either from ignorant users or the malicious. For the purpose of this paper and in relation to the proof of concept device, we will limit the methods of collection to a

single device that could be essentially “dead dropped,” never to be retrieved again. This type of action would realistically only be used by the malicious type of user. However because of new technology, a classic “dead drop” isn’t necessary but can be done.

Dead Drops

In the world of espionage, dead drops have been a very popular and successful method of transferring information without having direct contact. Indeed, forms of dead drops have been used throughout history. As technology improves, they become more sophisticated, but the concept is the same. One of the flaws with a traditional dead drop is the signal communicating that a drop has been made and information is ready for pickup. The Covert Transmission Malware System eliminates the need for a signal or handler to pick up the information.

The Federal Bureau of Investigation (FBI) classifies a dead drop as “a ‘container’ not easily found… that should be possible to approach and fill or empty but not easily observable.” (Examiner 2012) This method allows the exchange of information without requiring any actual physical contact with each party. Even with the elimination of interaction with each other, “both parties have to be in the same geographic area.” (Kumar 2012) The dead drop eventually needs to be retrieved and often all parties risk capture or identification if the location has been discovered by authorities.

Figure 6: Hollowed Out Rock (Rynolds 2006)

Figure 5: 1948 Alger Hiss Hollowed out Pumpkin (Finin 2006)

Some of the more well-known dead drops include microfilm in hallowed out pumpkins and rocks, dead animals, and portable toilets as seen in Figure 5 and 6. Dead drops could be as simple as "dropping a universal serial bus (USB) device in the woods" (Kumar 2012) However, with each of these, all information still needs to be retrieved-- carrying an inherent risk.

In more recent times dead drops have changed in form but still have the same flaw--the data still needs to be picked up. In the case of the hollowed out rock, the handler was caught in the act of collecting the data. More modern forms of dead drops make use of cyber cafés. In these instances the "person holding the information simply needs to pretend to be using the café all the while using peer-to-peer networking to communicate information to someone who could simply be driving by." (Kumar 2012) In recent news, terrorists have been using a digital form of dead drops by creating a free

email account and then saving draft messages to communicate the desired information. With the recent popularity of Global Positioning System (GPS) and geocaching, it has been suggested that a dread drop could be "disguised if placed near an innocent geocache site." (Dead Letter Drops and Geo Caches 2014)

Covert Communication

You can break communication channels down into two basic types: overt and covert. Overt channels are channels that operate within designed channels. Covert channels are "communication channels that exists, contrary to its design" (Moskowitz 1994) meaning the design of the original system. This definition has not changed significantly since the start of the digital revolution. In 1983 the US Department of Defense classified covert channels as any transfer of information that violates the system's security policy. (Defense 1983)

All channels of communication have certain characteristics, and covert channels are no different. Creators of covert channels need to consider three things according to Renaud Didou: capacity, noise, and transmission mode. (Didou n.d.) Capacity refers to the amount of information that can pass through the covert channel at any given time. Noise refers to the types of interference that affect the information. Transmission mode is either synchronous or asynchronous. Synchronous is constant transmission. Asynchronous is when a transmission is made intermittently. Covert Transmission Malware System is asynchronous because we never know when the next infected mobile device is going to enter the range of the passive device.

It is important to understand the purpose of covert channels. Covert channels obfuscate identities, circumvent security features, and are designed to be hidden or concealed. Each one of these purposes adds to the successfulness of the covert channel. If any one of these purposes is missing, it will endanger the others. If identities are known, they can be watched and tracked. If the channel does not circumvent security features, the whole purpose of a covert channel is defeated. Lastly if security features have discovered the channel, security professionals can follow the data to the various suspects.

Obfuscation of Identities

Generally covert channels are used for purposes that are not in compliance with the policy and procedures of an organization. For this reason the users of covert channels do not want to be identified. A successful covert channel not only masks the identities of its users but also their relationships. (Dingledine 2004) If successfully done, even when the channel is discovered there would not be collateral evidence collected.

Covert channels are put into place to keep the sender and receiver independent of each other and to eliminate any possible connection between the two. Raymond Sbrusch, in his 2006 SANS paper "Network Covert Channels: Subversive Secrecy," mentions the use of "anonymity sets." This refers to the set of total individual subjects that can be used in transmission or reception of the covert message. As the membership in the sets increases, it becomes more difficult for the covert channel and its real participants to be discovered.

Circumvent Security

Security policies are implemented to protect proprietary information and resources. Covert channels are generally used to subvert and avoid those policies. It is also important to note that not all covert communication is malicious in nature. Sabastian Zander notes that “often even ordinary employees use covert channels to bypass their company firewalls in order to access Internet resources.” (Zander 2007) In countries where there is government censorship, covert channels are used to access prohibited Internet sites.

Concealed

As the name implies, covert channels are meant to be concealed. This might be the most important of the three purposes of covert channels. Both obfuscation and circumventing security are dependent on the channel being hidden. Once the channel is detected, significant resources can be put into closing it and identifying involved parties.

Covert channels should not be confused with encrypted communication. Covert channels can be encrypted, but not all encrypted communication is covert. Encrypted communication simply prevents unauthorized reading of information. One of the main purposes of a covert channel is to keep the communications concealed, which has nothing to do with encryption.

Covert Countermeasures

Security professionals need to always be vigilant about interactions in their networks. Security measures need to be taken to prevent not only threats from the outside from getting in, but also internal threats trying to get information out. Covert channels are one of those threats that will never go away. Many researchers believe that "covert channels cannot be completely eliminated" (Moskowitz 1994) but only reduced.

Detection of covert channels is difficult. Research into countermeasures "shows that industry products still lack methods to deal with covert channels." (Zander 2007) Security professionals are generally always playing catch up when it comes to intrusions in their systems; covert channels are no different.

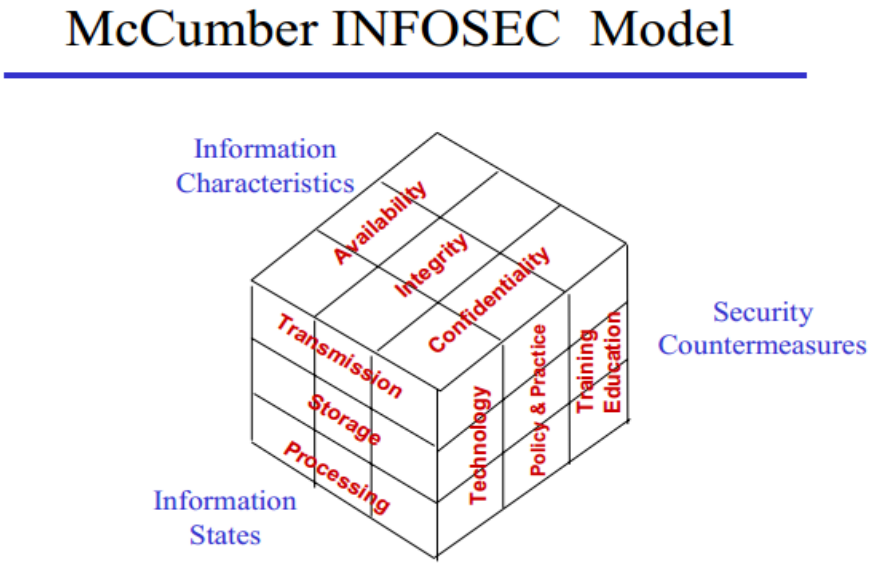

Figure 7: McCumber Cube

In 1991 John McCumber created an information systems security model named the McCumber Cube. (Figure 7) It is a concise breakdown of the information systems security discipline. (W. Victor Maconachy 2001) Following this model will help protect information systems against unauthorized access or modification and ultimately help detect and counter threats against the information system.

While all points on the McCumber cube are important, within the scope of the Covert Transmission Malware System, we will focus on the three Security Countermeasures: Technology, Policy and Practices, and Training and Education.

Technology portion of the McCumber model comprises hardware and all software that the system uses. They include any devices, components or programs that help secure the information system. These different technology defenses help protect information systems but do not have the overreaching effect into private mobile devices. While there are host based security features on mobile devices, they are not very effective. As long as the Covert Transmission Malware does not interact with the information system, its defense technology would not detect it.

Policy and Practices are very important in securing information systems. Again if those policies and practices do not include private devices then their effectiveness is limited. Many policies do not limit where applications can be acquired, leaving mobile devices open to grey markets. Most organizations are really good at basic security including patching and updating their systems; this basic security has been reflected in the mobile

devices that are used. Often times the newest update happens when the employee gets a new device, generally every two years.

Policies and Practices do not cover mobile devices as effectively as standard computer systems. Many policies allow employees to bring their own devices – indeed, many employees demand it. Organizations are not always able to implement security on private devices.

Lastly Training and Education is important in securing information systems. Security is only as good as the people operating the systems. They need to have a higher level of awareness, literacy, training and education in sound security practices for systems to be secure. (W. Victor Maconachy 2001) Most failures in security are based off of employees clicking, accepting or opening malicious items. In relation to personal devices, training is one of the most important aspects to device security. Oftentimes owners are the only individuals in charge of device security, so training can bring awareness to mobile device security needs.

There are many methods to reduce covert channels. According to Sabastian Zander, the best methods are host security, network security, and traffic normalization. Each one of these methods helps security specialists detect traditional covert channels that run through their own internal networks. These methods; however, may not be able to detect a Covert Transmission Malware System due to its use of mobile broad band.

Chapter 5: Malware

What is Malware?

There are many different definitions of malware. For this paper, the definition used is from Microsoft:

Malware is short for "malicious software." Malware is any kind of unwanted software that is installed without your adequate consent. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware. (Microsoft 2014)

The key takeaway from this definition is “unwanted software that is installed without your adequate consent.” Most malicious software installs without user knowledge. The nature of shadier malware is buried in the fine print and generally over-simplified. Oftentimes users are fooled into using software that have sneaky end-user license agreements (EULAs). The possibilities of acquiring malware or shady applications (apps) are increasing as people download more apps onto their devices. In 2013 the average

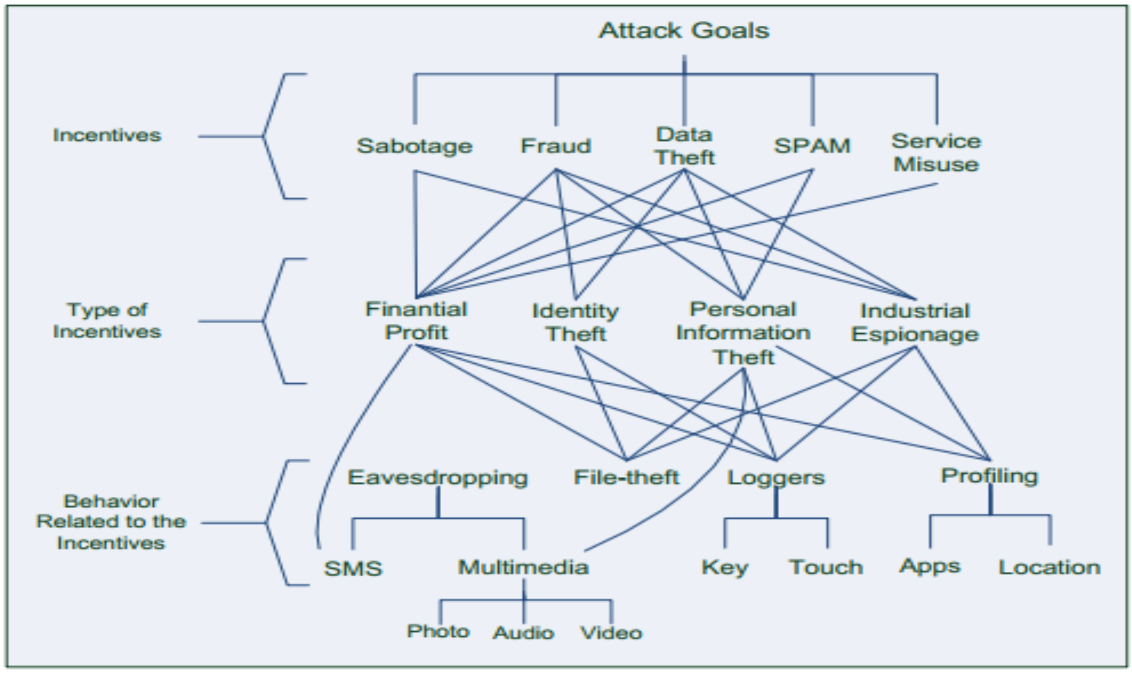

Figure 8: Malware Attack Goals

number of apps per devices increased from 32 to 41. (Suarez-Tangil 2013)

Often malware is divided into groups depending on their attack goals. Figure 8 is a visual representation of these attack goals and how they are broken down. This is done to better help understand how they work and how they might interact with various systems, ultimately leading to methods for detecting them. The attack goals are "sabotage, fraud, data theft, spam, and service misuse." (Suarez-Tangil 2013) The Covert Transmission Malware System would bring those attack goals up to six.

Protection from Malware

As the use of technology rises and malware becomes more prevalent, the question of how can we protect our devices always arises. This question is difficult to answer, because there is no clear solution. Because of the variety of devices, operating systems, and environments, no device will ever be 100 percent protected from malware.

The two main security models for mobile devices are market protection and platform protection. Both models offer advantages and disadvantages and, in most cases, they are used in tandem. While these models are a good start, they are not capable enough to protect devices completely. Ultimately users need to become better educated and aware of their devices and how they should be working.

Market Protection

Market protection is also commonly known as the "Walled-garden model." (Suarez-Tangil 2013) The idea behind this model is that protection is provided by secure

markets that prevent bad apps from getting into the market place. Ideally when market protection is in place, users will be able to download any app from the market without concern or worry that it might contain malware.

This model is time-consuming and expensive to successfully employ. Apple is the main company that employs this market protection. Every app that is published and sold on iTunes has been vetted and approved by Apple before becoming available to the public. All Apple devices by default can only obtain apps from iTunes, which makes their products fairly secure.

The Android market on the other hand attempts to employ a version of this model but less successfully. It is more difficult for Android to employ this model because of their "open nature policy and lax regulations for app developers." (Celestino, Trojanized Apps Vs. Malicious Apps 2013) In the case of the Android market, any app review or vetting is done by other programmers and users on their own time. In 2013 security researchers found over "2,500 scam apps in Google's storefront" (InfraGard - Watch Out For Malware on Android 2013) as a direct result of loose market protection. One example of malware found in Google's store front was a TOR anonymity network app which was downloaded over a million times. (InfraGard - Android malware using TOR Anonymity Network Makes a Debut 2014) This app waited until the phone was charging and then began mining bitcoins for the publisher of the app. (InfraGard - Hidden Crypto Currency-Mining Code Spotted in Apps on Gogle Play 2014) It should be noted that hidden in the EULA was permission for the publisher to use the phone in such a way.

One of the main problems with the market protection model is the limited offerings and the cost of those apps. Many people using all devices look for apps on gray markets, significantly raising their chances of malware infections. Often times these people are looking for free methods to acquire paid apps. It was found that “100 percent of the top paid apps on Android and 56 percent on iOS were being impersonated in a compromised form on gray markets.” (InfraGard - Beware of Counterfeit Versions of Top Android, iOS Apps 2013) Secondary market users significantly increase their chances of encountering malware.

Platform Protection

The platform protection model revolves around the idea that protection needs to be at the device level. This model uses a number of methods to protect the device including permissions, sandboxing, and remote management. While these are not the only methods for protection, they are the most active methods.

Permission-based protection is initiated at installation of apps on devices. When an app is installed, it gives a list of components that it will access and asks permission to use those components. Essentially it is trying to restrict apps privileges. Apps can ask for any privileges whether they need those privileges or not. If a user wants to use the app, they will grant permission in an all or none scenario. This type of protection has been “proven patently insufficient” (Suarez-Tangil 2013) because users don’t understand what they are agreeing to and really don’t care.

Current trends in permission-based protection are not focused on fixing this broken method. One solution proposed by Peter Hornyack was to provide “fake data” (Peter hornyack 2011) to applications that demand more access than they should. While this helps protect private information, it does not not protect the overall system. The intent of a Covert Transmission Malware System is to use the hardware to transfer “other” data and not private information from the device. This type of protection does not stop Covert Transmission Malware.

Mobile operating systems have been designed to essentially sandbox apps. This method of protection keeps apps from communicating with each other. The idea is that different apps will not interact with each other creating exploits or exploiting the system. This type of protection works well in most instances. However some malware have been found to skirt this type of protection by going under the operating system to the hardware level where sandboxing is not employed.

Within Android devices there are a number of known covert channels that applications can use without user permission that circumvent the sandboxing. These types of covert channels usually use hardware such as vibration and volume to communicate between applications. (Hill 2013) While it is possible to detect these types of covert channels, many of the detection methods are dependent on uncompromised operating systems. Many of these channels can only be detected if the host device has security software that has control over all processes.

Remote management protection is not true protection but post-infection-protection. Remote management allows either service providers or manufacturers to remotely remove or fix the malware after it has been discovered. It is not on-the-fly protection but an after-the-fact protection. This type of protection is important, but users risk their private information depending on how service providers and manufacturers use that information.

Mobile Platforms and Malware

Malware is designed and generally dependent on the operating system. Of the many operating systems for mobile devices, this paper discusses Google's Android and Apple's iOS. These two operating systems comprise close to 94 percent (Dilger 2013) of the mobile device market. Because of the nature of malware and its purposes, the largest markets are generally hit the hardest.

As of the third quarter of 2013, Google's Android operating system controlled 81 percent (Dilger 2013) of the mobile market. Because of the nature of the Android operating system and its market place, malware creators have had great success infecting devices and finding ways to exploit those devices. Organizations allowing the use of Android devices are having an incredibly difficult time protecting all the possible systems.

One of the most important preventative malware measures is updating operating systems. It has been estimated that over a third of all Android Devices have not been updated since February 2011 and a quarter since December 2011. (Fung 2013) These updates are usually issued by the service provider. Figure 9 gives breaks down current Android versions on the market. Once a device is no longer being supported by the service provider, the chance that it will be updated is close to zero.

Version	Codename	API	Distribution
2.2	Froyo	8	1.1%
2.3.3 - 2.3.7	Gingerbread	10	17.8%
3.2	Honeycomb	13	0.1%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	14.3%
4.1.x	Jelly Bean	16	34.4%
4.2.x		17	18.1%
4.3		18	8.9%
4.4	KitKat	19	5.3%

Figure 9: Versions of Android's Operating systems

Apple's iOS is the second most used operating system with about 12.9 percent of the market. (Dilger 2013) It has been growing because of the innovation and quality of the mobile devices that Apple produces. Apple's iOS happens to be more secure due to its stringent app requirements; however, security is seldom the reason for its purchase by the general public. Even with all the security features that iOS has, there are ways to jailbreak and unlock those devices allowing apps from grey markets to be installed. As Apple products continue to grow in popularity, more malware will be written for them.

Malware into the Future

Malware will never disappear in the future. As long as it is profitable to steal information, people will write code to steal it. Everyday more information is transferred to the Internet and digital media and illegitimate methods to acquire that information increase.

Figure 10 shows the Top Threat Type Distribution. These are the most frequent types of malware active today. Premium Service Abusers is malware that upgrades the types of services that mobile devices have allowing them to charge more for those services. It is a very easy form of malware to create and is generally very profitable. Data stealers are the second most common form of malware and their purpose is to acquire as much

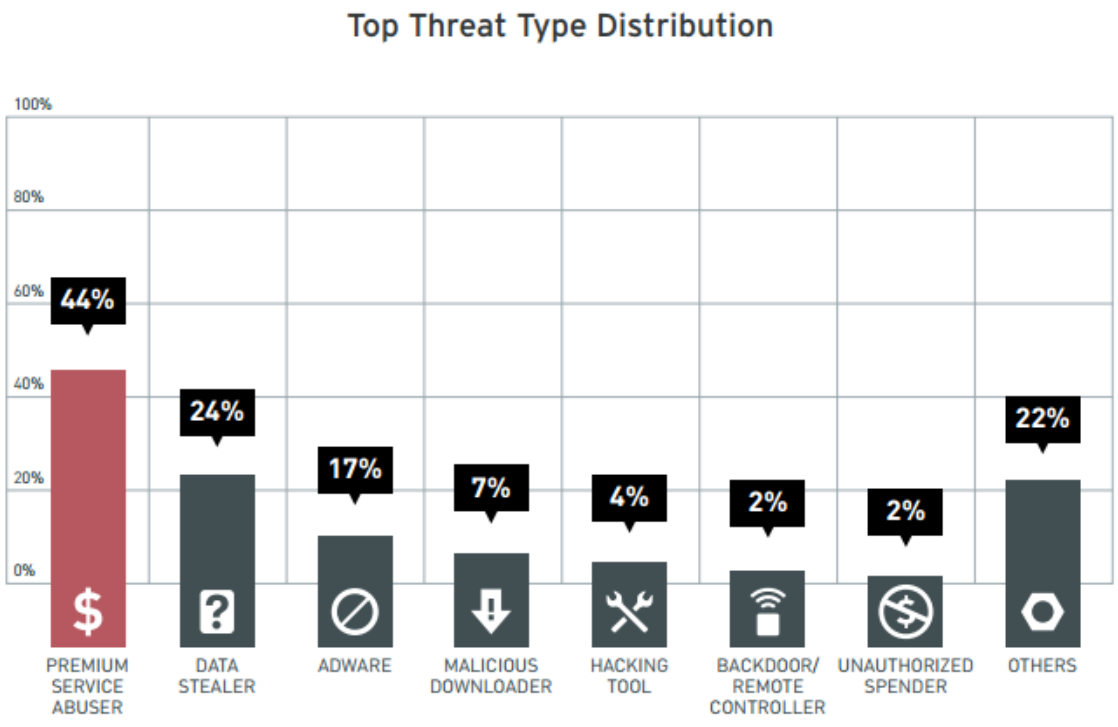

Figure 10: Top Threat Type Distribution (Trend Micro 2013)

private data as possible. They collect such data as credit card and social security numbers, and generally any information that might lead to financial gain.

A Covert Transmission Malware System currently would fall under the “other” category but as it increases in use it will likely become its own category.

Where malware will go in the future is difficult to predict. Implementation of digital security for the most part is in response to intrusions and exploits. Writers of malware programs are creative and many program as a career and also as a hobby. The only things that limit malware are current technology and the creative ability of the writers. Malware is so unpredictable that it is impossible to be 100 percent protected.

Future malware will be more capable because of improvements in technology--both as mobile devices become more powerful and as broadband speeds increase. 5G mobile broadband with speeds of 1Gbps are estimated to be available in 2021. (Freeman 2014) Recently it was announced that Wi-Fi with speeds of up to 10Gbps will be available in 2015 (Quantenna Communications 2014). The increases in power and speeds will open even greater vectors for malware to enter.

Chapter 6: Covert Transmission Malware System

Overview

The Covert Transmission Malware System is a data transmission system which allows mobile data communication from one point to another through infected broadband mobile devices. Historically malware attack goals have fallen under one of five different attack goals: “sabotage, fraud, theft, spam, and service misuse.” (Suarez-Tangil 2013) The Covert Transmission Malware System would bring that list up to six with covert transmissions. The main goal of a Covert Transmission Malware System is to allow the transmission of data not only anonymously but over unsuspecting third-party broadband devices. Similar to a bot net, significant amounts of data could be retrieved without physical interaction by the originating party, given enough infected devices.

In May 2013 an Android Trojan by the name of “NotCompatible” was discovered out in the wild. (Lookout 2012) NotCompatible infected phones turning them into a basic TCP relay/proxy. They were then used to transfer encrypted “adult content” between websites. (ThreatTrack Security 2013) This Trojan is a poor example of transmission malware being used by criminal organizations. It was very basic and easily discovered. While this is closely related to the Covert Transmission Malware System, it is only half of the system and truly does not live up to the total potential.

Application Scenario

A government organization “A” is attempting to document all individuals entering and leaving a facility of interest. To capture images of those individuals, a passive system has

secretly been set up in a nearby location with a view of the entry point. At various times of the day, activated by a motion sensor, the system takes snap shots of individuals. The hidden system cannot be retrieved and does not have a consistent static network connection. In addition, if the device is discovered, the original organization wants complete anonymity regarding its origins and how the device communicates with them.

Employees entering and leaving the facility temporarily pass within the vicinity of the passive device. Their mobile devices previously infected with malware become active around the passive device's location. This malware infects the mobile device by a previously downloaded application. The malware activates its Wi-Fi, Bluetooth, or near field communication (NFC) modules. Once active, the mobile device sends an encrypted

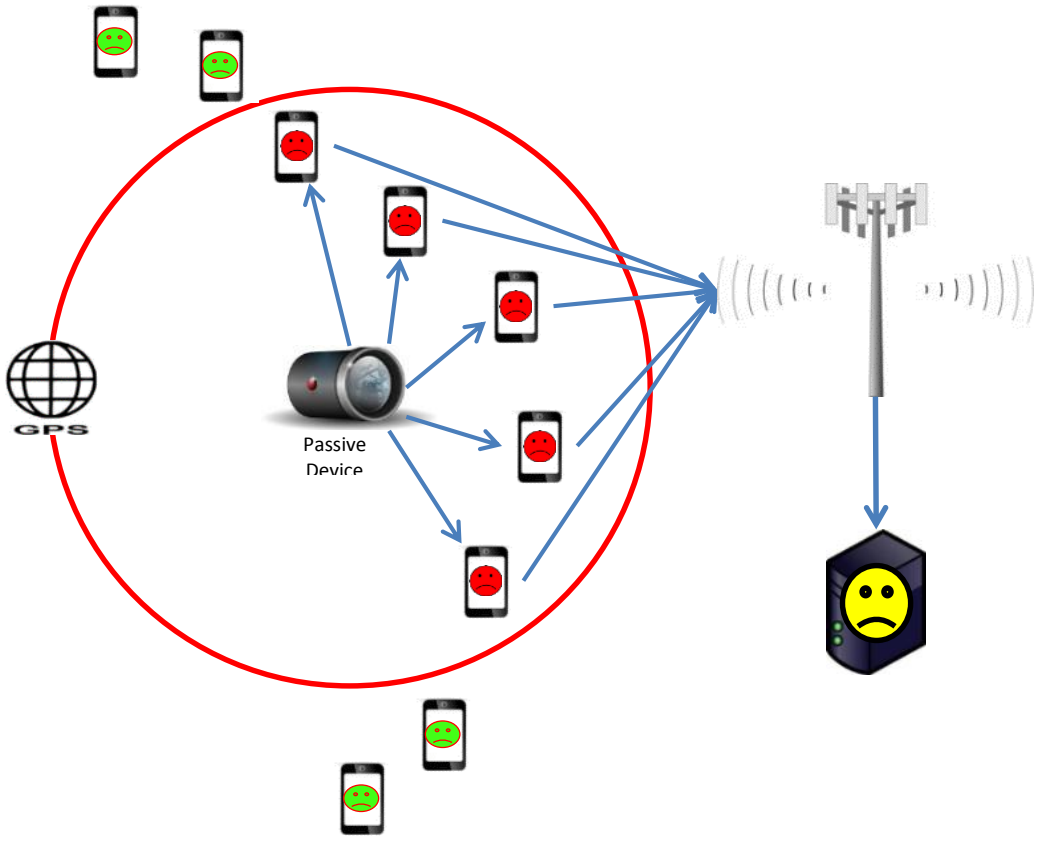

Figure 11: Covert Transmission System.

Green frowny faces are non-active infected devices; red ones are active infected phones

transmission code to the passive device, instructing it to send a small encrypted portion of its data payload. The passive device sends its payload using the infected device's mobile broadband to the collection server.

Each time an infected mobile device nears the passive device small encrypted portions of the data are sent to the collection server to be pieced back together into completed files. With enough infected mobile devices, significant amounts of data could be transferred out of secured areas with minimal risk of discovery and no risk of a real life asset being captured. A visual representation of this process is found in Figure 11. Gina Fisk calculated that with just one covert bit of data per packet, a website could lose over 26GB annually. That amount of data grows exponentially as more potential devices are infected.

Components of the Covert Transmission Malware System

The major components of the Covert Transmission Malware System are the Covert Transmission Malware (CTM), the infected mobile device, and the passive device. Within the mobile device, the malware can take control of a variety of components. These malware controlled components could be the GPS, wireless components, and the device's data plan. The passive device could be any covert tool that collects data and is capable of wireless access.

Covert Transmission Malware

Within the Covert Transmission Malware System the key component is the CTM. It is through this malware that the entire Covert Transmission Malware System is capable of being a threat. Within this section, the CTM and its characteristics will be discussed.

The method of infection is important to creating an undetectable CTM. In many instances, malware is added to legitimate apps and then downloaded through shady markets that cater to jail-broken and unlocked devices. To reach the most users, with the lowest possibility of detection, the CTM would need to be built into or updated into an original popular app. How to write a popular app is outside the scope of this project; however, a nation state with enough resources could write an app that would be desirable enough to gain the mass distribution and maximize effectiveness.

Malware operating as a method of covert transmission needs to be virtually undetectable. To have the lowest possibility of detection and raise the least suspicion, the app needs to have a number of possible characteristics and abilities, including GPS coordinates, reasons to be near passive devices, in-app updates, the ability to remove malware components, and a use agreement that permits access for these abilities. Dead Drop, a popular game on iTunes, incorporates some of these characteristics. According to the description “Dead Drop is a live-action multiplayer elimination game played by

groups of friends in and around their communities." (TinkerTailor 2012) It incorporates all of the components that could make a CTM.

A potential CTM app should have GPS coordinates. These GPS coordinates would help disguise the real passive device locations. A popular growing activity is geocaching. Geocaching is where individuals hunt for hidden items or locations using GPS coordinates. Having a geocaching component would deflect suspicion of passive device coordinates within the infected device. While geocaching will entice certain people, to get the popularity needed, more incentives are needed. To get the initial app subscription and acceptance, money or prizes might be necessary with a possible social aspect to the game.

In-app updates are important to help avoid detection. The initial app would not contain any portion of the malware code. Only when certain conditions were met would the malware download and activate. Having those conditions connected to the GPS location and or network-based geolocation would prevent security professionals from detecting the malware in lab environments. The in-app updates would also allow for continued dead drop location updates.

Along with in-app updates, the ability to remove the malware and its components is important. This could be an automatic command that takes place once a device is no longer near a passive device. If a passive device is discovered, all connection or references would be removed from the mobile devices.

All apps have use agreements that each user accepts in order to install the software. Most people do not read or understand what these agreements are requiring. For example most apps don't need access to a person's contacts list or their text messages but could easily include that in the EULA. In addition to the use agreements, most people do not read the Terms of Service, privacy policy, and deletion policy that could allow further access to their device. These legal agreements would need to be written in such a way that would not draw suspicion.

Infected Device

Another key component of the Covert Transmission Malware System is the mobile broadband devices that will be used to transfer data. Ideally any mobile device that has broadband could be used. Because of CTM's reliance on GPS, any device without this ability would never have the malware component installed. Of all mobile device manufacturers, Apple is the most stringent at vetting apps in the iTunes store. For this reason, the Covert Transmission Malware System would be based around the Android and Windows Phone mobile operating systems.

GPS

As mentioned before, the CTM is reliant on knowing its location in order to contact the passive device. Mobile device locations can be calculated by two main methods: network-based geolocation and GPS. Both methods could be used by the CTM; however, GPS is the least resource-intensive method currently.

In the past, network-based geolocation resulted in only a general location. Matt Blaze, a cybersecurity researcher, testified before the House Judiciary subcommittee that this is no longer the case. He said that with the "increasing specificity as cellular sectors become smaller... it could identify a floor or even a room within a building." (Blaze 2010) This type of calculation occurs by the service provider and would not only be extremely difficult for the mobile device but resource intensive. Network-based geolocation would not be a practical method for the CTM.

GPSs are now starting to come standard on most mobile devices. GPS in mobile devices are accurate to within three meters. (U.S. Government 2014) This makes it an ideal method of calculating location. A potential method of detection could be the activation and deactivation of the GPS by the CTM.

Wireless Capabilities

Mobile devices often have multiple forms of wireless. These can include Wi-Fi, Bluetooth, infrared, and near-field communication (NFC). Any one of these forms of wireless could be used to communicate with the passive device. However, both Bluetooth and Wi-Fi can have a reach of up to "300 feet" (Romanov 2012) making them both possible vectors of transmission.

Broadband

Many mobile broadband subscriptions have data limitations. The Covert Transmission Malware System would limit how much data was transferred at any given time period

per infected device. Even if the device's owner scrutinized data usage, covert data could be appended to overt packets making it near impossible to detect. It could even be feasible to check data logs on infected devices to guarantee that the Covert Transmission Malware System is not drawing attention to its actions.

Passive Devices

Passive devices that could be used in a Covert Transmission Malware System are truly limitless. In this proof of concept, a Raspberry Pi Model B with a simple camera and USB Wi-Fi dongle was used. The size of this proof of concept is significantly larger compared to other espionage-like devices, about the size of a credit card. The type of passive device used would depend on the complexity of the data collected. The complexity of the passive device would depend on how many other systems it might be interacting with.

Simple audio or video recording devices like our proof of concept could be deployed anywhere without much difficulty. These types of devices have a lower risk of being detected because of the benign nature of their collection. Low risk passive devices like this are not very complex.

Within the appendix the components and programing are found that were used to create the proof of concept passive device. The passive device is not a true passive device but mimics how it would work; it is constantly on and looking for a specific Wi-Fi SSID. Once that Wi-Fi SSID is found in range, it connects and starts sending the captured images.

The system used a free program called Motion to monitor the percentage change in pixels from the camera. When it detected pixel changes, it captured the images. Motion is capable of not only taking pictures but also video. While not a true motion detector it worked very well capturing pictures.

Every two minutes a program called ZipandMail runs. ZipandMail first checks to see if there are any captured images. If captured images are found it then divides those images into folders of 20 images apiece. Once the images are divided the separate folders are zipped and emailed to a test email address. Encryption can be used during the zipping and email phase of the passive device operation.

A freeware email client called Mutt is used for mailing the captured images. Mutt is a Linux based command line email client. It is capable of sending and receiving emails along with adding attachments with the help of an SSMTP client.

A more complex type of passive system would be capable interacting with computers and networks. Connecting these systems to secured networks carries more risk to the asset planting them, but is still within the realm of possibilities. A recent article in CT Magazine discussed a proof of concept malware mouse that was capable of downloading trojan software to the host machine. (Benchoff 2014) A modified mouse could very well be capable of searching the host machine for specific data and then transmitting it out via a Covert Transmission Malware System.

To test the proof of concept, a hollowed out book was employed to hide the passive device (Figure 12). It was hidden on a book shelf during the defense of this thesis. As

committee members entered, it documented their movements. Every two minutes, it transmitted captured pictures through a mobile broadband device.

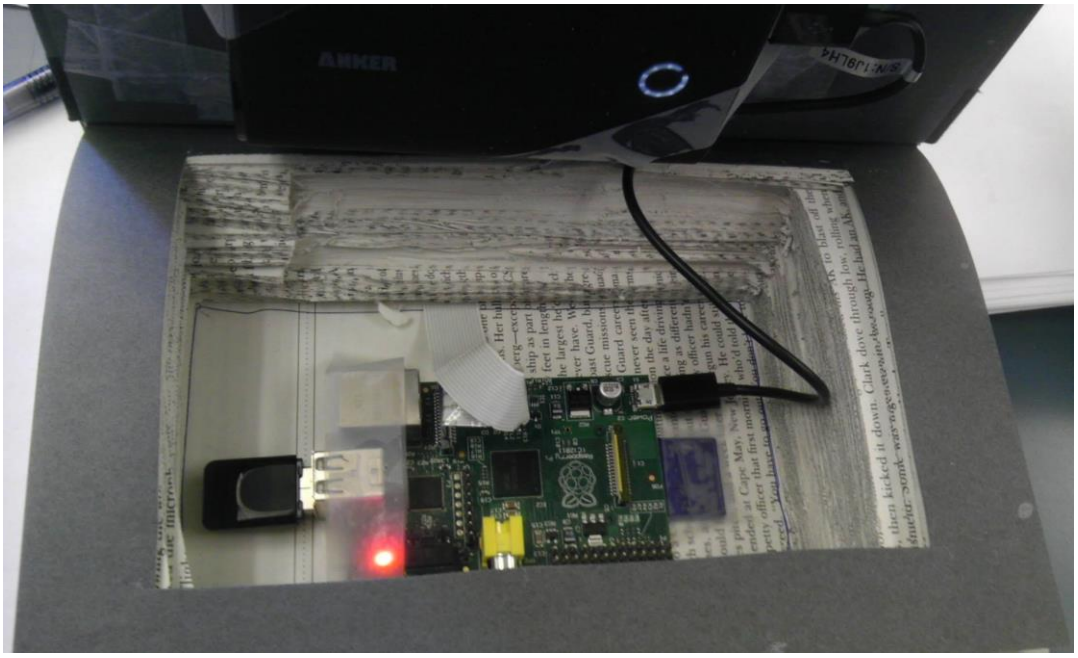

Figure 12: Passive Device

Chapter 7: Future Research

Future research for the Covert Transmission Malware System would be focused on a better proof of concept, additional research in current malware similar to the Covert Transmission Malware System and methods of detection and prevention. Currently the proof of concept centers around the dead drop; a benign form of the Covert Transmission Malware that incorporates characteristics described within this paper would help explain possible dangers. Further analysis of the Malware NotCompatible, as a very simple precursor to the Covert Transmission Malware, would also be beneficial to the next generation. Finally since detection and prevention are critical to safeguard data, developing a security plan to prevent and detect this type of malware is necessary.

A true proof of concept of the Covert Transmission Malware is needed to truly demonstrate the potential gain and loss from this type of malware. The malware characteristics that have been described in this paper are just the basic that it would be needed. True development of this malware and its legitimate program needs to be completed.

As a precursor to the Covert Transmission Malware, NotCompatible needs to be analyzed. Its creation and purpose is the closest to what the Covert Transmission Malware could be. NotCompatible was discovered by accident when it asked permission to install; it was disguised as an Android security update. While this allowed Notcompatible to propagate, it was insufficient to reach the majority of mobile devices.

This malwares failure's and ability to be detected need to be studied and used to prevent detection in the Covert Transmission Malware.

As security professionals, it is critical that security plans are developed to prevent data loss. A Covert Transmission Malware System on private mobile devices will be difficult to detect. Private devices are out of the general scope of corporate and government security. Finding an efficient and effective way to protect against malware transmission threats is critical in private devices.

Chapter 8: Conclusion

It is feasible that nation states or organizations could build a Covert Transmission System. Very basic forms of covert transmission malware have been found infecting mobile devices. Mobile broadband speeds permit significant amounts of data to be transmitted from one point to another through overt and covert channels. These two significant realities make a Covert Transmission Malware System a real threat to governments and industries. As the risk of data theft increases from malicious insiders and outsiders, security professionals need to be ever vigilant.

Mobile device security currently is dependent on market protection and platform protection. Market protection by way of application review cannot prevent all malware from becoming available. Furthermore shady and third-party markets do not review apps, creating potential for exploits. Platform protection mainly relies on permissions that restrict applications but are insufficient. Many malware programs take advantage of the fact that people are not aware of what their devices are doing. When a warning does pop up, oftentimes it is swiftly dismissed.

As technology advances and our mobile devices become more powerful, the potential for malware to both exploit and be detected increases. More powerful devices mean that they can transmit and process more data with out noticeable performance issues. With increased power, applications will be developed that will more successfully detect and prevent malware. These advancements are both positive and negative for a Covert Transmission Malware System.

Covert Transmission Malware Systems are a threat, and organizations need to prepare for them. Mobile devices are becoming the computing devices of choice. Failure to prepare for the age of mobile computing could result in the loss of significant amounts of information at an astronomical financial cost.

Bibliography

Airwave Management LLC. *Cell Phone Tower Statistics.* Nov 13, 2013. http://www.statisticbrain.com/cell-phone-tower-statistics/ (accessed 02 10, 2014).

Anderson, Bill. "Insider Threat the Game has Changed." *Scmagazine.* June 14, 2012. http://www.scmagazine.com/insider-threat-the-game-has-changed/article/245759/?DCMP=EMC-SCUS_Newswire (accessed May 5, 2014).

Audio Surveillance Ghost Transmitter. 2013. http://www.gcomtech.com/ccp0-prodshow/audio-surveillance-ghost-transmitter.html (accessed Feb 24, 2014).

AUDIOJAVA. *Scheduled webcam motion detection surveillance with auto-email feature using Raspberry Pi (Arch Linux).* 12 28, 2013. http://codrspace.com/audiojava/scheduled-webcam-surveillance-using-raspberry-pi-arch-linux-/ (accessed 04 01, 2014).

Benchoff, Brian. *Malware In a Mouse.* Mar 30, 2014. http://hackaday.com/2014/03/30/malware-in-a-mouse/ (accessed Mar 30, 2014).

Bidou, Renaud. "Covert Channels." *iv2-technologies.* n.d. http://www.iv2-technologies.com//CovertChannels.pdf.

Blaze, Matt. *Hearing on ECPA Reform and the Revolution in Location Based.* Testimony, Washington DC: House Committee on the Judiciary, 2010.

Blue Coat. *How Users Drive the Mobile Threat Landscape.* Blue Coat Systems, 2013.

Boyle, Greg. "Only 20% of Android Mobile Device Users Have a Secuirty App Installed." *http://fearlessweb.trendmicro.com.* May 07, 2012. http://fearlessweb.trendmicro.com/2012/misc/only-20-of-android-mobile-device-users-have-a-security-app-installed/ (accessed Dec 20, 2013).

Celestino, Oscar. *Mobile Apps: New Frontier for Cybercrime.* Tredn Micro, 2013.

—. *Trojanized Apps Vs. Malicious Apps.* 2013. http://about-threats.trendmicro.com/us/webattack/119/Mobile%20Apps%20New%20Frontier%20for%20Cybercrime (accessed 09 20, 2013).

Coat, Blue. *How Users Drive the Mobile Threat Landscape.* Blue Coat Systems, 2013.

Covert Channel Signals for Meetings or Dead Letter Drops. 2014. https://p10.secure.hostingprod.com/@spyblog.org.uk/ssl/ht4w/covert-channel-signals-for-mee.html (accessed Feb 24, 2014).

Dead Letter Drops and Geo Caches. 2014. https://p10.secure.hostingprod.com/@spyblog.org.uk/ssl/ht4w/dead-letter-drops-and-geo-cach.html (accessed 10 24, 2013).

Defense, Department of. "Department of Defense Trusted Computer System Evaluation Criteria." *Department of Defense Standard.* Aug 15, 1983. http://csrc.nist.gov/publications/history/dod85.pdf (accessed 02 28, 2014).

Department of Defense. *Trusted Computer System Evaluation Criteria.* Washington DC: DoD USA, 1985.

Didou, Renaud. "Covert Channels." *iv2-technologies.* n.d. http://www.iv2-technologies.com//CovertChannels.pdf (accessed 02 28, 2014).

Dilger, Daniel Eran. *IDC data shows 66% of Android's 81% smartphone share are junk phones selling for $215.* Nov 12, 2013. http://appleinsider.com/articles/13/11/12/idc-data-shows-66-of-androids-81-smartphone-share-are-junk-phones-selling-for-215 (accessed Mar 20, 2014).

Dingledine, Roger. "Tor: The Second-Generation Onion Router." *Torproject.* 2004. https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf (accessed 02 28, 2014).

Elkins, Michael R. *The Mutt E-mail Client.* 03 26, 2014. http://www.mutt.org/ (accessed 04 05, 2014).

Ericsson. *Ericsson Mobility Report.* Industry , Douglas Gilstrap, 2012.

Espionage. n.d. http://en.wikipedia.org/wiki/Espionage (accessed 12 20, 2013).

Examiner. *Common Russian spy techniques and tradecraft shown in FBI release of videos.* may 22, 2012. http://www.examiner.com/article/common-russian-spy-techniques-and-tradecraft-shown-fbi-release-of-videos (accessed 10 23, 2013).

Finin, Tim. *Bluetooth Spy Rocks Replace Pumpkins.* Jan 28, 2006. http://ebiquity.umbc.edu/blogger/2006/01/28/bluetooth-spy-rocks-replace-pumpkins/ (accessed 10 26, 2013).

FireTalk. *FireTalk Legal.* A. V. M. Software. 12 09, 2011. http://www.firetalk.com/Home/Legal (accessed 04 05, 2014).

Fisk, Gina. "Eliminating Steganography in Internet Traffic with Active Wardens." *www.Woozle.org.* Oct 2002. http://www.woozle.org/~mfisk/papers/ih02.pdf (accessed 02 28, 2014).

Freeman, Angela. *A Look Into the Future: 5G Network Speeds and When They'll Arrive.* Mar 8, 2014. http://tech.co/look-future-5g-network-speeds-theyll-arrive-2014-03 (accessed Apr 17, 2014).

Fung, Brian. "How Zombie Phones Could Create a Gigantic, Mobile Botnet." *National Journal*, 2013.

Guillermo Suarez-Tangil, Juan E Tapiador, pedro Peris-Lopez. *Evolution, Detection and Analysis of Malware for Smart Devices.* IEEE, 2013.

Hill, Raquel. "Quantifying and Classifying Covert Communications on Android." *Springer Science+Business media*, 2013: 79-87.

Information Telecommunication Union. "ITU Facts and Figures 2013." 2013. http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf (accessed 04 2, 2014).

InfraGard - 2014 is the Tipping Point year of Mobile Malware: RSA Chief Art Coviello. *2014 is the Tipping Point year of Mobile Malware: RSA Chief Art Coviello.* 12 19, 2013. (accessed 03 29, 2014).

InfraGard - Android malware using TOR Anonymity Network Makes a Debut. *Android malware using TOR Anonymity Network Makes a Debut.* 02 26, 2014. (accessed 03 27, 2014).

InfraGard - Beware of Counterfeit Versions of Top Android, iOS Apps. *Beware of Counterfeit Versions of Top Android, iOS Apps.* 12 31, 2013. (accessed 03 29, 2014).

InfraGard - Hidden Crypto Currency-Mining Code Spotted in Apps on Gogle Play. *Hidden Crypto Currency-Mining Code Spotted in Apps on Gogle Play.* 03 28, 2014. (accessed 03 29, 2014).

InfraGard - Legitimate Apps Bundled up With Secret Bitcoin Miner. *Legitimate Apps Bundled up With Secret Bitcoin Miner.* 12 04, 2013. (accessed 03 29, 2014).

InfraGard - The mobile Zombie Botnet Apocalypse. *The mobile Zombie Botnet Apocalypse.* 11 04, 2013. (accessed 03 29, 2014).

InfraGard - Watch Out For Malware on Android. *Watch Out For Malware on Android.* 12 17, 2013. (accessed 03 29, 2014).

InfraGard. "Counterintelligence Now Riskier Than Terrorism, Intelligence Officials Report." *InfraGard.* 01 31, 2014. (accessed 03 27, 2014).

International Data Group. *How Mobility is Disrupting Technology and Information Consumption.* IDG Global Solutions, 2012.

Kemmerer, Richard A. "A practical Approach to Identifying Storage and Timing Channels: Twenty years Later." 2002. https://www.acsac.org/2002/papers/classic-channels.pdf (accessed 12 2013).

—. "A Practical Approach to Identifying Storage and Timing Channels." *Proc. IEEE Symp. Security and Privacy.*, Apr 1982.

Kumar, Mohit. *New Dead Drop Techniques Used by Security Agencies.* Nov 09, 2012. http://thehackernews.com/2012/11/new-dead-drop-techniques-used-by.html (accessed 10 26, 2013).

Lampson, Butler W. "A Note on the Confinement Problem." 01 1973. http://www.cs.umd.edu/~jkatz/TEACHING/comp_sec_F04/downloads/confinement.pdf (accessed 04 02, 2014).

Lavrsen, Kenneth Jahn. *Motion .* 02 15, 2014. http://www.lavrsen.dk/foswiki/bin/view/Motion/WebHome (accessed 04 05, 2014).

Levin, Adam. *Top 4 Ways to Keep Your Cellphone From Getting Hacked.* 01 26, 2014. http://abcnews.go.com/Business/average-person-cellphone-hack/story?id=21655340 (accessed 01 2014).

Lookout. *UPDATE: Security Alert: Hacked Websites Serve Suspicious Android Apps (NotCompatible).* May 2, 2012. https://blog.lookout.com/blog/2012/05/02/security-alert-hacked-websites-serve-suspicious-android-apps-noncompatible/ (accessed Apr 15, 2014).

Marforio, Claudio. *Analysis of the Communication between Colluding Applicaions on Modern Smartphones.* Orlando: ACSAC, 2012.

Marforio, Claudio. "Analysis of the Communication between Colluding Applications on Modern Spartphones." (ACSAC), no. Dec (2012).

MI5. *What is Espionage?* 2013. https://www.mi5.gov.uk/home/the-threats/espionage/what-is-espionage.html (accessed 01 10, 2014).

Microsoft. *What is malware?* 2014. http://www.microsoft.com/security/resources/malware-whatis.aspx (accessed 10 23, 2013).

Mobile Broadband. Feb 24, 2014. http://en.wikipedia.org/wiki/Mobile_broadband (accessed Feb 24, 2014).

Mobile Virus . Feb 21, 2014. http://en.wikipedia.org/w/index.php?title=Mobile_virus&oldid=596439246 (accessed Feb 21, 2014).

Moskowitz, Ira S. *Covert Channels - Here to Stay?* Gaithersburg: U.S. Navy, 1994.

MSDN Microsoft. *Benefits of Peer Networking.* 2014. http://msdn.microsoft.com/en-us/library/windows/desktop/dd433180(v=vs.85).aspx (accessed 04 08, 2014).

National Security Agency. *SIGINT Frequently Asked Questions.* 2014. http://www.nsa.gov/sigint/faqs.shtml (accessed May 05, 2014).

network Topology. n.d. http://en.wikipedia.org/wiki/Network_topology (accessed 02 25, 2014).

Network Topology. n.d. http://en.wikipedia.org/wiki/Network_topology (accessed 02 25, 2014).

Office of the Director of National Intelligence. *Worldwide Threat Assessment of the US Intelligence Community.* Washington DC: United States of America, 2014.

Peer-to-peer. 2014. http://en.wikipedia.org/wiki/Peer-to-peer (accessed Feb 24, 2014).

Peter hornyack, Seungyoep Han, Jaeyeon Jung. "These Aren't the Droids You're Looking For": Retrofitting Android to Protect Data from Imperious Applications." *University of Washington.* 2011. http://homes.cs.washington.edu/~pjh/pubs/hornyack_appfence_ccs2011.pdf (accessed May 05, 2014).

Quantenna Communications. "Quantenna Developing World's First 10G Wi-Fi™ For Maximum MU-MIMO Performance." *Quantenna Communications.* Apr 14, 2014. http://www.quantenna.com/pressrelease-04_14_14.html (accessed Apr 17, 2014).

Raspberry Pi Foundation. *Raspberrypi.org.* 2012. http://Raspberrypi.org (accessed 04 05, 2014).

Raspbian. *Raspbian.* 2012. http://www.raspbian.org/ (accessed 04 05, 2014).

Romanov, Alex. *Proximity marketing: NFC vs. Bluetooth and Wi-Fi.* Oct 12, 2012. http://www.networkworld.com/news/tech/2012/101212-proximity-marketing-263335.html (accessed Apr 13, 2014).

Rynolds, Paul. *Old Spying Lives On In New Ways.* Jan 23, 2006. http://news.bbc.co.uk/2/hi/europe/4639758.stm (accessed Dec 24, 2013).

Sbrusch, Raymond. "Network Covert Channels: Subversive Secrecy." *SANS.* 2006. SANS.org (accessed 03 27, 2014).

Scavix. *Raspberry Pi as low-cost HD Surveillance Camera.* 2013. http://www.instructables.com/id/Raspberry-Pi-as-low-cost-HD-surveillance-camera/?ALLSTEPS (accessed 04 01, 2014).

Schneier, Bruce. *Wireless Dead Drop.* Jan 31, 2006. https://www.schneier.com/blog/archives/2006/01/wireless_dead_d.html (accessed Feb 24, 2014).

Smith, I. C. "The FBI and Chinese Espionage." *Wikileaks.* n.d. http://wikileaks.org/gifiles/attach/34/34378_smith-%20The%20FBI%20and%20Chinese%20Espionage.pdf (accessed May 05, 2014).

Sources, Online. *Espionage for Everyone: Dead Drop — There's an app for that - See more at: http://execsecurity.com/blog/?p=222#sthash.XVHYsgaL.dpuf.* Aug 01, 2012. http://execsecurity.com/blog/?p=222#sthash.XVHYsgaL.dpbs (accessed Feb 24, 2014).

Speedguide. *What are 1G, 2G, 3G and 4G Networds.* 2014. http://www.speedguide.net/faq_in_q.php?qid=365 (accessed Feb 20, 2014).

Suarez-Tangil, G. *Evolution, Detection and Analysis of Malware for Smart Devices.* March 22, 2013. http://www.seg.inf.uc3m.es/~guillermo-suarez-tangil/papers/2013cst-ieee.pdf (accessed 02 21, 2014).

Symantec. "What's yours is Mine: How Employees are Putting Your Intellecual Property at Risk." *Symantec.* 2013. www.symantec.com (accessed 12 20, 2013).

Tang, Yong. "A Distributed Hybrid Scheme for Unstructured Peer-to-Peer Networks." 2006. (accessed 04 08, 2014).

ThreatTrack Security. *Android Trojan NotCompatible Gets an Upgrade.* July 10, 2013. http://www.threattracksecurity.com/it-blog/android-trojan-notcompatible-gets-an-upgrade/ (accessed Apr 15, 2014).

TinkerTailor. *Dead Drop.* Aug 01, 2012. https://itunes.apple.com/us/app/dead-drop/id499598666?mt=8#sthash.XVHYsgaL.UThEvkYk.dpuf (accessed Feb 10, 2014).

Trend Micro. "Android Under Siege: Popularity Comes at a Price." *TrendLabs 3Q 2012 Security Roundup.* 10 01, 2012. www.trendmicro.com (accessed 12 01, 2013).

—. "Blurring Boundaries: Trend Micro Security Predictions for 2014 and Beyond." *Trend Micro.* 2013. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-trend-micro-security-predictions-for-2014-and-beyond.pdf (accessed 12 2013).

—. "Mobile Threats Go Full Throttle." *TrendLabs 2Q 2013 Security Roundup.* 2013. www.trendmicro.com (accessed 10 01, 2013).

U.S. Government. *GPS Accuracy.* Mar 17, 2014. http://www.gps.gov/systems/gps/performance/accuracy/ (accessed 04 Apr, 2014).

Villeneuve, Nart. "Safe: A Targeted Threat." *Trend Micro.* 2013. www.trendmicro.com (accessed 12 2013).

Virginia Tech. *Mobile Broadband at Virginia Tech.* 2012. http://net.educause.edu/ir/library/pdf/nmd0423.pdf (accessed 04 08, 2014).

Viruses and Mobile Phones. n.d. http://www.gsma.com/technicalprojects/fraud-security/security-advice-for-mobile-phone-users/viruses-and-mobile-phones (accessed 02 21, 2014).

W. Victor Maconachy, Corey D. Schou. "A Model for Information Assurance: An Integrated Approach." *BYU.net.* June 5, 2001. http://it210web.groups.et.byu.net/lectures/MSRW%20Paper.pdf (accessed May 29, 2014).

White, Stanley I. "Economic Divitalization and Espionage." *InfraGard.* n.d. https://private.infragard.org/sites/default/files/private/economic_divitalization.pdf (accessed 03 27, 2014).

Wikipedia, The Free Encyclopedia. Feb 21, 2014. http://en.wikipedia.org/w/index.php?title=Mobile_virus&oldid=596439246 (accessed Feb 21, 2014).

Zander, Sebastian. "A Survey of Covert Channels and Countermeasures in Computer Network Protocols." *IEEE Communications.* 2007. www.comsoc.org/pubs/surveys (accessed 02 28, 2014).

Appendices

Passive Camera System

System Setup

Raspberry Pi:

A $35 single-board computer.
Onboard components:

- Dimensions: 86.6 x 56 x 21mm
- 10/100 Base T Ethernet
- HDMI
- (2) USB 2.0
- RCA Video Out
- SD card socket
- 3.5 mm Audio Out Jack
- Broadcom BCM2835 700MHz Arm Processor
- Videocore 4 GPU
- 256MB Ram

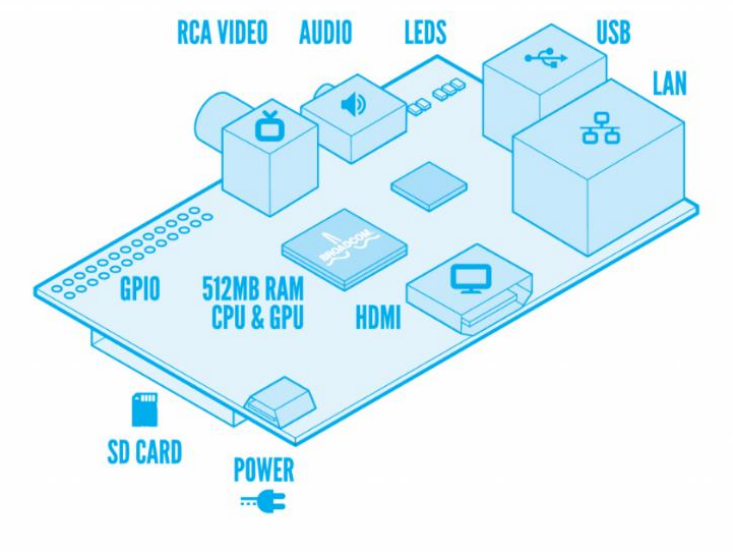

Figure 13: Raspberry Pi Model B

Raspberry Pi Camera Board

Camera module add-on for the Raspberry Pi.

- Dimensions: 25 x 20 x 9mm.
- Weight: 3 grams.
- Native Resolution: 5 megapixels

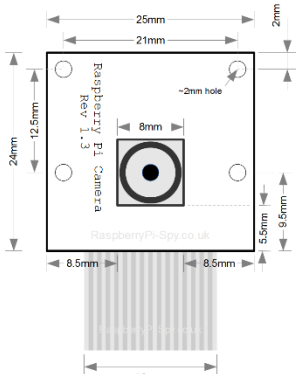

Figure 14: Raspberry Pi Camera 5 Megapixels

TP-Link Wireless Mini USB Adapter

- Model: TL-WN823N
- Speed: 300 Mbps
- Interface: USB 2.0
- Dimensions: 39 x 18.35 x 7.87mm
- Wireless Standards: IEEE 802.11b,g,n

Figure 15: TP-Link TL-WN823N 300 Mbps Wireless Mini USB Adapter

Anker 2nd Gen Astro3

- Capacity: 12000mAh Battery System
- Weight: 11 oz.
- Size: 111 x 83 x 26mm

Figure 16: Anker Astro 3

Passive Camera System

- Raspberry Pi
- Raspberry Pi Camera
- TP-Link Wireless Adapter

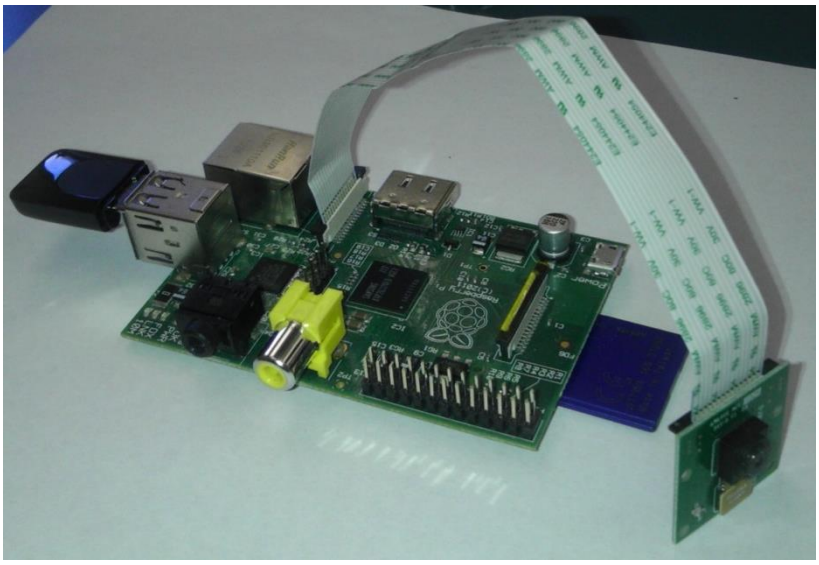

Figure 17: Passive Camera System

Operating System

Raspbian: is a free operating system based on Debian optimized for the Raspberry Pi hardware. An operating system is the set of basic programs and utilities that make your Raspberry Pi run. However, Raspbian provides more than a pure OS: it comes with over 35,000 packages, pre-compiled software bundled in a nice format for easy installation on your Raspberry Pi. (Raspbian 2012)

Motion

Motion is a program that monitors the video signal from cameras. It is able to detect if a significant part of the picture has changed; in other words, it can detect motion. (Lavrsen 2014)

Auto Mailer

SSMTP (automated email forwarding program)

Mutt (text-based email client) Mutt is a small but very powerful text-based mail client for Unix operating systems. The current stable public release version is 1.4.2.3. (Elkins 2014) Mutt is compatible with Raspbian.

Test Email Gmail Account: MarsSmithThesis@gmail.com

Bash Script (splits files into smaller directories and zips them) (AUDIOJAVA 2013)o

Raspberry PI Setup

This tutorial begins from at the point where Raspbian has successfully been imaged onto the SD card and booted.

The following commands will bring the Raspbian OS up to date:

```
sudo apt-get install rpi-update
sudo rpi-update
```

The Following commands will update all packages:

```
sudo apt-get update

sudo apt-get upgrade
```

Wi-Fi Setup

1. Edit network properties

```
sudo nano /etc/network/interfaces
```

2. Add following information to your interfaces.

```
allow-hotplug wlan0

iface wlan0 inet dhcp

wpa-ssid "SmithThesis"

wpa-psk "Thesis"
```

3. Reboot Raspberry Pi

```
sudo reboot
```

Motion Setup

1. Run Command to install Motion Software

```
sudo apt-get install motion
```

2. Install Libraries needed for motion to operate

```
cd /tmp

sudo apt-get install -y libjpeg62 libjpeg62-dev libavformat53 libavformat-dev libavco
dec53 libavcodec-dev libavutil51 libavutil-dev libc6-dev zlib1g-dev libmysqlclient18
libmysqlclient-dev libpq5 libpq-dev

wget https://www.dropbox.com/s/xdfcxm5hu71s97d/motion-mmal.tar.gz
```

3. Unpack the downloaded file to the /tmp directory:

```
tar zxvf motion-mmal.tar.gz
```

4. Update motion with the downloaded build:

```
sudo mv motion /usr/bin/motion

sudo mv motion-mmalcam.conf /etc/motion.conf
```

5. Enable the motion daemon to auto run:

```
sudo nano /etc/default/motion

start_motion_daemon=yes
```

6. A very important command to edit the motion configuration file is

```
sudo nano /etc/motion.conf

sudo chmod 664 /etc/motion.conf

sudo chmod 755 /usr/bin/motion

sudo touch /tmp/motion.log

sudo chmod 775 /tmp/motion.log
```

7. Make sure that motion is always running as a daemon in the background:

```
daemon on
```

8. We want to store the logfile in /tmp instead (otherwise autostart user won't be able to acces it in /home/pi/ folder):

```
logfile /tmp/motion.log
```

9. As we want to use a high quality surveillance video, we've set the resolution to 1280x720:

```
width 1280

height 720
```

10. For our proof of concept the minimum frame rate of 2 per second is sufficient.

```
framerate 2
```

11. This is a very handy feature of the motion software: record some (1 in our configuration) frames before and after the motion in the image was detected:

```
pre_capture 1

post_capture 1
```

12. Enable access to the live stream from anywhere. Otherwise only localhost would be allowed to access the live stream:

```
stream_localhost off
```

13. If you want to protect the live stream with a username and password, you should enable this:

```
stream_auth_method 2

stream_authentication CovertPi:covert
```

14. Reboot the Raspberry:

```
sudo reboot
```

15. After the reboot, the red light of the camera module should be turned on, which shows that motion currently is using the camera to detect any movement.

Raspbian Email Setup

For the proof of concept, a simple email service will be utilized to send captures images to our test email account: Marssmiththesis@gmail.com. In a real malware scenario, all communication would be encrypted and broken down into less detectable pieces.

SSMTP Setup

1. Install SSMTP (automated email forwarding program) and mail utilities:

```
sudo apt-get install ssmtp

sudo apt-get install mailutils
```

2. Edit SSMTP Configuration file:

```
Nano /etc/ssmtp/ssmtp.conf
```

Add the following lines

root=marssmiththesis@gmail.com
mailhub=smtp.gmail.com:587
hostname=marssmiththesis@gmail.com
authUser=marssmiththesis@gmail.com
AuthPass=YourGMailPassword
UseTLS=YES
UseSTARTTLS=YES
FromLineOverride=YES

Mutt Setup

1. Download and Install Mutt

```
sudo –s

apt-get install mutt
```

2. Configure Mutt Email Client by changing the .muttrc file in your home directory

```
Nano /etc/muttrc
```

3. Add the following configured code. This configuration uses Google's free mail service. Make note that text highlighted is specific configuration information for the email account.

Figure 18: Mutt Configuration File

```
#

# System configuration file for Mutt

#

# Default list of header fields to weed when displaying.

# Ignore all lines by default...

ignore *

# ... then allow these through.

unignore from: subject to cc date x-mailer x-url user-agent

# Display the fields in this order

hdr_order date from to cc subject

# emacs-like bindings

bind editor    "\e<delete>"    kill-word

bind editor    "\e<backspace>" kill-word

# map delete-char to a sane value

bind editor     <delete>  delete-char

# some people actually like these settings

#set pager_stop
```

```
#bind pager <up> previous-line
#bind pager <down> next-line


# Specifies how to sort messages in the index menu.
set sort=threads
# The behavior of this option on the Debian mutt package is
# not the original one because exim4, the default SMTP on Debian
# does not strip bcc headers so this can cause privacy problems;
# see man muttrc for more info
#unset write_bcc
# Postfix and qmail use Delivered-To for detecting loops
unset bounce_delivered
set mixmaster="mixmaster-filter"
# System-wide CA file managed by the ca-certificates package
set ssl_ca_certificates_file="/etc/ssl/certs/ca-certificates.crt"
# imitate the old search-body function
macro index \eb "<search>~b " "search in message bodies"
# simulate the old url menu
macro index,pager,attach,compose \cb "\
<enter-command> set my_pipe_decode=\$pipe_decode pipe_decode<Enter>\
<pipe-message> urlview<Enter>\
## to mutt, and can be searched for with ~g, ~G, and ~k.)
##
## I've added x-pkcs7 to this, since it functions (for S/MIME)
## analogously to PGP signature attachments. S/MIME isn't supported
## in a stock mutt build, but we can still treat it specially here.
##
attachments   +A */.*
```

```
attachments   -A text/x-vcard application/pgp.*
attachments   -A application/x-pkcs7-.*
## Discount all MIME parts with an "inline" disposition, unless they're
## text/plain. (Why inline a text/plain part unless it's external to the
## message flow?)
##
attachments   +I text/plain
## These two lines make Mutt qualify MIME containers. (So, for example,
## a message/rfc822 forward will count as an attachment.)  The first
## line is unnecessary if you already have "attach-allow */.*", of
## course. These are off by default!  The MIME elements contained
## within a message/* or multipart/* are still examined, even if the
## containers themselves don't qualify.
##
#attachments  +A message/.* multipart/.*
#attachments  +I message/.* multipart/.*
## You probably don't really care to know about deleted attachments.
attachments   -A message/external-body
attachments   -I message/external-body
##
# See /usr/share/doc/mutt/README.Debian for details.
source /usr/lib/mutt/source-muttrc.d|

set from = "marssmiththesis@gmail.com"
set realname = "DeadDrop1"
set imap_user = "marssmiththesis@gmail.com"
set imap_pass = "**********"
# REMOTE GMAIL FOLDERS
```

```
set folder = "imaps://imap.gmail.com:993"
set spoolfile = "+INBOX"
set postponed ="+[Google Mail]/Drafts"
set trash = "+[Google Mail]/Trash"
set any_label = "+[Google Mail]/any_label"
# LOCAL FOLDERS FOR CACHED HEADERS AND CERTIFICATES
set header_cache =~/.mutt/cache/headers
set message_cachedir =~/.mutt/cache/bodies
set certificate_file =~/.mutt/certificates
# SMTP SETTINGS
set smtp_url = "smtp://marssmiththesis@smtp.gmail.com:587/"
set smtp_pass = "**********" # use the same passowrd as for IMAP
# SECURING
set move = no  #Stop asking to "move read messages to mbox"!
set imap_keepalive = 900
bind editor <space> noop
macro index gi "<change-folder>=INBOX<enter>" "Go to inbox"
macro index ga "<change-folder>=[Google Mail]/All Mail<enter>" "Go to all mail"
macro index gs "<change-folder>=[Google Mail]/Sent Mail<enter>" "Go to Sent Mai$
macro index gd "<change-folder>=[Google Mail]/Drafts<enter>" "Go to drafts"
```

Auto Zip and Mail

Auto Zip and Mail is a bash script that will prepare, zip and mail files captured from the motion camera system. This script was written by audiojava and all credit is given to him. (AUDIOJAVA 2013) For more efficient use in relation to the proof of concept, a few lines of code have been added that simply check to see if there are any files to zip and mail. If no file are found the script is terminated. Adjusted code is in bold and highlighted letters.

Figure 19: Zip and Mail Bash Script

```
#!/bin/bash
splitsize=500
recipient="marssmiththesis@gmail.com" # for multiple recipients
#Email subject and message
subject="Captured Images"
message="This is the body of the mail"
#Motion target files path
targetfilepath="/tmp/covert/pics/"
#Motion target directory path
targetdirpath="/data/webcam"
####################################
echo "Running zipandmail.sh..." `date`
#count number of files in motion directory
numfiles=$( ls -l $targetfilepath | egrep -c '^-')
numfolders=`expr $numfiles / $splitsize`
lastfoldercount=`expr $numfiles % $splitsize`
echo $numfiles
#echo $numfolders
#echo $lastfoldercount
#M.Smith Thesis Adjusted Code
  if [ "numfiles" -eq "0" ]; then
    echo "No Files Found"
    exit
  fi
```

```
#Move all files from motion directory to newly created directories based on $numfolders
COUNTER=0
while [ $COUNTER -le $numfolders ]; do
  echo "Creating directory... " `date`
  destination="$targetfilepath$COUNTER"
  rm -rf $destination
  mkdir -p $destination
#move multiples of $splitsize files to new folder(s) except the remainder files (that's less than $splitsize)
  if [ "$COUNTER" -lt "$numfolders" ]; then
    for file in $(ls -p $targetfilepath | grep -v / | tail -$splitsize); do
      mv $targetfilepath$file $destination
    done
#move remainder files in last new motion folder
  else
    for file in $(ls -p $targetfilepath | grep -v / | tail -$lastfoldercount); do
      mv $targetfilepath$file $destination
    done
  fi
  echo "Creating zip file... " `date`
  pushd $targetdirpath
  zip -9 -r -q motion$COUNTER.zip ./motion$COUNTER/
  popd
  echo "Sending mail to recipient... " `date`
  echo "content of the email" | mutt -s "subject of the email" $recipient -a $targetfilepath$COUNTER.zip
  let COUNTER=COUNTER+1
done
```