JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Volume 11, Issue 2
August 2018
ISSN: 1946-1836

In this issue:

4. **What's "Appening" to our Privacy? A Student's Perspective on Downloading Mobile Apps**
Karen Paullet, Robert Morris University
Adnan A. Chawdhry, California University of Pennsylvania
David M. Douglas, Robert Morris University
Joseph Compimizzi, Florida Atlantic University

13. **An Exploratory Analysis of Gender Differences in IT Project Commitment, Continuation, and Escalation**
Melinda L. Korzaan, Middle Tennessee State University
Amy H. Harris, Middle Tennessee State University
Nita G. Brooks, Middle Tennessee State University

24. **Information Security and Privacy Legislation: Current State and Future Direction**
Lex Dunlap, University of North Carolina Wilmington
Jeff Cummings, University of North Carolina Wilmington
Thomas Janicki, University of North Carolina Wilmington

33. **Protecting IoT Devices from the Mirai Botnet**
Charles Frank, Dakota State University
Samuel Jarocki, Dakota State University
Cory Nance, Dakota State University
Wayne E. Pauli, Dakota State University

iscap
Information Systems
& Computing
Academic Professionals

The **Journal of Information Systems Applied Research** (JISAR) is a double-blind peer-reviewed academic journal published by **ISCAP,** Information Systems and Computing Academic Professionals. Publishing frequency is three issues a year. The first date of publication was December 1, 2008.

JISAR is published online (http://jisar.org) in connection with CONISAR, the Conference on Information Systems Applied Research, which is also double-blind peer reviewed. Our sister publication, the Proceedings of CONISAR, features all papers, panels, workshops, and presentations from the conference. (http://conisar.org)

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the JISAR journal. Currently the target acceptance rate for the journal is about 40%.

Questions should be addressed to the editor at editor@jisar.org or the publisher at publisher@jisar.org. Special thanks to members of AITP-EDSIG who perform the editorial and review processes for JISAR.

Journal of
Information Systems Applied Research

Editors

2018 JISAR Editorial Board

What's "Appening" to our Privacy? A Student's Perspective on Downloading Mobile Apps

Karen Paullet
paullet@rmu.edu
Robert Morris University
Moon Township, PA 15108

Adnan A. Chawdhry
Chawdhry_a@calu.edu
California University of Pennsylvania
California, PA 15419

David M. Douglas
douglas@rmu.edu
Robert Morris University
Moon Township, PA 15108

Joseph Compimizzi
jcompomizzi@fau.edu
Florida Atlantic University
Boca Raton, FL 33431

Abstract

Smartphones and mobile device sales continue to grow allowing mobile applications (apps) to develop in variety and usage. Mobile device users have downloaded over 225 billion apps and this number continues to grow. While there is an inherent benefit to our daily lives of having applications that are available at our fingertips or by the sound of our voice, they come with an associated and undiscussed cost of security and privacy issues. One must consider these risks, how they may impact our lives, and the best alternative of mitigating the risk with the balance of convenience. This study explores specific apps downloaded by end-users, the number of apps they download, and how they correlate to their awareness of mobile app security and privacy concerns. A total of 124 undergraduate and graduate students were surveyed at two mid-Atlantic Universities in both traditional and online programs. The study concluded that students download apps regardless of the security or privacy risks that are being exposed.

Keywords: mobile security, mobile applications, apps, mobile device, application privacy

1. INTRODUCTION

With the increased use of smartphones and mobile devices, mobile applications have become an integral part of our everyday lives. Numerous applications are being developed daily and are created by developers of different ages, cultures, and social / economic backgrounds. These applications strive to provide users with an easier life and less stress by supplementing manual activities with application driven ones. With the extensive library of applications available to use, it appears these applications have filled our present and perceived needs. According to Statistica (2016), there has been an upward trend in mobile application usage. In 2011, users had downloaded 22 billion free and another 2.9 billion paid applications. However, as of June 2017, these numbers have significantly increased to 211 billion free and 13.49 billion paid applications. The variance between these two numbers illustrates that people download more because its free.

Mobile technology is significantly impacting the way people interact with each other, organizations, and with technology itself. Mobile applications, or apps as commonly called, promote communications, information retrieval and exchange, and any other number of tasks users need to complete at a literal touch of a screen. These third party interfacing platforms offer users ease. In addition to convenience, mobile apps also come with risks associated with security and privacy.

Developers are creating applications for various reasons including fun, profit, or possibly to fill a gap in the growing library of "must have" applications. In some respects, apps certainly provide us clear advantages, however, they also come at a cost of a more complacent and indolent mobile community in regards to cyber security and oversharing of information.

As with any technological advancement, there are always unintended consequences that must be balanced against its perceived benefits. These applications are at the tip of our fingers on our smart phones and in some cases, usable by the sound of our voice. Knowingly and unknowingly, we tend to overshare private information in cyberspace about our personal lives. Unfortunately, once this information is released in cyberspace, it can be difficult, if not impossible, to retrieve or change it. The information is now in the public domain and beyond our grasp or control. Our carelessness can open the gateways for a hacker or rouge agency to digitally access our financial data and other aspects of our lives. Before divulging too much, one must carefully consider the risks to ourselves and our privacy plus any security concerns to our digital lives.

2. RELATED LITERATURE

In the article "The Mobile Application Preferences of Undergraduate University Students: A Longitudinal Study" Potgieter indicates her study revealed that "even though users were aware of security threats associated with downloading apps, this knowledge did not deter them from continuing to download apps" (2015, p. 1). A study conducted by Chawdhry, Paullet, Douglas, and Compomizzi confirmed similar results in that students downloaded mobile apps without fully understanding the security risks associated with such action (2017, p. 35). In their study, while 96.64% of students indicated that they download mobile apps, only 70.69% did not install any type of anti-malware on their devices. Interestingly, in this same study 64.60% of students surveyed disclosed that they also uninstalled an app after discovering how much personal information was shared.

Why students download mobile applications in spite of security risks gives insight to their motivations. As studies by Potgieter reveal, "In 2013, 48% of respondents indicated that they searched for an app when they 'need information on a brand, its product or its services, whereas the most popular reason in 2014 for searching for an app was that respondents 'wanted to be entertained'" (2015, p. 3). Other reasons indicated by students in the research studies by Potgieter as to why they downloaded a mobile application included family or friend recommendation of the app, curiosity about the app, reference to the app on regularly used websites, or the desire to purpose a product or service. Researchers like Baily (2016), maintain that consumers of mobile applications conduct a cost-benefit analysis and conclude that the convenience is worth more than privacy (p. 5). Other researchers such as Soukup (2015) present that mobile technology platforms call "attention to personal presence, personal choices, and the social forces that shape both" (p. 5). Soukup's observations advocate that these devices and platforms promote social cohesion.

Given these motivations, the number and types of mobile apps employed by college students provide insight to the presence of security risks as well. In a study conducted by Compomizzi (2013) regarding social use of mobile technology, 21.3% of study participants indicated that they downloaded 41 or more apps. Of these apps, 12.0% indicated that half of the apps downloaded were related to academic tasks. Regarding social use of mobile applications in this study, "Facebook was the social media app listed most frequently by participants with Twitter following as the second most frequently accessed social media app" (p. 128). The study by Potgieter (2015) found similar results: "Facebook was a clear favorite with 75% of respondents indicating that they had this app on their smartphone, whereas in 2014, WhatsApp had been installed by 73% of respondents" (p. 5).

Advanced mobile operating systems implement a "sandbox" permission system whose function is to provide security and privacy policy for third-party apps. "To provide better services to users and gain more downloads of Apps, mobile App developers try to request more and more data access permissions, which can help to implement the intelligent applications, such as social sharing services. However, these services may result in potential security and privacy risks" (Zhu, Xiong, Yong, Chen, p. 2-3).

A July 9, 2017 Wall Street journal article by Fritz and Mickle stated that according to estimates by Bernstein Research: "iTunes videos, music, book and magazine sales last year accounted for an estimated $4.1 billion in revenue, making it the second-largest services business behind App Store sales, which were nearly twice as large …" (Fritz, et.al. 2017).

Baily sheds some light on the impacts of technological interface with application users. In the article "Why Consumers Opt Out of Privacy by Buying into the Internet of Things" from the Texas Law Review (2016), Baily describes a possible effect that is applied to app users called unrealistic optimism or over optimism. She asserts that with unrealistic optimism, a "user may be subject to the above average effect because they may believe that they are less likely than the average person to experience harm from data loss" (p. 1029). Drawing on the research of Miyazaki and Fernandez, Baily emphasized, "Moreover, the more Internet experience a person has, the lower his perceived risk toward risky online behaviors" (p. 1029).

Koved, et al. (2013) discussed four increased risks associated with authentication and authorization regarding interaction with the mobile platforms of smartphones and tablet devices. These risks include (a) user action observation by others who may than impersonate (authenticate) on another device. (b) stolen or lost devices could expose sensitive or personal information to unauthorized persons (c) "man in the middle attacks" which would allow attackers to "capture authentication credentials and perform actions" as the device owner (d) multiple passwords saved on mobile devices may save time but increase risk of unauthorized access and authentication (p,1). Moreover, Koved, et al. (2013) suggests that to guard against these perceived and actual security risks it is essential to have a trusted authentication strategy and communications systems that are secure. Part of the solution they argue, is various authentication methods are part of the solution. Since passwords can be observed it is not considered a single or reliable approach (p. 1). "In particular, mobile device applications, including their web browsers, are caching authentication credentials, enabling an attacker to exploit them" (Koved, et al., p.1. 2013).

Although current smartphone and tablet devices can capture biometric data via cameras and microphones which offers a potential and partial security solution, some users most likely would consider it an added burden. As user interaction with their mobile devices is generally brief, it is perceived they do not want to bother with the distraction of a lengthy or complex authentication process. This is especially true if they do not understand the reasons or importance for authentication. "Little is known about peoples' awareness of these mobile device authentication risks" (Koved, et al., p.1. 2013).

The use of biometrics is now being utilized in mobile applications. "In 2015, Citigroup began testing an ATM that would scan a customer's iris and make four-digit access codes obsolete" (Demos, T., p, B4, 2017). As of 2018, Citi has all but abandoned the project. Reason one, cost and complexity. Collecting and managing a database of millions of customer biometric data would be enormous. Reason two, a biometric database and genetic template of this magnitude and value would be an alluring target for a legion of hackers from lone wolves to international gangsters. (Demos, T., p, B4). Passwords can be easily replaced, but biometric authentication such as fingerprints and irises obviously cannot.

Wells Fargo, J.P. Morgan, and Bank of America have begun to utilize ATM's that can link biometric data to the smartphone devices of customers. Instead of the financial institution storing customer biometric information, it is the customer's responsibility to store and safeguard their biometric authentication. One method uses the customers fingerprint to sign in via their mobile device which would transmit a code to the ATM (Demos, T., p, B4). According to banking-technology start-up HYPR Corporation there are "about two billion units globally can use fingerprints, pictures of eyes and faces, and voice recognition … "and are already used for mobile banking applications (Demos, T., p, B4).

3. METHODOLOGY

The study surveyed students from two mid-Atlantic Universities from March to April 2016. For this study, the population chosen comprised of undergraduate and graduate students enrolled in on-campus or online programs. This population was chosen to ensure students surveyed would be 18 years or older which comprised of a total of 124 students completing the survey. The researchers utilized Survey Monkey, an online survey tool, to collect data, which were then imported into SPSS for organization and analysis. As part of the analysis, the researchers used a Chi-square approach with a statistical significance level of .05 margin of error and a 95% confidence Level. The study addressed the following two research questions.

1. Does the use of specific mobile applications impact the level of mobile security and privacy awareness?

2. How does the number of applications installed on a mobile device impact the user's actions to prevent security and privacy issues?

The survey administered to students consisted of 22 closed-ended questions and one open-ended question for further understanding of the participant's responses. The questions focused on whether students were aware of security and privacy concerns that exist with downloading mobile applications. Additionally, participants were asked to identify the applications they are using and the number of applications they have downloaded. The questions primarily focused on responses of "Yes" and "No", while a few questions provided additional options for students to select the type of mobile device they use, applications they use on their phone, and how many apps they have downloaded.

4. RESULTS

The survey began with various foundational / demographic questions about the participants. For this study, the first question of primary importance was to understand which apps were being downloaded and used. The question allowed the users to select as many as needed that were applicable to their personal use. The apps included Facebook, Twitter, Instagram, Snapchat, Accessing Email, Playing Games, Listening to Music, Reading Books, and Searching for Information. Additionally, the users were asked how many applications they have downloaded with the response categorized as 1-10, 11-20, 21-30, 31-40, and 40+. A summary illustrating the percentage of participants who responded to each question can be found in Tables 1 and 2 . From the findings, more than half of the respondents have used each of the applications mentioned with the exception of "Reading Books" which only illustrated 31.5% of the respondents. Additionally, the majority, 63.8%, of respondents have downloaded 20 apps or less. The largest responses suggested that the users downloaded between 11-20 apps on their mobile device.

Table 1: Summary of Applications downloaded by Users.

Application Downloaded	Uninstalled After Learning About App
Facebook	70.20%
Twitter	50.00%
Instagram	56.50%
Snapchat	62.10%
Accessing Email	91.10%
Playing games	56.50%
Listening to music	81.50%
Reading books	31.50%
Searching for information	84.70%

Table 2: Number of Apps Downloaded

Number of Apps Downloaded	Percentage of Respondents
1-10	28.30%
11-20	35.50%
21-30	17.70%
31-40	4.80%
40+	13.70%

A second component to this study's analysis was to analyze the data using Chi-square. The objective was to determine the statistical significance between two variables using a .05 margin of error and a 95% confidence interval. The results are illustrated in Table 3 and Table 4. Table 3 (in appendix) illustrates the application downloaded assessed against a number of activities illustrating the users were aware of a potential security and privacy concerns. Only one application illustrated a statistical significance given the .05 margin of error. Facebook had a value of .05. Instagram had significance with having Anti-Malware installed and a value of .021. Instagram also had statistical significance with Reading the Terms of Use with a value of .04. Lastly, Snapchat had a statistical significance with Having Anti-Malware Software having a value of .049.

Additionally, the researchers compared various security and privacy activities with the number of applications downloaded. Only one activity, Having Anti-Malware Software, had a statistical significance of .048 with the number of applications downloaded. Further details are provided in Table 4 below.

Table 4: Chi-square Analysis of Security / Privacy Activity vs Number of Applications Downloaded

Security / Privacy Activity	Number of Applications Downloaded
Disabled Location Services	0.866
Clear Browsing History	0.89
Have Anti-Malware Software	0.048
Read Terms of Use	0.137
Uninstalled / Not installed an App	0.687
Uninstalled / Not Installed an App	0.684
Uninstalled / Not installed an App	0.727
Not Installed After Learning About App	0.775
Uninstalled After Learning About App	0.517

It was also important to see how many participants undertook security and privacy risk mitigation activities and how it correlated to the applications they downloaded. The activities included disabling location services, clearing browsing history, backing up their phone, having anti-malware software installed, another person accessing their phone, and reading the terms of use. Over 50% of the users who downloaded Facebook, Instagram, Snapchat, Email, Music, and Searching for Music applications stated they disabled location services. Additionally, over 50% of users who downloaded Facebook, Email, Music, and Searching for Information stated they cleared their browsing history. Lastly, over 50% of the users of Facebook, Snapchat, Email, Music, and Searching for Information reported that another person has access to their phone. All other areas reported less than a 50% response rate. The details of this analysis can be found in Table 5 in the Appendix.

Similarly, the researchers did an analysis of various security and privacy risk mitigation activities and compared it against how many applications were downloaded. The activities included disabling location services, clearing browsing history, installing anti-malware software, another person accessing their phone, reading terms of use, uninstalling / not install an app, not installing an app after learning about it, and uninstalling an app after learning about it. For each activity, the largest response was either in the 1-10 or the 11 – 20 categories. In most cases, over one third of the respondents fell in the 11-20 category. Further details of this analysis are available in Table 6 in the Appendix.

5. DISCUSSION

Mobile Application Impact

Based upon the chi-square analysis of the applications users download and the activities to mitigate the security and privacy risk, the researchers found three applications that had some level of statistical significance. The first research question sought to find out if the use of specific mobile applications impacts the level of mobile security and privacy awareness. These applications included Facebook with disabling location services, Instagram and Snapchat with installing anti-malware software, and Snapchat with reading the terms of use. The interesting part of this analysis is that all three of these applications are categorized as social media sites. In addition to these, accessing email, listening to music, and searching for information also had large response rates (over 50%) for the same activities in addition to clearing your browsing history. However, it is important to note that clearing your browsing history was not statistically significant.

From this analysis one could assume that certain applications like Facebook, Instagram, and Snapchat do affect the level of security and privacy awareness given that their users were more likely to act to protect themselves. Further extrapolation lead the researchers to believe that the respondents may consider social media applications risky in relation to security and privacy issues and therefore act to mitigate this risk. However, Twitter, another social media site, was not statistically significant and less than 50% of the respondents stated they undertook an activity to protect themselves. One assumption could be that this social media is used less than the other social media applications. Another thought is that users do not perceive Twitter as risky in comparison to Facebook, Instagram, and Snapchat.

Number of Applications

The second research question determined if the number of applications installed on a mobile device impact the user's actions to prevent security and privacy issues. When reviewing the number of applications downloaded, the largest category was 35.5% of the respondents saying that they downloaded 11-20 apps. Second to that were 28.3% of the participants stating they downloaded 1-10 applications. Most participants downloaded less than 20 applications. Lastly, 17.7% of the participants stated they downloaded 21-30 apps. Given these numbers, it was important to note that the researchers had a good variety of participants from ones who download few applications to those who download many applications.

One form of assessments was to review the chi-square values when comparing the number of apps downloaded with the various security and privacy risk mitigation activities. Of each of the values, only reading the terms of use showed a statistical correlation. There is a trend with the number of apps downloaded and reading the terms of use. Essentially one could interpret this as users are reading the terms of use more as they are downloading more apps. This could be because of being more familiar with the apps and the risks they possess. Therefore, users are reading the terms of use more frequently. Another notion is that users who have downloaded less apps have read the terms of use and realized that the risk associated with the apps is not worth it. And by doing so they chose not to download other apps.

Many of the other activities did not have a statistical correlation with the number of applications downloaded. One of great importance was disabling location services. Although we could not see a correlation with the number of applications, it was seen that users were still disabling location services. Lastly, it was important to note that there was consistency of whether users uninstalled / not installed an application before and after they learned about it. This consistency was across all the categories for the number of applications downloaded. Therefore, it is difficult to assess the impact of learning about the application had on their choices in relation to security and privacy concerns.

6. CONCLUSIONS

With the advent of the concepts of big data and the Internet of Things, research regarding the use of mobile applications, user practices, and user sense of security is growing. Studying the needs and preferences of users, yields understanding to the practices and appreciation of privacy users demonstrate, especially college students. Although statistical significance was not prevalent throughout this study it is apparent that at least half of the student populations download apps without completely understanding the potential security risks to their data and privacy. This study was important because it illustrated regardless of security risks, it is becoming a trend that students are ignoring concerns that can risk their privacy and security.

Mobile applications are here to stay. It is apparent that convenience to some outweighs the risks associated with downloading some apps. Below are a list of tips to help keep our data and privacy secure:

1. Install apps from trusted sources such as an app store
2. Install anti-malware or security software on mobile devices
3. Read the terms of use and information regarding privacy and what the app can actually access on the mobile device
4. Review permissions when an app sends a notice to update
5. Enable app security features such as a password
6. Always keep the latest update on the mobile device. The updates can assist with catching viruses
7. Remove applications that are not necessary
8. Turn off connecting automatically to Wi-Fi or Bluetooth

7. REFERENCES

Bailey, M. (2015). Seduction by technology: why consumers opt out or privacy by buying into the Internet of Things. Texas Law Review, Austin, TX pp. 1023-1054

Chawdhry, A., Paullet, K., Douglas, D. & Compomizzi, J. (2017). Downloading mobile applications: Are students protecting themselves? *Journal of Information Systems Applied Research.* Vol 10, Issue 2, pp. 35-42

Compomizzi, J., (2013). *The Influence of iPad Technology on the Academic and Social Experiences of Veteran and Military Students: Academic Preparation, Collaboration, Socialization, and Information Access* (Doctoral Dissertation). Retrieved on 7/6/2016 from Proquest 3565603.

Demos, T. (2017, July 9). Why your phone will be the key to ATMs of the future. The Wall Street Journal, P. B4. Retrieved on July 10, 2017 from https://www.wsj.com/articles/why-your-phone-will-be-the-key-to-atms-of-the-future-1499598001

Fritz, B., Mickle, T. (2017, July 9). Apple loses ground in the digital-movie battle. The Wall Street Journal, P. B1, B2. Retrieved on July 10, 2017 from https://www.wsj.com/articles/apples-itunes-falls-short-in-battle-for-video-viewers-1499601601

Koved, L., Trewin, S., Swart, C., Singh, K., Cheng, P., and Chari, S. (2013). Perceived security risks in mobile interaction. Symposium on Usable Privacy and Security (SOUPS) 2013, July 24-26, 2013, Newcastle, UK

Potgieter, A. (September 18, 2015). The application preferences of undergraduate university students: A longitudinal study', *South African Journal of Information Management* 17 (1). Art. #650, 6 pages. Retrieved on July 1, 2017 from http://dx.doi.org/10.4102/sajim.v17i1.650

Soukup, P.A., SJ. (2015). Smartphones. Communication Research Trends. Vol. 24, No. 4 pp 1-39.

Statistica, (2016). The statistics portal. Number of free and mobile app store downloads worldwide from 2011 to 2017 (in billions). Retrieved on July14, 2017 from www. Statistica.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/

Zhu, H., Xiong, H., Yong, G., Chen, E. (2014). Mobile App recommendations with security and privacy awareness. University of Science and Technology of China, Rutgers University, UNC Charlotte. Retrieved from http://dx.doi.org/10.1145/2623330.2623705

Appendices and Annexures

Table 3: Chi-Square Analysis of Applications Downloaded Versus Security and Privacy Awareness

Application	Disabled Location Services	Clear Browsing History	Have Anti-Malware Software	Read Terms of Use
Facebook	0.05	0.548	0.135	0.296
Twitter	0.405	0.66	0.195	0.351
Instagram	0.134	0.179	0.021	0.04
Snapchat	0.29	0.682	0.049	0.06
Accessing Email	0.936	0.166	0.485	0.951
Playing Games	0.942	0.632	0.829	0.65
Listening to Music	0.7	0.252	0.438	0.16
Reading Books	0.607	0.626	0.267	0.291
Searching for information	0.468	0.943	0.729	0.93

Table 5: Participants Undertaking Security / Privacy Activities Based upon Applications Downloaded

Application Downloaded	Location Services Disabled	Browsing History Cleared	Phone Backed up	Anti-Malware Installed	Another Person Access Your Phone	Read Terms of Use
Facebook	61.29%	52.42%	26.61%	17.74%	61.29%	25.81%
Twitter	43.55%	37.90%	21.77%	15.32%	42.74%	15.32%
Instagram	50.00%	44.35%	21.77%	12.10%	49.19%	15.32%
Snapchat	54.03%	46.77%	24.19%	14.52%	54.03%	17.74%
Accessing Email	75.00%	66.94%	29.03%	26.61%	75.00%	30.65%
Playing games	47.58%	42.74%	20.16%	16.13%	48.39%	18.55%
Listening to music	68.55%	61.29%	25.81%	22.58%	70.16%	25.81%
Reading books	25.81%	24.19%	12.10%	11.29%	26.61%	12.90%
Searching for information	70.16%	62.10%	29.03%	25.00%	71.77%	29.03%

Table 6: Participants Undertaking Security / Privacy Activities Based upon Number of Applications Downloaded

Number of Apps Downloaded	Location Services Disabled	Browsing History Cleared	Anti-Malware Installed	Another Person Access Your Phone	Read Terms of Use	Uninstalled / Not installed an App	Not Installed After Learning About App	Uninstalled After Learning About App
1-10	22.68%	23.53%	38.24%	25.32%	17.50%	29.31%	22.09%	27.78%
11-20	39.18%	35.29%	20.59%	37.97%	37.50%	34.48%	38.37%	36.11%
21-30	19.59%	20.00%	20.59%	22.78%	15.00%	18.10%	18.60%	16.67%
31-40	4.12%	5.88%	8.82%	6.33%	12.50%	4.31%	6.98%	5.56%
40+	14.43%	15.29%	11.76%	7.59%	17.50%	13.79%	13.95%	13.89%
Total	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%

An Exploratory Analysis of Gender Differences in IT Project Commitment, Continuation, and Escalation

Melinda L. Korzaan
melinda.korzaan@mtsu.edu

Amy H. Harris
amy.harris@mtsu.edu

Nita G. Brooks
nita.brooks@mtsu.edu

Department of Computer Information Systems
Middle Tennessee State University
Murfreesboro, TN USA

Abstract

This study examines the IT project environment with a focus on understanding gender differences that exist in key constructs known to influence project continuation. These constructs were chosen from two key streams of project-based research known to influence intention to continue: commitment and escalation. Commitment is a multi-faceted construct reflecting an individual's need or desire to continue working on a project. Escalation is also multi-faceted construct that generally refers to an individual's inclination to continue working on a project even in the face of negative information. Findings from a web-based survey resulted in 199 usable responses with the sample consisting of 56.7% males and 43.2% females. Data analysis revealed that gender differences existed in both continuance commitment and intention to continue the project. Differences were also found in constructs identified as being related to escalation within IT projects: desire for project success, negative information/status, over optimism, and sunk cost. Implications for these findings as well as directions for additional study are provided.

Keywords: Gender, IT Projects, Project Continuation, Commitment, Escalation.

1. INTRODUCTION

Within the field of information technology (IT), many different areas have been researched and explored that focus on understanding how to create, maintain, and implement valuable IT products. IT projects have received specific attention as they provide the mechanisms through which systems and tools are designed and eventually introduced to the end user. IT Projects can be complicated due to the technical nature of technology in general and to the management of interactions between individuals representing different project components.

Previous research has examined the IT project environment from many perspectives. Two primary areas include commitment and escalation as they relate to the continuation of projects (Keil, Mann, & Rai, 2000; Korzaan & Brooks, 2015; Newman & Sabherwal, 1996). Previous research has also acknowledged the lack of and need for research related to the examination of gender differences in the context of the project environment (Henderson & Stackman, 2010).

The field of project management has historically been male-dominated, but it has been found that women are taking on more roles (Henderson & Stackman, 2010). To begin examination of these issues and to better understand the evolution of project-based work, the current study takes an exploratory approach into the examination of differences that exist between males and females in IT project teams and investigates these differences in terms of project commitment constructs and psychological factors associated with project escalation.

The constructs that will be examined are established predictors of an individual's inclination or intention to continue investing time, money, and resources into an IT project. From a commitment theory perspective, we examine gender differences in affective commitment, continuance commitment, and normative commitment. From an escalation theory perspective, we examine gender differences in desire for project success, perceptions of negative information, over-optimism, the sunk cost effect, self-justification, and the completion effect.

We also examine differences in the outcome variable itself, intention to continue. Intention or inclination toward project continuation is important to success when the project is on track and is conversely a contributor to failure when the project is troubled and in need of termination or redirection (Korzaan & Brooks, 2015; Keil, et al., 2000; Lee, Keil, & Wong, 2015).

2. LITERATURE REVIEW

Gender

Examining gender as it relates to the IT project environment can provide additional insight into why IT projects fail and why they succeed. Looking across the IT literature, the importance of gender and including it in research models becomes obvious. Differences between men and women have been found related to motivations, levels of computer anxiety, attitude, autonomy, adoption, and innovation (Ahuja & Thatcher, 2005; Venkatesh, Morris, & Ackerman, 2000). It has also been found that "women encounter problems gaining entry and acceptance in the project environment, because the culture of traditional project-based industries...is masculine in orientation" (Cartwright & Gale, 1995 p. 12). Many previous studies have focused on this concept. The project environment has historically been viewed as being one primarily defined by masculine characteristics (Cartwright & Gale, 1995), but it has been noted that a shift is occurring highlighting the importance of feminine qualities as used to define project work (Buckle & Thomas, 2003).

Gender differences have also been noted in many other areas of study. For example, Feingold (1994) provided a summary of research related specifically to personality and how men and women differ across key traits. Research on financial decision-making has revealed that women and men differ in areas related to risk seeking behavior (Powell & Ansic, 1997). These types of findings highlight the potential for gender to play a role in project-based decisions and outcomes. The IT profession provides a unique environment in which to examine project work. Technology has been defined as a masculine issue (Lindgren & Packendorff, 2006). Additionally, within the IT profession in general, women have historically had low representation, which can play a role in defining areas of opportunities for IT and project work. The National Center for Women and IT found that in 2015 women accounted for 25% of computing-related occupations (Ashcraft, McLain, & Eger, 2016). When looking at all occupations in the same year, women accounted for 57% of the U.S. workforce. These numbers have been consistent throughout research on the IT profession (Ahuja & Thatcher, 2005).

IT Project Continuation

One of the key dependent variables driving IT project research has been intention to continue. Regardless of the theory used or approach taken, the goal is often to understand what influences the continuation of a project. Within the literature, there have been several approaches taken to aid our understanding of projects in situations where success is likely and in situations where failure is probable. Two primary theoretical foundations that have provided some stability and insight into this stream of research are theories of commitment and escalation. Each of these theoretical foundations will be discussed along with specific constructs used to examine the models in totality.

Commitment

Newman & Sabherwal (1996) identify project commitment to be important for IT project success but also acknowledge that too much commitment may lead to decisions to continue a failing course of action when the project is off track or spiraling out of control. Commitment has been identified as a key construct with both positive and negative implications based upon context, and has also been found to manifest in multiple discriminant constructs. These constructs include affective, continuance, and normative commitment. All three forms of commitment have been found to be significant predictors of project continuation intentions (Korzaan & Brooks, 2015). The dependent variable in such studies is intention to continue, which taps into the individual willingness or inclination to persist and continue with the technology project as planned (Korzaan & Brooks, 2015).

Affective, continuance, and normative commitment were originally drawn from the organizational literature and applied to the context of IT projects (Korzaan & Brooks, 2015). Affective commitment is conceptually defined as an individual's emotional attachment and desire to work on the project. Affective commitment taps into involvement with the project, pride in working on the project, and a feeling of emotional attachment to the project. Continuance commitment indicates an attachment to a project resulting from a need to avoid the negative consequences associated with terminating the project. Such negative consequences may also include a loss of reward or incentives. Normative commitment arises from an individual's sense of obligation or duty toward the project (Korzaan & Brooks, 2015).

Escalation

When looking at escalation, and the role that escalation plays in determining project continuation, several constructs have been found to play a significant role in these processes. These include desire for project success, negative information, an overly optimistic view of eventual project success, the sunk cost effect, perceived responsibility, and completion effect (Keil, et al., 2000; Lee, Keil, & Wong, 2015). Information about each of these key constructs will be discussed in the sections that follow.

Desire for Project Success (Goal Valence/Desirability)

Goal theory has been used to guide prior escalation research (Lee, Keil, & Wong, 2015). In addition, escalation has been described as an instance of "persistence in goal-directed behavior" (Fox & Hoffman, 2002, p. 273) and is an extension of the factors that drive the initiation and sustainability of goal-directed behavior (Fox & Hoffman, 2002). Goal valence or goal desirability is a central concept in goal theory that influences inclinations to continue or escalate projects through its influence on commitment (Lee, Keil, & Wong, 2015). Goal valence refers to the degree to which achieving a goal is desirable or important to an individual with the underlying foundation of valence being rooted in an individual's needs. The stronger an individual's need to meet the goal, then the higher the valence (Lewin, 1935). In the context of information technology projects, goal valence or desirability is conceptualized as the desire for project success and is defined as the degree of importance and attractiveness of the outcome of the project

Negative Information

The awareness of and response to negative information about a project distinguishes between project escalation and project de-escalation (Keil and Robey, 1999; Montealegre and Keil, 2000). In other words, if the project is in trouble yet negative information about the project is either ignored or perceived as insignificant then the project will likely continue along its current course without corrective action being taken. This type of information asymmetry in turn sets up the project for escalating out of control (Montealegre and Keil, 2000; Keil, 1995; Keil et al., 2004).

Over Optimism

Over optimism is a form of information bias that manifests in overestimating the likelihood of success (Newman & Sabherwal, 1996). It is surmised that this bias could occur when negative project status information is easily concealed, negative project status information is ignored, information that is contrary to existing beliefs is refuted, and/or only information that confirms beliefs in project success is used. Over optimism may also arise from cultural scripts such as "staying the course" and "weathering the storm" where a belief exists that persisting in the face of challenges will ultimately lead to overcoming the obstacle and achieving success (Keil, et al., 2000; Staw & Ross, 1987). Overall, the definition of over optimism adopted for this study is an absolute assurance and confident belief that the project will finish successfully (Keil, et al., 2000; Mayer & Schoorman, 1992). Optimistic bias has been shown to have a significant effect on escalation in failing projects (Meyer, 2014).

Sunk Cost Effect

The sunk cost effect is an irrational tendency to continue in an unproductive or failing course of action precipitated by past investments. In the context of project management and escalation theory, the sunk cost effect is typically fueled by a belief that the extent of prior investment is a legitimate reason to continue with a project along its existing planned course. There is a focal point on the loss that would occur if the project is terminated (Keil, et al., 2000). The rational possibility that continuing with the project as planned could result in even greater loss of time, money, and energy is forfeited for the conjecture that if a troubled project is continued at least some prior investment can be recaptured. The sunk cost effect is established in the literature as a key underlying influence in escalation, (Keil, et al., 2000; Sofis, Jarmolowics, Hudnall, & Reed, 2015) in addition strong effects of sunk cost have been noted in IT projects compared to non-IT project (Wang & Keil, 2007).

Perceived Responsibility

Perceived responsibility for the outcome of a project is a representative construct in self-justification theory (Brockner, 1992; Cheng et al., 2009; Keil, 1995). In general, self-justification encompasses a disregard or bias in the interpretation of negative information to justify the choice of prior investments and resources in a course of action (Brockner, 1992; Keil, et al., 2000; Staw & Ross, 1987). Studies have shown that the effect of this bias is not limited to those who have actual responsibility for the project, but also includes those who feel a sense of responsibility toward the project (Schultz-Hardt, Thurow-Kroning, & Frey, 2009). This bias has been supported as a significant contributing factor in escalation situations with troubled projects (Keil, et al., 2000; Cheng, Schultz, & Booth, 2009).

Completion Effect

The completion effect is characterized by the proximity of project completion as a motivational force to increase commitment to continuing a project, whether the project is on target for meeting its goals and objectives or is off-track and headed toward failure. Finishing the project essentially replaces the project target goals and organizational goals for which the project was originally initiated; this is similar to the goal substitution effect (Sleesman, Conlon, McNamara, & Niles, 2012). Completion becomes the predominant motivational force. Individuals become focused on reaching the end of the project instead of meeting those original goals and objectives (Barsky & Zyphur, 2016; Conlon & Garland, 1993; Zeigarnik, 1927). The closer one perceives the project is to finishing, the stronger the motivation to continue. The completion effect is identified as a contributing factor to the phenomenon of escalation (Keil, et al., 2000; Barsky & Zyphur, 2016) including having a strengthening effect on the relationship between sunk costs and escalation when it is covaried with sunk costs (Sleesman et al., 2012).

3. METHOD AND RESULTS

Data for this study was gathered from a web-based survey administered to individuals currently working in information technology-related projects. Participants were identified through contact with upper management (e.g. CIO) at several Fortune 500 organizations. The resulting sample included IT project team participants and primary decision makers. Out of a sample of 222 responses, 23 identified themselves as the primary decision maker and of these 23 managers only two were female. These 23 responses from primary decision makers were removed from the sample to avoid potential bias. The remaining 199 responses were divided into a sample of 113 (57%) males and a sample of 86 (43%) females. These numbers provide an unexpected opportunity with a larger than expected representation of females working on these IT projects.

Respondents to the survey were primarily between the ages of 30 and 49 (75%) with at least a 4-year college degree (79%). They had on average 9.9 years of experience at their organization and an average of 9.8 years of experience in IT. Demographic information is also included in the Appendices.

As the purpose of this research is to take an exploratory approach in examining whether differences exist in the aforementioned constructs between men and women in the sample, a simple t-test for equality of means was conducted for each construct between the two samples. A discussion of the results follows organized by IT project continuation, commitment-related constructs, and escalation-related constructs.

IT Project Continuation

An analysis of the difference between men and women for IT Project Continuation revealed that women are more inclined to continue an IT project (p=.01). The results of this analysis are shown in Table 1.

Construct	Mean	Std Deviation	Sig. (2-tail)
IT Project Continuation			
Male	**5.5**	**1.4**	**.01**
Female	**6.0**	**1.2**	

Table 1: IT Project Continuation Analysis Results

Commitment Constructs

Findings from our examination of commitment-related items indicate that women present higher levels of continuance commitment toward the project compared to men. There were no significant differences in their affective or normative commitment to the project. Detailed results for the commitment constructs can be found in Table 2.

Construct	Mean	Std Deviation	Sig. (2-tail)
Continuance Commitment			
Male	**3.4**	**1.4**	**.01**
Female	**4.0**	**1.4**	
Affective Commitment			
Male	5.1	1.4	.06
Female	5.5	1.3	
Normative Commitment			
Male	5.6	1.4	.07
Female	5.9	1.0	

Table 2: Commitment Construct Analysis Results

Escalation Constructs

Findings revealed that women were more likely to want or desire the project to be successful (goal valence/desirability) when compared to men. Women were less likely than men to perceive the project status as being negative or challenged and were more likely than men to be confident that the project would be successfully completed (over optimism).

Construct	Mean	Std Deviation	Sig. (2-tail)
Desire for Project Success			
Male	**5.9**	**1.1**	**.02**
Female	**6.2**	**.8**	
Negative Information			
Male	**4.7**	**1.2**	**.01**
Female	**4.2**	**1.4**	
Over Optimism			
Male	**4.7**	**1.7**	**.01**
Female	**5.2**	**1.3**	
Sunk Cost Effect			
Male	**4.3**	**1.8**	**.01**
Female	**4.9**	**1.4**	
Perceived Responsibility			
Male	4.6	1.6	.74
Female	4.7	1.6	
Completion Effect			
Male	4.5	1.7	.06
Female	4.9	1.3	

Table 3: Escalation Construct Analysis Results

In addition, women were more likely than men to view previous resource investments in the project as a good reason for continuing the project (sunk cost effect). There were no significant differences in their perception of perceived responsibility or their perception that the project was too close to completion to abandon. Specific findings can be found in Table 3.

4. DISCUSSION

This study indicates that differences exist in the level of commitment that men and women have to completing an IT project. There are many potential explanations for this study's findings rooted in previous research examining gender differences. While an exhaustive presentation of potential explanations is beyond the scope of the present work, a few potential explanations are outlined below.

One possible explanation for the differences we found in women and men's levels of project commitment might have to do with gender differences in risk aversion. Research has shown that women tend to be more risk averse than men (Croson & Gneezy, 2009; Eckel & Grossman, 2008). This may contribute to a tendency for women to remain committed to an existing project (even if challenged) rather than taking the risk of moving on to another project. Facebook Chief Operating Officer Sheryl Sandberg observed, "in my experience, more men look for stretch assignments and take on high-visibility projects, while more women hang back." (Sandberg, 2013 p. 62) She cited research stating this is especially true in situations where individual performance is emphasized and when women are working closely with men (Pater, Van Vianen, Fischer, & Van Genkil, 2009). Given that one or both of these elements is typically at work in the IT project environment, it might be that the environment itself contributes to increased levels of risk aversion for women, and hence a stronger desire to continue working on a given project.

Another potential explanation for why women would exhibit a higher continuance commitment and intention to continue is that women are more likely to perceive project failure as a form of personal failure. Previous research has shown that women are more likely than men to attribute failure to a lack of ability rather than external factors (Beyer, 1998). If project failure equates to personal failure, then there would be greater fear of negative professional consequences associated with project termination.

From an escalation theory standpoint, the fear of being associated with a project failure might also explain why the women in this study reported a stronger desire for project success and higher levels of over-optimism related to project success. That over-optimism might also explain why women were less likely to perceive a project as being challenged and more likely to experience the sunk cost effect. It may be that women are generally more willing to turn a blind eye to problems because they are more deeply invested in seeing the project through to completion.

Women might also be more likely to consider project termination to be a form of negative performance feedback. Prior research has shown that women experience greater drops in self-confidence and self-esteem than men when presented with negative feedback (Roberts & Nolan-Hoeksema, 1989; Johnson & Helgeson, 2002). To the extent that women consider project failure to be reflective of personal performance, they may exhibit higher continuance commitment as a means of avoiding these negative outcomes.

5. LIMITATIONS AND FUTURE RESEARCH

This study opens several interesting avenues for future research. As detailed in the discussion section, there are many possible explanations for the findings presented here. Each of those explanations detailed above - as well as others drawing from other relevant research streams - could serve as the basis for a future research.

In terms of limitations, the convenience sample used in the analysis only includes project team members, not those who identified as primary decision-makers. Future research direction would be examining whether the gender differences identified in this study hold when focusing on those with the power to make project decisions.

6. CONCLUSION

This study extends the existing literature by demonstrating that gender differences exist for some project commitment and escalation constructs. Previous research related specifically to project-based environments did not find differences in success factors when comparing males and females in key areas such as satisfaction and importance of meeting user requirements (Muller & Turner, 2007). Given the practical importance of learning more about the nuances of project success, there is great value in exploring gender differences

Two opportunities emerged from this research. First, we were able to examine the context of the IT project. Second, the data collected resulted in higher levels of females on the projects examined when compared to general expectations driven by the number of females in the profession. This could also warrant additional investigation related to the types of jobs women have in IT. Overall the numbers may be low, but in certain areas, like project management, they are higher.

One of the first items of interest to note related to our original sample for this analysis. Only two females held roles that defined them as the primary project decision-makers. There are many research studies that have examined this from several different contexts. A consensus coming from this body of research provides that when there are no women in higher level positions, there will tend to be fewer numbers of women in mid-level positions.

As noted, we are fortunate to have a nice representation of females in the sample we analyzed. As noted, the females did not hold positions of power. It would be interesting to look at women who are in the position to make decisions.

9. REFERENCES

Ahuja, M.K. & Thatcher, J.B. (2005). Moving Beyond Intentions and toward the Theory of Trying: Effects of Work Environment and Gender on Post-Adoption of Information Technology Use.

Ashcraft, C., McLain, B., & Eger, E. (2016). Women in tech: The facts.

Barsky, A. & Zyphur, M. (2016). Disentangling Sunk-Costs and Completion Proximity: The Role of Regulatory Focus. *Journal of Experimental Social Psychology*, 65, pp. 105-108.

Beyer, S. (1998). Gender differences in causal attributions by college students of performance on course examinations. *Current Psychology*, 17(4), 346.

Brockner, J. (1992). The escalation of commitment to a failing course of action: Toward theoretical progress. *Academy of Management Review*, 17(10), 39-61.

Buckle, P. & Thomas, J. (2003). Deconstructing Project Management: A Gender Analysis of Project Management Guidelines. *International Journal of Project Management*, 21, pp. 433-441.

Cartwright, S. & Gale, A. (1995). Project Management: Different Gender, Different Culture? A Discussion on Gender and Organizational Culture Part 2. *Leadership and Organization Development Journal*, 16(4), pp. 12-16.

Cheng, M., Schultz, A., & Booth, P. (2009) Knowledge Transfer in Project Reviews: The Effect of Self-Justification Bias and Moral Hazard. *Accounting and Finance*, 49, pp. 75-93.

Cheng, M., A. Schulz, P. Booth, and P. Luckett, 2003, The effects of hurdle rates on the level of escalation of commitment in capital budgeting, *Behavioural Research in Accounting* 15, 63–85.

Conlon, D. & Garland, H. (1993). The Role of Project Completion Information in Resource Allocation Decisions. *Academy of Management Journal*, 362, pp. 402-413.

Croson, R., & Gneezy, U. (2009). Gender differences in preferences. *Journal of Economic literature*, 47(2), 448-474.

Eckel, C. C., & Grossman, P. J. (2008). Men, women and risk aversion: Experimental evidence. *Handbook of experimental economics results*, 1, 1061-1073.

Feingold, A. (1994). Gender Differences in Personality: A Meta-Analysis. *Psychological Bulletin*, 116(3), pp. 429-456.

Fox, S., & Hoffman, M. (2002). Escalation behavior as a specific case of goal-directed activity: A persistence paradigm. *Basic and Applied Social Psychology*, 24(4), 273-285.

Henderson, L.S. & Stackman, R.W. (2010). An Exploratory Study of Gender in Project Management: Interrelationships with Role, Location, Technology, and Project Cost. *Project Management Journal,* 41(5), pp. 37-55.

Johnson, M., & Helgeson, V. S. (2002). Sex differences in response to evaluative feedback: A field study. *Psychology of Women Quarterly*, 26(3), 242-251.

Keil, M. (1995). Pulling the Plug: Software Project Management and the Problem of Project Escalation. *MIS Quarterly*, 19, pp. 421-447.

Keil, M, Mann, J. & Rai, A. (2000). Why Software Projects Escalate: An Empirical Analysis and Test of Four Theoretical Models. *MIS Quarterly*, 24(4), pp. 631-664.

Keil, M., & Robey, D. (1999). Turning around troubled software projects: An exploratory study of the deescalation of commitment to failing courses of action. *Journal of Management Information Systems*, 15(4), 63-87.

Keil, M., Smith, H. J., Pawlowski, S., & Jin, L. (2004). 'Why didn't somebody tell me?': climate, information asymmetry, and bad news about troubled projects. ACM SIGMIS Database, 35(2), 65-84.

Korzaan, M. and Brooks, N. (2015). The Silent Treatment in IT Projects: Gender Differences in Inclinations to Communicate Project Status Information. *Journal of Information Systems Applied Research*, 8(1), pp. 19-30.

Korzaan, M. and Brooks, N. (2015). The Binding and Blinding Influence of Project Commitment. *Information Resources Management Journal*, 28(1), pp. 57-74.

Lee, J., Keil, M., & Wong, K. (2015). The Effect of Goal Difficulty on Escalation of Commitment. *Journal of Behavioral Decision Making*, 28, pp. 114-129.

Lewin, K. (1935). Principles of topological psychology. New York: McGraw-Hill.

Lindgren, M. & Packendorff, J. (2006). What's New in New Forms of Organizing? On the Construction of Gender in Project-Based Work. *Journal of Management Studies*, 43(4), pp. 841-866.

Mayer, R. C. and Schoorman, F. D. (1992). Predicting participation and production outcomes through a two-dimensional model of organizational commitment. *Academy of Management Review,* 35(3), 671-684.

Meyer, W.G. (2014). The Effect of Optimism Bias on the Decision to Terminate Failing Projects. *Project Management Journal*, 45(4), pp. 7-20.

Montealegre, R., & Keil, M. (2000). De-escalating information technology projects: Lessons from the Denver International Airport. *MIS Quarterly*, 417-447.

Muller, R. & Turner, R. (2007). The Influence of Project Managers on Project Success Criteria and Project Success by Type of Project. *European Management Journal*, 25(4), pp. 298-309.

Newman, M., & Sabherwal, R. (1996). Determinants of commitment to information systems development: a longitudinal investigation. *MIS Quarterly*, 23-54.

Pater, E., Van Vianen, A., Fischer, A., & Van Genkil, W. (2009). Gender Differences in Task Choice. *Journal of Managerial Psychology*, 24(1), pp. 4-28.

Powell, M. & Ansic, D. (1997). Gender Differences in Risk Behavior in Financial Decision-Making: An Experimental Analysis. *Journal of Economic Psychology*, 18, pp. 605-628.

Roberts, T. A., & Nolen-Hoeksema, S. (1989). Sex differences in reactions to evaluative feedback. *Sex Roles*, 21(11-12), 725-747.

Sandberg, S. (2013). Lean in: Women, work, and the will to lead (First edition). New York: Alfred A. Knopf.

Schulz-Hardt, S., Thurow-Kroning, B. & Frey, D. (2009). Preference-based Escalation: A New Interpretation for the Responsibility Effect in Escalating Commitment and Entrapment. *Organizational Behavior and Human Decision Processes*, 108, pp. 175-186.

Sleesman, D., Conlon, D., McNamara, G., & Miles, J. (2012). Cleaning Up the Big Muddy: A Meta-Analytic Review of the Determinants of Escalation of Commitment. *Academy of Management Journal*, 55(3), pp. 541-562.

Sofis, M., Jarmolowics, D., Hudnall, J, & Reed, D. (2015). On Sunk Costs and Escalation. *Psychological Record*, 65(3), pp. 487-494.

Staw, B. M. and Ross, J. (1987). Behavior in escalation situations: Antecedents, prototypes, and solutions. *Research in Organizational Behavior*, 9, 39-78.

Wang, J. & Keil, M. (2007). A Meta-Analysis Comparing the Sunk cost Effect for IT and Non-IT Projects. *Information Resources Management Journal,* 20(3), pp. 1-18.

Venkatesh, V., Morris, M.G., & Ackerman, P.L. (2000). A Longitudinal Field Investigation of Gender Differences in Individual Technology Adoption Decision-Making Processes. *Organizational Behavior and Human Decision Processes*, 83(1), pp. 33-60.

Zeigarnik, B. (1927). On the retention of completed and uncompleted activities. *Psychologische Forschung*, *9*, 1-85

Editor's Note:

This paper was selected for inclusion in the journal as a CONISAR 2017 Distinguished Paper. The acceptance rate is typically 7% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2017.

.

Appendices

IT Project Continuation (Bhattacherjee, 2001; Korzaan & Brooks, 2015)	
Given the choice of whether or not to continue this project, how likely is it that you personally would	
IC1	Continue with the project
IC2	Persist until the project is completed
IC3	Continue with the project as planned
IC4	Keep investing resources in the project
Continuance Commitment (Mayer & Schoorman, 1992; Korzaan & Brooks, 2015)	
CC1	It would be hard on me if the project was cancelled at this time and I had to switch to a different project
CC2	I would be missing out on a lot if this project was cancelled
CC3	There would be significant costs for me if this project is abandoned now
CC4	It would be quite a loss for me if this project was cancelled
Affective Commitment (Mayer & Schoorman, 1992; Korzaan & Brooks, 2015)	
AC1	For me, this is one of the best projects to work on
AC2	I am proud to tell others that I am working on this project
AC3	I talk up this project to my colleagues as a good project to work on
AC4	This project inspires the best in me in the way of job performance
Normative Commitment (Akhtar and Tan, 1994; Korzaan & Brooks, 2015)	
NC1	I feel that it is my duty to support the project
NC2	I feel a sense of obligation toward this project
NC3	I feel a strong sense of responsibility toward this project
Desire for Project Success (Goal Valence/Desirability) **(Bagozzi et al, 2003; Elliot et al, 2000; Dholakia & Bagozzi, 2002)**	
DPS1	It is important to me that the project be successfully completed
DPS2	It is my desire for this project to be successfully completed
DPS3	I care very much about whether the project is successful or not
DPS4	I am often motivated on this project by my desire to see the project succeed

Table 4: Survey Items for Commitment Constructs and IT Project Continuation

Negative Information (Keil et al., 2004; Keil and Robey, 1999; Montealegre and Keil, 2000)	
While working on the project I often feel	
NI1	There are many challenges that must be overcome before this project can succeed
NI2	This project will need to overcome several obstacles
Over Optimism (Mayer & Schoorman, 1992; Korzaan & Brooks, 2015)	
Regarding this project, I am often	
OO1	Completely sure the project will finish successfully
OO2	Absolutely positive that this project will be a success
Sunk Cost Effect (Keil et al., 2000)	
Consider your reaction to the possible reasons for continuing this project:	
SCE1	Past investments in this project are a good reason to continue with this project
SCE2	There has been too much invested in this project to cancel the project
SCE3	There have already been too many resources allocated to this project to quit now
Completion Effect (Keil et al., 2000)	
Consider your reaction to the possible reasons for continuing this project:	
CE1	We have come too far on the project to quit now
CE2	We are close enough to the end of the project that we should keep going
CE3	Every day we get closer to the end of this project, so we should not quit the project
Perceived Responsibility (Schoorman & Holahan, 1996)	
RES1	The project’s performance is a reflection on me personally
RES2	I am responsible for the project’s outcome
RES3	I am accountable for the project’s success

Table 5: Survey Items for Escalation Constructs

	Male	Female
Gender	57%	43%

	20-29 yrs	30-39 yrs	40-49 yrs	>= 50 yrs
Age	12%	30%	45%	13%

	High School	Some College	Associate's Degree	4-year Degree	> 4-year Degree
Education	6%	9%	6%	61%	18%

Table 6: Respondent Demographics

Information Security and Privacy Legislation: Current State and Future Direction

Lex Dunlap
ad4991@uncw.edu

Jeff Cummings
cummingsj@uncw.edu

Thomas Janicki
janickit@uncw.edu

Department of Business Analytics, Information Systems and Supply Chain
University of North Carolina Wilmington
Wilmington, NC 28403

Abstract

The field of information security and privacy is continually growing and evolving to meet the needs of both individuals and organizations. While individuals may still struggle securing their own data, organizations must follow specific regulations concerning any data they hold that is considered private (e.g., social security number, driver's license number, etc.). However, the challenge for most organizations is understanding those regulation as they exist at both the federal and state level. Complicating matters further is the fact that laws may differ from state to state. The current research examines the security and privacy landscape that organizations must navigate. The goal is to get a better understanding of federal and state security/privacy laws while discussing future directions that should be taken at both levels to ensure the privacy and security of an individual's data.

Keywords: Information Security, privacy, regulation, laws

1. INTRODUCTION

Information security and privacy issues continue to dominate the news such as the recent WannaCry ransomware which has attacked over 200,000 computers in 150 countries (Sherr, 2017). These types of attacks target both businesses and consumers alike, emphasizing how quickly an individual's data may be compromised. Additionally, with the recent passage of legislation enabling Internet Service Providers (ISPs) to collect and disseminate customer information, the need for organizations to understand privacy continues to increase (Washington Post, 2017). Businesses, institutions, and customers alike need to consider how sensitive data is being managed. For companies, this requires not only an understanding of security methods necessary for maintaining data, but also the regulations and requirements organizations are legally bound to uphold.

The National Institute of Standards and Technology (NIST) defines information security as "the protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (Nieles, Dempsey and Pilliteri, 2017, p.2)." This research is concerned with confidentiality or "preserving authorized restrictions on information access and disclosure, including means of protecting personal privacy and proprietary information (Nieles et al. 2017, p.2)." Each company is required to adhere to the laws that are applicable to their corporation and the states in which they conduct business. This means each company must understand the laws that exist at both the federal and state levels. While there are some federal laws regarding the security of specific types of data (e.g., medical information or financial information), organizations often struggle to understand how to keep individual data secure as many of these laws vary based on the location of the company and the individual. Surprisingly, most security and privacy laws remain at the state level making organizational compliance daunting as states may have varying laws. The goal of this research is to get a better understanding of the current state of security and privacy laws in the US while providing some suggestions for future directions. In the following sections, we examine the varying viewpoints of what is "private data" and how current federal regulations impact organizations. In addition, a discussion of security and privacy laws at the state level will occur to understand how private information is handled from state to state. We conclude with a discussion of the possibilities moving forward and potential changes that may help with consumer data privacy. This research reflects the viewpoint of the information held by companies on individuals and not on the data held by individuals on themselves.

2. CURRENT SECURITY AND PRIVACY LAWS

Currently, laws and regulations regarding security and privacy of an individual's information exists at both the federal and state level. While most laws have been passed at the state level, we will discuss both levels in the following sections. However, we first discuss the idea behind what is considered private data to provide better context to the discussion surrounding laws protecting such data.

What is private data?

There has been a great deal of discussion as to what private information is and what it is not. The Federal Trade Commission (FTC) distinguishes data as being either "public" or "non-public" personal data. Public data is considered to be anything that is "reasonably" believed to be publicly available (e.g., telephone numbers listed in a directory). Non-public personal data is defined as data that is "personally identifiable financial information" (c.f. https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm). An example of this may be information such as Social Security Number, income, etc. that may be given while applying for loan.

However, not all data needs to be financial to be considered private. With online availability of a variety of information (e.g., health records), the definition of private data is continually evolving. Under Section 1171 (Part C of Subtitle F), health information includes anything oral or recorded that is received by the health care provider which relates to the past, present or future of any individual. Because so much data is now stored/available online, a succinct definition is difficult and has caused issues concerning what is or isn't private data.

For example, in 2016, legislation was passed that required ISPs to get permission from customers (or have them opt-in) whereas before the ISP could sell their data and browsing history (Coldewey, 2016). Less than a year later, new legislation repealed the law, going back to the system where customers are required to explicitly request for their information to remain private (Hatmaker, 2017). Thus, the overruling of the "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services Act" has demonstrated that the idea of "private data" is continually changing and there are differing views of private data from an ISP's perspective compared to a consumer idea of private data.

For the current discussion, private data will be defined as personal data the individual does not want to make available to the public. This includes things such as passwords, financial records, personally identifiable records (e.g., social security number).

Federal Laws

Currently, the primary information security law that has provided guidelines for subsequent law s is the *Federal Information Security Management Act of 2002* or FISMA (US Congress, 2002a). While this legislation does not apply directly to the private sector, and instead mandates a certain type of behavior from the public sector, it is an important foundational piece of legislation which has helped to inform subsequent policy and can be used to justify security practices in the private sector. FISMA, "requires the Director to establish and operate a central Federal information security incident center; and head of each agency operating or controlling a national security system to take measures to protect such system." This legislation mandates the creation and operation of an information security incident center. This requirement is helpful in providing a precedent for other organizations to follow, noting that creating a place for managing security incidents and protecting systems that possess sensitive information is a followed practice by the US government.

FISMA also states that standards will be issued by the National Institute of Standards and Technology (NIST), and that each Director, must assist in promulgating standards. The implicit rationale with mandating that the National Institute of Standards and Technology oversee developing and submitting guidelines, is that experts who are well informed regarding the most current threats can continually update and redefine standards. More will be discussed on the importance of NIST in the discussion section.

While having a bill that mandates all departments in the US Government comply with a set information security standards, creating legislation that accomplishes the same goal for all sections of the private sector has proven to be a challenge. Because of the variety of data collected and stored by different industries and companies, much of the regulation within the private sector has been industry specific. The following are a few of the industry specific laws currently in place:

- **Sarbanes-Oxley Act of 2002 (SOA)**
  This act dictates that companies who handle financial records must retain them for at least seven years (US Congress, 2002b). This act applies to accounting firms, and any type of organization the manages financial records. SOA has been amended several times since its passage into a law to bolster penalties for companies who have been failing to comply with regulations. The Public Company Accounting Oversight Board (PCAOB) is charged with overseeing, regulating and disciplining.

- **Health Insurance Portability and Accountability Act of 1996 (HIPPA)**
  This act applies to any and all offices which handle data related to healthcare of patients and, in an effort to simplify healthcare, shifts information to electronic form while protecting a patient's personal health information (US Congress, 1996). This legislation has very clear standards regarding who should be able to have access to patient data, and how this data should be stored and managed. Health and Human Service's Office of Civil Rights is charged with enforcing these regulations.

- **Gramm-Leach-Bliley Act**
  This act dictates that financial institutions are required to protect private information of clients and customers. The Federal Trade Commission (FTC) currently helps to enforce this act (US Congress, 1999).

- **Family Educational Rights and Privacy Act of 2011 (FERPA)**
  This act applies to a student's records and the rights of parents to see (or not see) performance and other evaluative data. This act applies to those schools receiving federal funding for any program. It does have an exemption for the types of data that might be seen by parents of a minor.

These laws are some of the most commonly referenced legislation that applies to the private and potentially public sector and relates to information security. However, this does not cover many of the issues commonly associated with security breaches and privacy issues. This evokes the question: Do the laws that we currently have in place protect consumer data and information? This is often left to individual states which will be discussed next.

State Laws

In addition to the federal restrictions that are in place, companies must also be aware of local (i.e., state) laws that mandate specific types of security protocol or procedure for managing sensitive data, or reporting compromises of that data. Much of the legislation concerning privacy and security of individual data has been placed at the state instead of the federal level. Because of this, it is common for new cybersecurity legislation to be introduced yearly at the state levels to keep up with the ever-changing cybersecurity landscape.

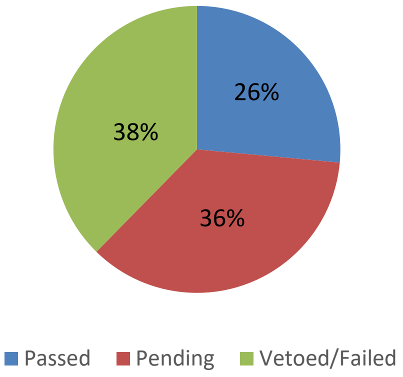


Figure 1. 2015-16 State Security Legislation Introduced and Status

For example, per the National Conference on State Legislatures (www.ncsl.org), over 170 new cybersecurity laws have been introduced across 37 states in the past 2 years (2015-2016). Figure 1 shows how many of these have passed, are pending votes or have been vetoed/failed. The data reflects that while 38% have failed to receive legislative approval, over 60% are still in the consideration stage. This shows the ever-evolving landscape of legislation that organizations must address.

The most active states in this arena are New York, California and Washington. Surprisingly, Delaware which has a significant number of corporations registered only had 2 laws pertaining to privacy and security
At the state level, laws concerning security and privacy include security breach notifications, data disposal and identity theft protection. While there are other laws that vary state to state, these laws and regulations are specifically focused on individual data and are common in most states. These laws will be discussed further in the following subsections.

Security Breach Laws
Currently, 48 states as well as Puerto Rico and the District of Columbia have passed laws requiring both private and government agencies to notify individuals when breaches occur. These will typically include: who should be informed, a definition of what private data is, what constitutes a breach, etc. The first such law was enacted by the state of California in 2002.

California State Bill 1386 states that:

> "Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person (California State Senate, 2002, Section 1798.82 a)."

As this law set the basis for most other state breach laws, it is important to point out that it specifically relates to businesses that conduct business in California and the distinction of California residents. Thus, in states such as Alabama and South Dakota which lack such laws, there is no legal obligation to notify residents of security breaches. The challenge for organizations is that with 48 states writing their own privacy and security laws there are many varying requirements.

Data Disposal Laws
As of the end of 2016, 31 states and Puerto Rico have enacted laws pertaining to: "the destruction, disposition or otherwise make personal information unreadable or undecipherable". (National Conference of State Legislature (NCSL)). The FTC (Federal Trade Commission) has also enacted legislation requiring the proper disposal of individuals' information.

Interestingly, of the states that have passed data disposal laws, all the laws apply to businesses within their state, but only 13 of 31 apply to state and local governments. Following is an example from the state of Delaware on what must be destroyed to make these data elements non-readable:

> "Personal identifying information'' means a consumer's first name or first initial and last name in combination with any 1 of the following data elements that relate to the consumer, when either the name or the data elements are not encrypted: Social Security number; passport number; driver's license or state identification card number; insurance policy number; financial services account number; bank account number; credit card number; debit card number; tax or payroll information or confidential health-care information including all information relating to a patient's health-care history; diagnosis condition, treatment; or evaluation obtained from a health-care provider who has treated the patient which explicitly or by implication identifies a particular patient.(State of Delaware, Title 6, Commerce and Trade, Chapter 50, 2014)."

In the area of data disposal, the federal government through the FTC and the Graham Leach Bliley Act tend to provide significant guidance as most states have deferred to the FTC guidelines in the area of financial records. The FTC defines proper disposal as:

> "Practices that are reasonable and appropriate to prevent the unauthorized access to – or use of – information in a consumer report. For example, reasonable measures for disposing of consumer report information could include establishing and complying with policies to: burn, pulverize, or shred papers containing consumer report information so that the information cannot be read or reconstructed; destroy or erase electronic files or media

> containing consumer report information so that the information cannot be read or reconstructed; conduct due diligence and hire a document destruction contractor to dispose of material specifically identified as consumer report information consistent with the Rule (Federal Trade Commission, 2017)."

In summary, the data disposal laws provide clearer guidelines than other areas of data privacy as the records are more tangible in either electronic or written form.

Identity Theft Protection Laws

In just the past two years, federal legislation was written to future enhance Identity Theft (Department of Justice, 2017). This legislation defines identity theft as knowingly using another individual's identifying information for illegal purposes. At the state level, all 50 states have passed some form of identity theft laws, with the penalty ranging from felonies in Alabama to just misdemeanors in Virginia. NCSL, 2017).

Several states have enacted more stringent legislation. An example is the North Carolina "Identity Theft Protection Act," which describes the consumer's rights to their data and information, allowing them to effectively 'freeze' companies out of obtaining copies of the individual's credit report. The legislation also mandates that companies take "reasonable measures to protect against unauthorized access to or use of…" sensitive data, and requires businesses to report security breaches if any consumer data has been compromised. Per the North Carolina Department of Justice, 3,400 breaches have been reported, which have affected 9.3 million North Carolina consumers. While potentially burdensome to monitor this information, it is clear that requiring companies to report breaches is an important part of the legal infrastructure around information security. If breaches in security did not mandate a report, millions of consumers could be at risk to damaged credit, identity theft, and other forms of crime. The state of North Carolina has prioritized the importance of their citizens to be protected, and informed when they need to make changes in order to remain safe. (North Carolina, 2005).

Legislatures also face the dueling priorities of increased data privacy and protection versus the costs to businesses. A recently introduced bill mandates a report which reflects the cost of, "(1) security for computers, networks, software, storage systems, data transmission, equipment, and support services; (2) measures to mitigate and hedge against compromises of information systems; and (3) economic loss or harm caused by such compromises." The findings in such a report could lead to some sweeping improvements in upcoming bills. Reporting on the cost of security measures versus the cost of security breaches and how that directly effects the economy could produce updated legislation that focuses on flexible and agile methods for mandating security. This would provide companies with requirements for protecting consumer data, while allowing them to do so in a way that was cost effective and could easily be updated or modified to adjust to new, yet unknown, threats.

3. DISCUSSION OF FUTURE CYBERSECURITY LEGISLATION

Security and privacy legislation continues to evolve at both the state and federal level. As previously mentioned, laws at the federal level focus on specific industries while state laws attempt to focus on individuals within those states. The following section discusses the current issues with legislation and potential direction the US should follow moving forward.

Private Data

One issue present in both federal and state laws is the definition of what is and what is not private. Federal laws are based on the industry they regulate thus much of the definition of private data is industry specific (e.g., HIPPA focusing on health information). However, while many state laws are similar, there is no requirement to be consistent across states when it comes to the definition of private data at the state level. We recommend that this is something that should be addressed at the federal level to provide a constant definition regardless of residency. However, this may be a moot point as recent surveys have shown that many of the employees working with private data may not know the laws in place.

While there is an argument over what type of personal data should be protected, or considered private, a new survey conducted by Dell, shows that even if legislation requires groups and companies to adhere to strict guidelines regarding sensitive information, it may not be enough. The survey resulted in having 72 percent of professionals stating that they would be willing to share sensitive, confidential or regulated information (Dell Technologies, 2017). This type of overwhelming response is frightening in its implications, leading us to believe that regulations and compliance policy for protecting information and data are relatively useless in the face of disregard for said policies.

While the reports of the study go on to explain some of the circumstances in which employees might have felt it was acceptable to share data, companies should be taking more responsibility for explaining the importance of maintaining proper security practices when it comes to sensitive information. Thus, not only should there be a definition of private data at the federal level, there must also be a change in how organizations inform their employees of such laws and regulations relation to privacy and security.

Federal or State?
The broader concern for security and privacy laws lies in where these laws exist – the federal level or state level. Currently, federal laws are enforced across a broad range of agencies including the Federal Trade Commission (FTC), Health & Human Services and the Public Company Accounting Oversight Board. In 2016, under the Obama administration, the Cybersecurity National Action Plan was implemented to help move the US enhance cybersecurity awareness and protections (Daniel, et al., 2016). While much of the plan focused on the federal level, it also had actions to enable individuals to increase security (e.g., requiring multi-factor authentication) to protect their identity online. However, while the action plan was a step forward, it was only an action plan with no specific legislation tied to it. We recommend that future 'state' laws cease to exempt themselves from the privacy laws and impose restrictions upon state and local government for compliance.

Recently, the new administration has issued an Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (Gottlieb, 2017). This requires federal agencies to adopt of the Framework for Improving Critical Infrastructure Cybersecurity developed by NIST. While this is an important step forward for federal agencies, the order does not require any private agencies to follow such guidelines. This is where the federal agencies can be proactive by requiring the implementation of NIST guidelines in organization across the US to increase the security of the infrastructure which in turn reduces the need of breach notification laws.

What should occur at the state level? This is a question that has stirred much debate in the cybersecurity industry. Some states have been much more proactive than others. California and New York lead with more developed and stringent security laws. For example, New York recently enacted legislation requiring financial firms to go beyond compliance of Gramm-Leach-Bliley Act (Reuters, 2017). These regulations include increased scrutinization of third-party vendor security, risk assessments to design programs specific to the firm and an annual certification of compliance. While this covers firms in New York, what happens to those operating in Chicago or Boston? It is evident that the focus on standardization at the federal level must also be implemented at a state level as well. An example of the exposure to third party vendor liability was the 2014 theft of consumer accounts at Target Stores. The theft occurred via the network of a heating and air vendor.

Nature of Cybersecurity
One of the most important questions is whether complying corresponds to more secure information. The goal of creating regulation to protect information and sensitive data is for that data to be secure and private. However, Black (2017) suggests there is a clear defect in regulation as it lags far behind the innovation of those trying to get to the data (i.e., hackers or the 'bad guys'). He argues that current iterations of cyber and information security policy are outdated compared to the current threats especially as companies focus on compliance with a law that was designed to protect against threats that are several iterations older than its current form. The article proports that the expense of coming into compliance is so heavy that companies are dissuaded from pursing real security measures, which seem to add more cost, without providing any legal incentive. As noted earlier legislatures are incorporating consideration of the costs of implementation versus potential loss of data into their future laws.

The author claims that providing legislation that requires companies to protect consumer data and not to disclose it without approval and having the legislation remain open ended regarding the implementation of any security measures used in order to maintain security over the consumer's private data is the best method for providing actual compliance, and allowing for companies to continue to grow flexibly and expand their security measures in an elastic way (Black). This theory, however, assumes that the company has tech experts who are able to implement flexible, high level, agile systems. Unfortunately, there are many businesses without the means to do so. By ridding legislation of any details in how to get into compliance, information security becomes a much larger hurdle for companies who are not steeped in information security systems.

Business' Perspective

While security and privacy laws are in place to protect the individual, companies must also shoulder the burden of these laws, often at a cost to the organization. Even within larger companies, executives like CIOs, Security Officers and other experts are often expected to know which laws apply their respective industry and how to apply the requirements to their prospective programs, however that does not always happen to be true (Burke 2003). While the details on compliance are stated in the laws themselves, the challenge is finding the full laws and knowing which ones are required to be compliant. This becomes more difficult for small companies who wish to work as contractors for the government, an odd place where the public and private sector meet and in addition to your local and federal legislation you must also consider FISMA. This can be so overwhelming as to detract companies who could provide services to the government from pursuing that option, it can also scare people away from creating new businesses in general.

Beyond understanding which regulations are applicable, the burden of becoming compliant are substantial for both small and large companies, as your companies grow so does the required scale of your security apparatuses. For smaller companies the financial expense can be business-squashing. Being able to afford an expert in security will be out of reach for many small businesses, and hiring a third-party company is a large upfront cost for a company who is just getting started. Because of these costs, it is likely that many startups either forego security compliance, or fail to invest in the company's growth potential. A bright spot for smaller firms will be the moving of their data centers to cloud service providers that will be able to provide increased security not feasible for smaller firms. Larger companies often face the same choices, as updating security systems becomes so overwhelming that they either update too slowly, or potentially stagnate due to inability to handle more growth based on their current systems (Vanderburg, 2011).

4. CONCLUSION / RECOMMENDATIONS

The question of protection of an individual's security and privacy of data is not easily answered. The landscape for both individuals and organizations is vast and often challenging to understand. Ultimately, it may come down to the federal government to lead the race to security and privacy regulations for securing systems. However, these regulations are also in desperate need of revamping.

Much of the current federal legislation was originally drafted in the 90s or early 2000s, fifteen to twenty-five years later the requirements for maintaining up to date security measures look very different. The rate at which threats that exist to information security are evolving continue to grow at a steady clip. While regulations can be burdensome to companies, ridding the government of the responsibility to hold institutions accountable for maintain privacy for citizen's private data would be unconscionable. Instead, amending legislation in an effort to produce a more flexible system for maintaining compliance with regulations would be a welcome shift to the current processes that are in place. Having updated standards of security results used as a measurement of compliance, as opposed to having detailed methods of hardware and network setup would be much more effective, particularly for larger companies, or companies with onsite technology experts with the capacity for implementing a proper security system.

State legislatures also need to be involved as they tend to enact more legislation in this area. It is imperative that security associations work with state representatives to provide them the expertise to enact meaningful legislation at the state and local area.

This does not necessarily solve the problem for smaller companies, who may not have access to experts, or the funding to hire them. A possible solution to this problem would be to have a certification program for hardware that falls into compliance with the current security standards, and to make this list of certified hardware available to the private sector. Part of the certification condition would be that the hardware must be updated on a consistent basis, to provide security updates to all businesses who purchased the hardware in an effort for that company's hardware to remain compliant. This would rid small businesses of the need to have on site experts, and they could instead focus the time and energy on growing their company. In addition to requiring certain hardware parameters, companies should be required to hold more training sessions, or produce some sort of reporting showing that their employee base is staying up to date with proper information security handling procedures.

Employees should be required, by law, if handling sensitive information, to either obtain some type of certification as evidence of their competence in information handling, or the employer should be able to produce some type of proof of their training system and employee retention of relevant material.

While the perfect ratio of regulation to innovation in the realm of information security remains obscured, the perpetual buzz of threats, viruses, and exposed information continues to become a louder noise in the zeitgeist. As the conversation continues to grow, in addition to providing more context for businesses to take information security seriously, it should also allow for consumers to become more educated about where they choose to spend their money and share their personal information with.

If a company is known to sell information, or handle sensitive data sloppily, consumers should become more aware and choose not to associate with that organization. Although regulations may produce added cost to companies, they also provide a level of protection and resource for consumers, an important aspect that society is still struggling to understand.

5. REFERENCES

Black, D. (2017, May 2). Security Regulations vs. Cybersecurity: the War. White Paper. Coralville: SANS Institute InfoSec Reading Room. Retrieved May 3 2017 from http://www.huffingtonpost.com/entry/security-regulations-vs-cyber-security-the-war_us_59089d7ce4b03b105b44bc22

Burke, T. (2003). U.S. Government IT Security Laws. SANS Institute InfoSec Reading Room. Retrieved April 30 2017 from https://www.sans.org/reading-room/whitepapers/legal/us-government-security-laws-1306

California State Senate (2002). California State Bill 1386, Personal Information: privacy. Sacramento, CA.

Coldewey, D. (2016, October 27). New FCC rule protects users from the prying eyes of ISPs. Retrieved May 24, 2017 from https://techcrunch.com/2016/10/27/new-fcc-rule-protects-users-from-the-prying-eyes-of-isps/

Daniel, M., Scott, T. and Felten, E. (2016). The President’s National Cybersecurity Plan: What You Need to Know. The White House Blog. Retrieved June 6, 2017 from https://obamawhitehouse.archives.gov/blog/2016/02/09/presidents-national-cybersecurity-plan-what-you-need-know

Dell Technologies (2017). Dell End User Survey 2017. Retrieved May 24, 2017 from http://dellsecurity.dell.com/wp-content/uploads/2017/04/2017-Dell-End-User-Security-Survey_FINAL.pdf

Department of Justice (2017). Identify Theft: What are Identify Theft and Identity Fraud?. Last Retrieved June 7, 2017 from https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

Federal Trade Commission (2017). Disposing of Consumer Report Information. Retrieved June 5, 2017 from https://www.ftc.gov/tips-advice/business-center/guidance/disposing-consumer-report-information-rule-tells-how

Financial Services Committee (2002). *Sarbanes-Oxley Act of 2002*: United States Congress.

Gottlieb, R. (2017, May 25). President's Executive Order on Cybersecurity: Impact on Banks Unclear. Retrieved June 2, 2017 from http://www.lexology.com/library/detail.aspx?g=c02d0271-d879-493d-a5ec-ff3b85ee7bf4

Hatmaker, T. (2017, March 28). Congress just voted to let internet providers sell your browsing history. Retrieved May 24, 2017 from https://techcrunch.com/2017/03/28/house-vote-sj-34-isp-regulations-fcc/

National Conference of State Legislatures (2017). Data Disposal Laws. Retrieved June 1, 2017 from http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx

NCSL (2017). Identity Theft. Retrieved 6/6/2017. https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

Nieles, M., Dempsey, K., and Yan Pilliteri, V. (2017). An Introduction to Information Security. National Institute of Standards and Technology. Retrieved June 7, 2017 from http://csrc.nist.gov/publications/drafts/800-12r1/sp800_12_r1_draft.pdf

North Carolina (2005) Chapter 75 Article 2A. Identity Theft Protection Act. 2005. Bill. Retrieved June 7, 2017 from http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/ByArticle/Chapter_75/Article_2A.html

Reuters. (2017, February 16). Here's When New York State's Cybersecurity Rules Take Effect. *Fortune*.com. Retrieved May 15, 2017 from http://fortune.com/2017/02/16/newyorkstatecybersecurityregulation/

Sherr, I. (2017). WannaCry ransomware: Everything you need to know. Retrieved May 23, 2017 from https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/

State of Delaware (2016). Safe Destruction of Records Containing Personal Identifying information. Retrieved June 5, 2017 from http://delcode.delaware.gov/title6/c050c/index.shtml

Vanderburg, E. (2011). Information Security Compliance: Which regulations relate to me? Retrieved April 30, 2017 from http://www.jurinnov.com/information-security-compliance-which-regulations/

Washington Post (2017), "What to expect now that Internet Providers can collect and sell your browser history, Retrieved 6/5/2017, https://www.washingtonpost.com/news/the-switch/wp/2017/03/29/what-to-expect-now-that-internet-providers-can-collect-and-sell-your-web-browser-history/?utm_term=.437383d9f7d3

US Congress (1996). Health Insurance Portability and Accountability Act of 1996. Washington, DC.

US Congress (1999). Gramm-Leach-Bliley Act. Washington, DC.

US Congress (2002a). Federal Information Security Management Act of 2002. Washington, DC.

US Congress (2002b). Sarbanes-Oxley Act of 2002. Washington, DC

Protecting IoT Devices from the Mirai Botnet

Charles Frank
charles.frank@trojans.dsu.edu

Samuel Jarocki
samuel.jarocki@trojans.dsu.edu

Cory Nance
cory.nance@trojans.dsu.edu

Wayne E Pauli
wayne.pauli@dsu.edu

Dakota State University
Madison, SD

Abstract

This paper details the Mirai botnet capabilities to perform massive DDoS attacks and reviews existing research to detect and prevent Mirai botnets. The Mirai architecture is presented and a code audit is performed to analyze how the malware is loaded onto a device, joins the botnet, and searches for new victims. Based upon the code analysis, novel signatures were discovered. A hardening script for IoT devices was created to prevent the botnet from loading the Mirai malware onto a device. Another script was on the IoT device to detect and prevent communication to the CNC server. A test environment was orchestrated consisting of a Mirai CNC, loader, and several simulated IoT devices. The hardening script was shown to be successful in preventing the initial Mirai malware infection on the IoT device, and the detection script was successful in recognizing and stopping an already existing infection on the Mirai bot. The conclusion section suggests future possible research directions.

Keywords: Mirai, IoT, botnet, DDoS, malware, detection, prevention

1. INTRODUCTION

Currently, there is an estimated 15 billion Internet of Things (IoT) devices. By 2020, the estimate is projected to be as high as 50 billion connected IoT devices (Higginbotham S, 2016). IoT incorporates the internetworking of physical devices, smart devices, smart buildings, smart cars, medical device, etc.; embedded with electronics, software, sensors, actuators, and internet connectivity. These objects collect and exchange data (Internet of Things, n.d.).

The value of IoT comes from the data it generates and the feedback it provides, such as real-time data analytics, insights, and improvements (Gorlich, K., 2016). There exist a myriad of applications for IoT, ranging from non-critical applications, such as wearables (e.g. smart watches), to crucial applications in healthcare (e.g. IoT smart medical device dispensing medicine to hospital patients (IoT Applications with Examples, 2016), military, and battlefield utilization (Goldstein, P., n.d.). IoT applications play an integrated role in people's everyday lives and clearly there are many IoT devices, and that number will grow exponentially over time

(Higginbotham S, 2016). Depending upon the IoT application, security could be paramount.

2. BOTNET HISTORY

In 1999, Sub7 (Gamblin, J., 2017) and Prettypark (Hariston K., Rozman, N., et al, n.d.) constructed an IRC channel to gain control of victim machines to issue malicious commands. In 2000, Global Threat Bot (GTBot) was based on the mIRC client (Fandom, n.d.). GTBot could run custom scripts in response to IRC events and had access to TCP and UDP sockets, allowing for Denial of Service (DoS) attacks. Also, GTBot scanned for Sub7 infected hosts and updated them to GTbots (Global Threat Bot, 2017).

In 2002 notable evolutions in botnet technology were observed with SDBot and Agobot. SDBot's source code was released to the public via the author; thus many subsequent bots include code or ideas from SDBot (Trend Micro, "Countermeasures..., n.d.). Agobot introduced the concept of a modular, staged attack, as payloads were delivered sequentially (Trend Micro, "SDBOT", n.d.). The initial attack installed a back door and used stealth techniques to avoid detection from antivirus. These early botnets concentrated on remote control and information theft (Global Threat Bot, 2017).

More advanced bot functionality began to set the stage for greater data exfiltration and service disruption and circumvention techniques. In 2003 Spybot (aka Rbot) included keylogging, information stealing, spam, and DDoS capabilities (Argobot, n.d.). The command and control (CNC) was conducted over IRC. Sinit was the first peer-to-peer botnet (Dark Reading, n.d.). Polybot employed polymorphism to avoid detection by changing its appearance as often as possible (Global Threat Bot, 2017). Later in 2005, Bagle and Bobax were the first spamming botnets, and the malware Mytob was a mailing worm based upon MyDoom and SDbot (Trendmicro, WORM_SPYBOT.A, n.d.); enabling large botnets distributed across many infected PCs. Soon after, in 2006, another invasive spamming botnet RuStock (Trendmicro, CounterMeasures Security, Privacy & Trust, n.d.) appeared, utilizing self-propagation. Undoubtedly, in a short period of time, botnets started to become more sophisticated in attacking, evading detection, and multiplying.

ZeuS is an information stealing tool that first appeared in 2010. ZeuS quickly became the most widely used information stealing botnet. Part of its appeal is that it includes simple point and click interfaces for managing infected machines. Zeus is regularly updated and new versions have been offered for sale, while older versions have been distributed online free of charge (Trendmicro, WORM_SPYBOT.A, n.d.). At this point, not only have botnets gotten more sophisticated in their method of infection via email spamming but they are now concerned with ease of use via point and click interfaces.

2014 witnessed many high-profile attacks; from an internet-connected refrigerator participating in a botnet sending over 750,000 spam emails (Rapid7, IOT Seeker, n.d.) to a DDoS attack of IoT devices successfully affecting availability of Sony and Microsoft's gaming networks Constantin, L., 2017). In December 2016, researchers from Imperva detected a colossal 650 Gbps DDoS attack generated by a new IoT botnet, named Leet (Simonroses.com, n.d.).

In April of 2017, Unit 42 researchers have identified a new variant of the IoT Linux botnet Tsunami, coined Amnesia (Jia, Y., Xiao, C., & Zheng, C., 2017). Amnesia targets an unpatched remote code execution vulnerability that was publicly disclosed in March 2016 in DVR (digital video recorder) devices made by TVT Digital. It is believed Amnesia is the first Linux malware to adopt virtual machine evasion techniques to defeat malware analysis sandboxes. Currently, Amnesia has not been used to mount large scale attacks.

Shown in Fig. 1, Wikipedia (Zeus, n.d.) presents a historical list of botnets, with many of the botnets described in the previous paragraphs. Currently, there are thousands of botnets that the Shadowserver Foundation is tracking (Botnet, n.d.). Typically, Trend Micro tracks tens of millions of infected PCs that are being used to send spam; and that does not include all the other infected PCs that are being used for information theft, DDoS or other botnet crimes (Trendmicro.eu, 2017).

3.MIRAI BOTNET

The Mirai botnet wreaked havoc on the internet in 2016. The botnet takes advantage of unsecured IoT devices that leave administrative channels (e.g. telnet/SSH) open and use well known, factory default, usernames and passwords. Mirai scans the internet looking for new systems to infest, such as those manufactured by XiongMai Technologies that had default passwords set in their firmware (prior to September 2015) which cannot be changed unless upgraded. These devices are especially vulnerable to the Mirai botnet, as well as other exploit payloads due to their insecure default firmware (Buntinx J.P., 2016). Mirai's size makes it a very powerful botnet capable of producing massive throughput. For example, in September of 2016, the Mirai botnet is reported to have generated 620 Gbps in its DDoS attack on "Kreb's on Security" (Mirai, n.d.).

In October 2016, the source code for Mirai was leaked on HackForums (ShadowServer, n.d.). This release has helped security researchers to better understand Mirai capabilities and how it works. Mirai performs wide-ranging scans of IP addresses with the intentions of locating IoT devices that can be remotely accessed via easily guessable login credentials, usually factory default usernames and passwords (e.g., admin/admin) (ShadowServer, n.d.).

Mirai is using several functions from the Linux kernel API related to network operations. For example, in killer.c there is a function named *killer_init* that kills several services: telnet (port 23), ssh (port 22) and http (port 80) to prevent others from accessing the compromised IoT device. (Femerling, 2016).

Mirai comes with a list of default/weak passwords to perform brute force attacks on IoT devices [29]. Mirai's attack function enables it to launch HTTP floods and various network (OSI layer 3-4) DDoS attacks. For network layer assaults, Mirai is capable of launching GRE IP and GRE ETH floods, SYN and ACK floods, STOMP (Simple Text Oriented Message Protocol) floods, DNS floods and UDP flood attacks (ShadowServer, n.d.).

There is even a "don't mess with" list for IP addresses (e.g. the United States Post Office, Dept. of Defense, and private IP space) and several killer scripts meant to eradicate other worms and trojans. Since the Mirai source code has been leaked, many variants have been detected. A few interesting variants include: the use of a DGA (Domain Generation Algorithm) Incapsula.com, n.d.) and trojanized Windows payloads that incorporate Mirai scanning (cfengine.com, n.d.).

To conclude, each bot scans for new bots to infect using the default list of usernames and passwords. Once a bot finds a new vulnerable device it forwards the IP, port, credentials, and device architecture to the ScanListener.

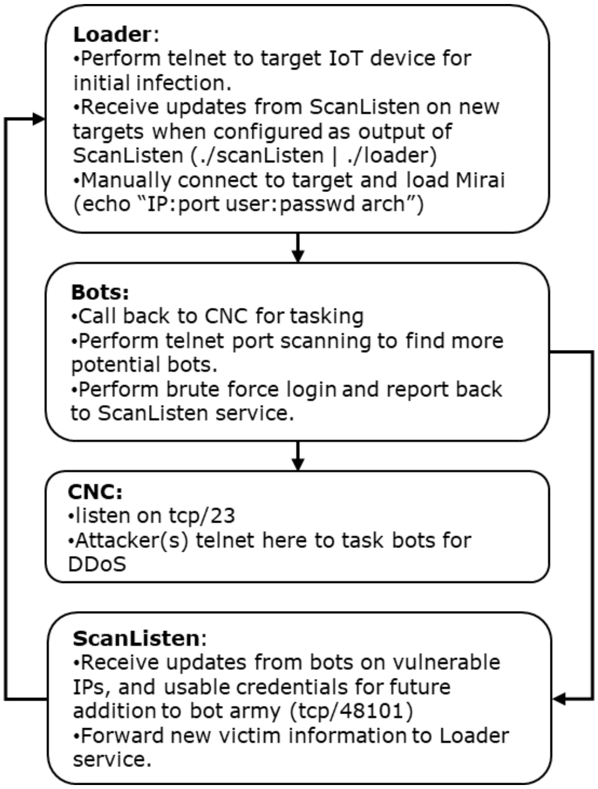

Loader:
•Perform telnet to target IoT device for initial infection.
•Receive updates from ScanListen on new targets when configured as output of ScanListen (./scanListen | ./loader)
•Manually connect to target and load Mirai (echo "IP:port user:passwd arch")
Bots:
•Call back to CNC for tasking
•Perform telnet port scanning to find more potential bots.
•Perform brute force login and report back to ScanListen service.
CNC:
•listen on tcp/23
•Attacker(s) telnet here to task bots for DDoS
ScanListen:
•Receive updates from bots on vulnerable IPs, and usable credentials for future addition to bot army (tcp/48101)
•Forward new victim information to Loader service.

Figure 2 Mirai Architecture

The ScanListener does the part of actually infecting the device. Once the IoT device has been infected with the Mirai malware via telnet and has become a bot, the CNC will communicate with the bot to execute DDoS attacks.

4. MIRAI CODE AUDIT

Tintorera calculated that Mirai is a small project and not too complicated to review (Roses S., 2016). The ScanListener, Loader, and the malware executing on the bots are written in the C programming language. The CNC is written in the GO language.

Figure 3 shows an example of the default administrative user id and password list utilized by bots for the telnet scanning and the CNC's ScanListener. The list is comprised of an obfuscated userid and password combination that is deobfuscated for attempting to log into the potential bot victim via telnet.

Three upload methods are utilized for uploading the Mirai malware onto the IoT device by the CNC Loader. Figure 4 shows, in sequential order, the Loader attempts to find: (1) wget (2) tftp (3) echo. The first utility found on the victim will be selected to perform the upload of the malware by the CNC.

```
func main() {
        tel, err := net.Listen("tcp", "0.0.0.0:23")
        if err != nil {
        fmt.Println(err)
        return
        }
```

Figure 5 CNC Listener

Shown above, the CNC Listens on port 23 for telnet traffic from bots. The CNC tasks bots for DDoS attacks.

5. BOTNET DETECTION AND PREVENTION

Recent studies from the INSuRE (Information Security Research and Education) research group have focused on IoT botnets (INSuRE, Online). In Kovacoc and Vargas (n.d.), an analysis of current botnets and botnet operations, command and control infrastructure, and detection approaches were presented. Rudesh (n.d.) determines the characteristics of Thingbots, identifies IoT devices that can participate in the botnet and determines a detection, isolation, and mitigation technique for Thingbots by reviewing existing techniques. Another project detected IoT botnets through the spreading of the hosts which have the botnet detection tool installed on them. Baki presents peer-to-peer botnet detection through Machine Learning (ML) (n.d.) (Abay, C., Hagel, L., & Williams, K., n.d.) isolates and analyzes a Zeus botnet node, and (Freeman, L., Hickey, R., etal, n.d.) develops a testbed for botnet countermeasures.

There are also efforts to secure IoT devices. One novel approach is using blockchain technology where security software on the kernel of the IoT device could receive a blacklist of IP addresses over the blockchain. (Faife, C., n.d.). Another study found a stack buffer overflow vulnerability in the Mirai malware that allows the malware to be crashed on the bot (Leyden, J., 2016). Lastly, an anti-worm "nematode" has been developed that could help to patch vulnerable devices and to help prevent Mirai bots (Pauli, D., 2016).

Figure 6 illustrates international research conducted by a team from Japan and Germany. The team, led by Yin Minn Pa Pa, and Shogo Suzuki authored an article on analyzing the rise of IoT compromises. The increasing threats against IoT devices show that telnet-based attacks that target IoT devices have skyrocketed since 2014 (Pa Pa, Y, Suzuki, S, etal, n.d.). With analysis from IotPOT, a honeypot for IoT, Fig. 6 indicates that there are at least four distinct DDoS malware families targeting telnet-enabled IoT devices.

Many of the patterns have common command sequences such as checking for the victim's shell and then eventually downloading the malicious binary. Compared to the other patterns, ZORRO 3 contained many more command sequences per day.

ShadowServer (Botnet, n.d.) suggests the best way to mitigate botnets is to keep them from forming. Botnets would not be a threat if they could not propagate and infect vast numbers of systems. IoT Seeker (Seals, T., n.d.) scans for IoT devices which could easily be hijacked by botnets. Methods of preventing IoT botnets from spreading are suggested by stopping the use of default/generic passwords and disabling all remote (WAN) access to your devices (ShadowServer, n.d.). CFEngine (Arghire, I., n.d.) significantly reduces end-point attack surface by: (1) closing any unnecessary services, especially remote access services, (2) changing factory default user accounts, (3) removing unnecessary software, and (4) avoiding legacy protocols and password logins. With the recent advent of trojanized Windows payloads that incorporate Mirai scanning and reporting within an intranet environment (cfengine.com, n.d.), the security offered by rejecting and blocking publicly accessible ports/services is diminished.

6. PROPOSED IOT HARDENING SCRIPTS

Two scripts are proposed for hardening IoT devices from Mirai: (1) antimirai.py and (2) secure.sh. antimirai.py is a python script that makes various changes on the IoT device, such as: (1) changing the default password (2) creating a busybox wrapper to filter out applets used by Mirai (3) changing the logon banner and (4) implementing */etc/host.deny*. These changes attempt to prevent the infection of Mirai on the IoT device.

Shown in Fig. 7, *replace_busybox()* will copy the existing busybox binary, on the IoT device, to *tmp_busybox*. Then, a busybox wrapper is created and the commands that are executed by the Mirai loader to upload the malware are detected [*words="telnet wget tftp"*]. In an attempt to prevent Mirai infection, these commands will return a success [0], even though the commands are prevented from being executed on the actual IoT device.

Shown in Fig. 8, the *change_passwd_telnet()* method will generate a new random password for the administrator of the IoT device. Lastly, *upload_run_script()* will upload and run the *secure.sh* script. *secure.sh* is a script that detects Mirai infections and reacts by stopping the Mirai malware from running.

Fig. 9 shows *secure.sh*, a busybox ash (Almquist shell) script. Once a bot is infected with Mirai, it opens a connection back to the CNC server on port 23 and runs 3 processes with the same randomly generated name. This script works by checking */proc/net/tcp* for a socket that has a remote connection to port 23 (0x17). It then locates the PID of the socket. With the socket's PID, the script locates the process's name and then sends the SIGKILL signal to each process with the same name, effectively stopping the infection and any communication with the CNC server.

In conclusion, *antimiarai.py* is a python script to harden the IoT device from Mirai infections. Not only will *antimaria.py* make configuration changes that prevent Mirai infections but it will also upload *secure.sh*. The script *secure.sh* is an ash script that will continuously check for an indication of the Mirai malware running. Once Mirai is found to be running, it is immediately killed. This combination of scripts should prevent an IoT device from becoming a part of the Mirai botnet.

7. TESTING ENVIRONMENT

The testing environment runs in virtual machines (VMs) on an isolated private network. It consists of two VMs. One houses the CNC and loader, while the other represents a vulnerable Linux-based IoT device. The vulnerable VM is running Ubuntu 14.04 with busybox, is configured with a default username and password, and is running busybox's telnetd on port 23. For each test, the loader was manually executed to attempt Mirai infections against the vulnerable VM.

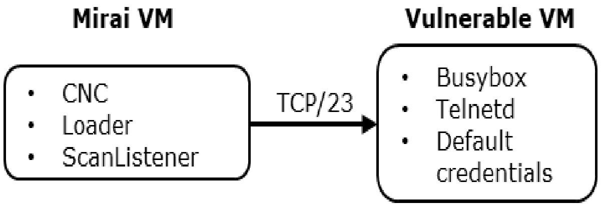


Figure 10 Testing Server Configuration

As shown above, the Mirai server and the simulated IoT Device contain private IP addresses. These private IP addresses isolate the testing environment from the publically routable internet. A Vagrant file (http://vagrantup.com) was used to orchestrate the creation of the VMs and private network (Nance, C., n.d.).

8. TESTING RESULTS

The hardening script (*antimirai.py*) was tested to determine the feasibility and outcome from basic protection (changing default password), obfuscation (modifying banner and changing server port), and redirection (wrapping busybox applets used for malicious functions). Not all functionality was incorporated due to platform and time limitations. Platform limitations such as telnet and/or ssh services not being compiled with the tcp wrapper library (libwrap) lack the host-based access control lists system to leverage additions to */etc/hosts.allow* and */etc/hosts.deny*, thereby rendering that specific hardening action ineffectual. Inability to disable/modify the superuser account (e.g. root), while not hindering device functionality, constituted a time limitation. Additional obfuscation techniques would provide demonstrations of change without furthering a proof-of-concept.

Execution of *antimirai.py* hardening script produced predictable results based on the testing environment and conditions. Issuing a change of default password to a random alphanumeric string is an effectual method for thwarting Mirai's scanner, and subsequent infection. Changing banner (via */etc/motd, /etc/issue, /etc/issue.net*) was not successful in preventing infection. Mirai inspects login prompt, such as *$, :, #*, etc. provided by telnetd/sshd.

Action	Expected Outcome	Actual Outcome
change password	Not infected	Not infected
change userid	Not infected	Not infected
change banner	Not infected	Infected
change telnet port	Not infected	Not infected
busybox wrapper to prevent Mirai malware upload	Not infected	Not infected
detect and prevent CNC communication	Infected then removed	Infected then removed

Figure 12 antimirai.py test results

There are multiple methods to changing login prompt based on platform; and available commands and configurations on host, thereby not feasible for implementation within time constraints. Modification of default service port prevented infection, however this method does not prevent a port scan from discovering new listening port.

Service detection paired with banner return may offer additional obfuscation (not tested). On-the-fly creation and deployment of a busybox wrapper script to intercept applets Mirai requires to download it's binary to a target device (e.g. wget, telnet, ftp) was successful in preventing infection.

Finally, deployment and execution of the *secure.sh* script, barring any other hardening techniques, successfully terminated repeated Mirai bot infections on target host. The *secure.sh* script was successful in detecting and subsequently terminating all infection attempts based on defined parameters of time and service port detection. Logically, any combination of multiple hardening techniques deployed to a viable host would offer increased protection within their individual limitations to provide a multi-faceted strategy of defense.

9. CONCLUSION

Mirai is an IoT botnet that has executed massive DDoS attacks on websites and internet services. It infects IoT devices via remote access thru telnet and default administrative ids and passwords. The CNC loads the malware onto the bot as well as controls the commands for various DDoS attacks. The bot responds to the commands and probes for new IoT devices to join the Mirai botnet.

Our research focused on detecting and preventing Mirai infections on the IoT device. Code auditing was shown to be effective in determining novel signatures for detecting communication between the CNC and the bot for loading the Mirai malware and trying to recruit new bots. Based upon code auditing, scripts were created and testing shows that the prevention script was effective at preventing a Mirai malware infection and the detection script was successful at detecting and removing Mirai malware from an infected bot.

Future research should include a more comprehensive code analysis of Mirai which encompasses all of the components of Mirai. Also, research should entail generating more comprehensive signatures for indicators of compromise for the IoT device, including network traffic analysis. Lastly, a more robust and complex testing environment would provide for more comprehensive testing and analysis.

10. REFERENCES

Abay, C., Hagel, L., & Williams, K. (n.d.). Peer-to-Peer Botnet Detection, Retrieved 29-Jan-2017 from https://purr.purdue.edu/projects/insurefall2016/files/browse?subdir=Projects/Botnet%20Study.

Arghire, I., (n.d.) New Mirai Variants Have Built-in Domain Generation Algorithm, Retrieved from http://www.securityweek.com/new-mirai-variants-have-built-domain-generation-algorithm

Argobot, (n.d.). Wikipedia. Retrieved 07-Feb-2017 from https://en.wikipedia.org/wiki/Agobot.

Baki, S., (n.d.). Network Under Control: Optimal Node Selection for Installing Botnet Detection Software Retrieved 29-Jan-2017 from https://purr.purdue.edu/projects/insurefall2016/files/browse?subdir=Projects/Botnet%20Study.

Botnet, (n.d.). Wikipedia Retrieved 07-Feb-2017 from https://en.wikipedia.org/wiki/Botnet.

Buntinx, J.P., (2016, Oct. 24). XiongMai Technologies Admits Their Devices Are Susceptible To Mirai Malware. *The Merkle*. Retrieved 30-Jan-2017 from https://themerkle.com/xiongmai-technologies-admits-their-devices-are-susceptible-to-Mirai-malware/.

Buntinx, J.P., (n.d.), Updated Mirai Botnet Malware Executes 54-hour DDoS Attack Retrieved 09-April-2017 from https://themerkle.com/updated-mirai-botnet-malware-executes-54-hour-DDoS-attack/.

CFEngine, (n.d.), Industrial Internet of Things – Systems Hardening, Retrieved from https://cfengine.com/solutions/industrial-iot-systems-hardening/

Constantin, L., (n.d.) Windows Trojan hacks into embedded devices to install Mirai, *PCWorld*, 09-Feb-2017

DarkReading, (n.d.). The World's Biggest Botnets, Retrieved 07-Feb-2017 from http://www.darkreading.com/the-worlds-biggest-botnets-/d/d-id/1129117?

Faife, C., (n.d.). This Bitcoin Botnet is Vying to Be Future of Secure IoT Retrieved 09-April-2017 from http://www.coindesk.com/this-bitcoin-botnet-is-vying-to-be-future-of-secure-iot/

Fandom, (n.d.). Virus Information. Prettypark, Retrieved 06-Feb-2017 from http://virus.wikia.com/wiki/Prettypark.

Femerling, S.R., (n.d.), "Mirai DDoS Botnet: Source Code & Binary Analysis," Retrieved from http://www.simonroses.com/2016/10/mirai-DDoS-botnet-source-code-binary-analysis/

Freeman, R., Hickey, R., Robertson, J., & Yeske, J., (n.d.).Botnet Study Retrieved 29-Jan-2017 from https://purr.purdue.edu/projects/insurefall2016/files/browse?subdir=Projects/Botnet%20Study.

Gamblin, J., (2017, Jan.07). Mirai-Source-Code. *GitHub*. Retrieved 30-Jan-2017 from https://github.com/jgamblin/Mirai-Source-Code.

Global Threat Bot (GTBot). (2017, Feb. 8). Technopedia Retrieved 08-Feb-2017 from https://www.techopedia.com/definition/59/global-threat-bot-gtbot.

Goldstein, P., (2016, May). The Internet of Things for the Battlefield Needs to Be Flexible, Army Official Says Retrieved 09-APR-2017 from http://www.fedtechmagazine.com/article/2016/05/internet-things-battlefield-needs-be-flexible-army-official-says.

Görlich, K., (2016, Jun. 20). Live Business: The Importance of the Internet of Things. *Digitalist Magazine*

Hariston, J., Rozman, K., Sissom, N., & Wright, D., (n.d.). Botnet Counterstrike: Implementation of Botnet Enclave Testbed Retrieved 29-Jan-2017 from https://purr.purdue.edu/projects/insurefall2016/files/browse?subdir=Projects/Botnet%20Study.

Hertig, A., (n.d.), Mirai, The Infamous Internet of Things Army, Can Now Mine Bitcoin Retrieved 10-April-2017 from http://www.coindesk.com/mirai-infamous-internet-things-army-can-now-mine-bitcoin/

Higginbotham, S. (2016, Mar. 18). Prediction: there won't be 50B connected IoT devices by 2020. *Structure Connect*. Retrieved 28-Jan-2017 from http://www.structureconnect.com/prediction-there-wont-be-50b-connected-iot-devices-by-2020/.

Imperva Incapsula (n.d.), Breaking Down Mirai: An IoT DDoS Botnet Analysis, Retrieved 29-Jan-2017 from https://www.incapsula.com/blog/malware-analysis-mirai-DDoS-botnet.html

INSuRE, Information Security Research and Education. (n.d.). Retrieved 29-Jan-2017 from https://purr.purdue.edu/projects/insurefall2016/files/browse?subdir=Projects/Botnet%20Study.

IoT Applications with Examples. (2016, Oct, 24). Internet of Things Wiki. Retrieved 28-Jan-2017 from http://internetofthingswiki.com/iot-applications-examples/541/

Internet of Things. (n.d.). Retrieved 28-Jan-2017 from https://en.wikipedia.org/wiki/Internet_of_things

Jia, Y., Xiao C., & Zheng, C., (April 2017) New IoT/Linux Malware Targets DVRs, Forms Botnet. Retrieved April 9, 2017 from http://researchcenter.paloaltonetworks.com/2017/04/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/?utm_source=hs_email&utm_medium=email&utm_content=50167168&_hsenc=p2ANqtz-9HGnfET3w5_BRVaC_tp_iEiHppZRK2tQPfem4dhiM3iP-7N6HvbaHLQBBKeebc_OFkSk_mw_1A7uzGlXIIUIt8HaASWw&_hsmi=50167168

Kovacoc, T., & Vargas, J., Botnet Study Retrieved 29-Jan-2017 from https://purr.purdue.edu/projects/insurefall2016/files/browse?subdir=Projects/Bo

Leyden, J., (2016, Oct) Researchers expose Mirai vulnerabilities that could be used to hack back against botnet Retrieved 09-April-2017 from http://www.theregister.co.uk/2016/10/28/mirai_botnet_hack_back/botnet%20Study.

Mirai. (n.d.). Wikipedia. Retrieved 26-Jan-2017 from https://en.wikipedia.org/wiki/Mirai.

Nance, C. (n.d.). miai. *GitHub* Retrieved 10-APR-2017. from https://github.com/canance/mirai?files=1

Pa Pa, Y.M., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T., & Rossow, C., (n.d.) IoTPOT: analyzing the rise of IoT compromises Retrieved 26-Feb-2017 from https://www.usenix.org/system/files/conference/woot15/woot15-paper-pa.pdf

Pauli, D., (2016, Oct). Boffin's anti-worm bot could silence epic Mirai DDoS attack army Retrieved 09-April-2017 from https://www.theregister.co.uk/2016/10/31/this_antiworm_patch_bot_could_silence_epic_mirai_DDoS_attack_army/

Rapid7, (n.d.). IOT Seeker, Retrieved from https://information.rapid7.com/iotseeker

Roses, S. (2016, Oct). Mirai DDoS Botnet: Source Code & Binary Analysis. Retrieved 8-Jan-2018 from http://www.simonroses.com/2016/10/mirai-DDoS-botnet-source-code-binary-analysis/

Rudesh, V., (n.d.). Thing bot Analysis and Detection Retrieved 29-Jan-2017 from https://purr.purdue.edu/projects/insurefall2016/files/browse?subdir=Projects/Botnet%20Study.

Seals, T., (n.d.). Leet IoT Botnet Bursts on the Scene with Massive DDoS Attack, Retrieved from https://www.infosecurity-magazine.com/news/leet-iot-botnet-bursts-on-the-scene/

ShadowServer, (n.d.). Retrieved 7-Feb-2017 from https://www.shadowserver.org/wiki/.

Trend Micro, (n.d.). CounterMeasures Security, Privacy & Trust. The history of the botnet – Part I Retrieved 06-Feb-2017 from http://countermeasures.trendmicro.eu/the-history-of-the-botnet-part-i/.

Trend Micro, (n.d.). CounterMeasures Security, Privacy & Trust. The history of the botnet – Part II Retrieved 08-Feb-2017 from http://countermeasures.trendmicro.eu/the-history-of-the-botnet-part-ii/.

Trend Micro, (n.d.). SDBOT, Retrieved 06-Feb-2017 from http://countermeasures.trendmicro. .com/vinfo/us/threat-encyclopedia/malware/sdbot

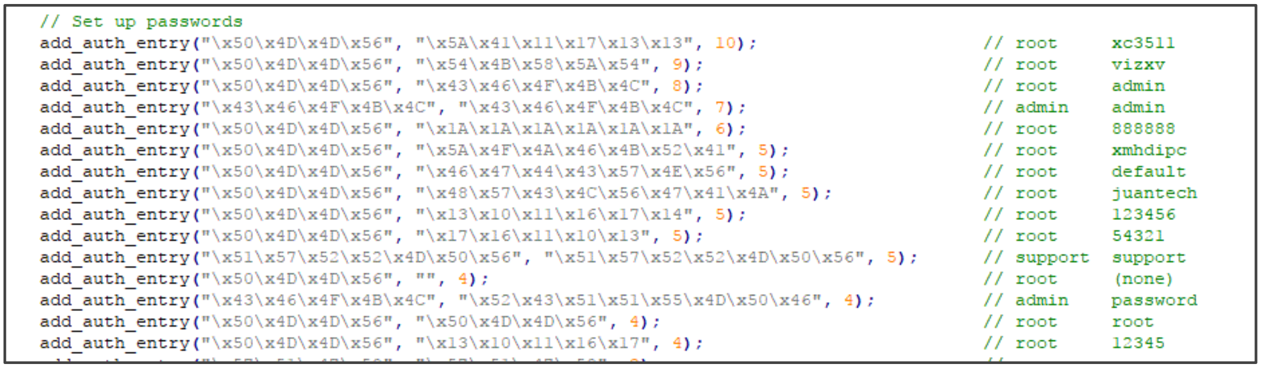
Trend Micro, (n.d.). WORM_SPYBOT.A Retrieved 07-Feb-2017 from https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/WORM_SPYBOT.A

Zeus, (n.d.). Wikipedia. Retrieved 07-Feb-2017 from https://en.wikipedia.org/wiki/Zeus.

APPENDIX

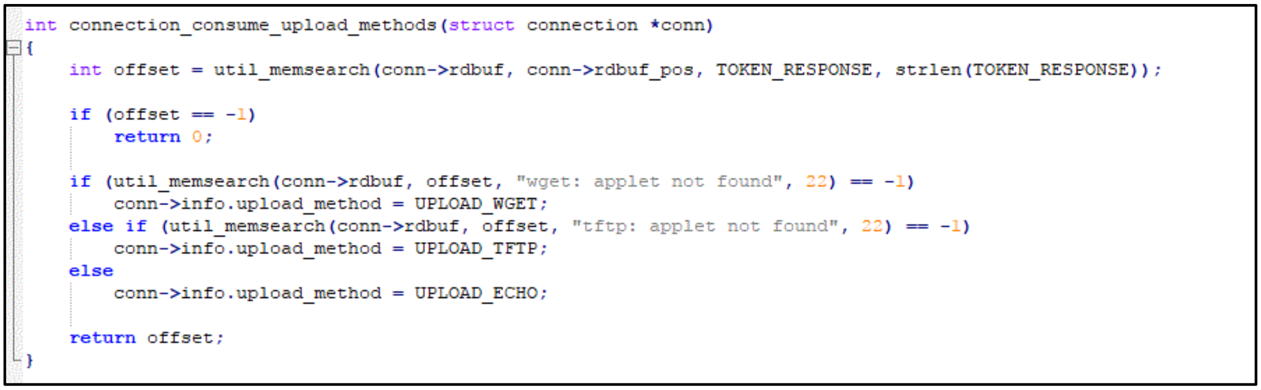
Date created	Name	Estimated no. of bots	Aliases
2004 (Early)	Bagle	230,000	Beagle, Mitglieder, Lodeight
	Marina Botnet	6,215,000	Damon Briant, BOB.dc, Cotmonger, Hacktool.Spammer, Kraken
	Torpig	180,000	Sinowal, Anserin
	Storm	160,000	Nuwar, Peacomm, Zhelatin
2006 (around)	Rustock	150,000	RKRustok, Costrat
	Donbot	125,000	Buzus, Bachsoy
2007 (around)	Cutwail	1,500,000	Pandex, Mutant (related to: Wigon, Pushdo)
2007	Akbot	1,300,000	
2007 (March)	Srizbi	450,000	Cbeplay, Exchanger
	Lethic	260,000	none
2007 (September)	dBot	10,000+ (Europe)	dentaoBot, d-net, SDBOT
	Xarvester	10,000	Rlsloup, Pixoliz
2008 (around)	Sality	1,000,000	Sector, Kuku
2008 (around)	Mariposa	12,000,000	
2008 (November)	Conficker	10,500,000+	DownUp, DownAndUp, DownAdUp, Kido
2008 (November)	Waledac	80,000	Waled, Waledpak
	Maazben	50,000	None
	Onewordsub	40,000	
	Gheg	30,000	Tofsee, Mondera
	Nucrypt	20,000	Loosky, Locksky
	Wopla	20,000	Pokier, Slogger, Cryptic
2008 (around)	Asprox	15,000	Danmec, Hydraflux
	Spamthru	12,000	Spam-DComServ, Covesmer, Xmiler
2008 (around)	Gumblar		
2009 (May)	BredoLab	30,000,000	Oficla
2009 (Around)	Grum	560,000	Tedroo
	Mega-D	509,000	Ozdok
	Kraken	495,000	Kracken
2009 (August)	Festi	250,000	Spamnost
2010 (January)	LowSec	11,000+	LowSecurity, FreeMoney, Ring0.Tools
2010 (around)	TDL4	4,500,000	TDSS, Alureon
	Zeus	3,600,000 (US only)	Zbot, PRG, Wsnpoem, Gorhax, Kneber
2010	Kelihos	300,000+	Hlux
2011 or earlier	Ramnit	3,000,000	
2012 (Around)	Chameleon	120,000	None
2016 (August)	Mirai (malware)	380,000	None

Figure 1 Wikipedia Historical Timeline of Botnets



```
// Set up passwords
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);           // root     xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                // root     vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                // root     admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);            // admin    admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);            // root     888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);        // root     xmhdipc
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);        // root     default
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);    // root     juantech
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);            // root     123456
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                // root     54321
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);  // support  support
add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                    // root     (none)
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);  // admin    password
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                    // root     root
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);                // root     12345
```

Figure 3 Scanner Default Admin. Password List



```
int connection_consume_upload_methods(struct connection *conn)
{
    int offset = util_memsearch(conn->rdbuf, conn->rdbuf_pos, TOKEN_RESPONSE, strlen(TOKEN_RESPONSE));

    if (offset == -1)
        return 0;

    if (util_memsearch(conn->rdbuf, offset, "wget: applet not found", 22) == -1)
        conn->info.upload_method = UPLOAD_WGET;
    else if (util_memsearch(conn->rdbuf, offset, "tftp: applet not found", 22) == -1)
        conn->info.upload_method = UPLOAD_TFTP;
    else
        conn->info.upload_method = UPLOAD_ECHO;

    return offset;
}
```

Figure 4 CNC Upload Methods

Pattern Name	Pattern of Command Sequence	Set of Command Sequence per Day (Average)
ZORRO 1	1. Check type of victim shell with command "sh" 2. Check error reply of victim by running non-existing command such as ZORRO. 3. Check whether wget command is usable or not. 4. Check whether busybox shell can be used or not by echoing ZORRO.	#
	5. Remove various command and files under /usr/bin/, /bin, var/run/, /dev. 6. Copy /bin/sh to random file name 7. Append series of binaries to random file name of step 6 and make attacker's own shell 8. Using attacker's own shell, download binary . IP Address and port number of malware download server can be seen in the command. 9. Run binary	
ZORRO 2	1. Check type of victim shell with command "sh" 2. Check error reply of victim by running non-existing command such as ZORRO. 3. Check whether wget command is usable or not. 4. Check whether busybox shell can be used or not by echoing ZORRO.	#
	6. Copy /bin/sh to random file name 7. Append series of binaries to random file name of step 6 and make attacker's own shell 8. Using attacker's own shell, download binary . IP Address and port	

	number of malware download server cannot be seen in the command because it is hard coded in the attacker's own shell. 9. Run binary	
ZORRO 3	1. Check type of victim shell with command "sh" 2. Check error reply of victim by running non-existing command such as ZORRO. 3. Check whether wget command is usable or not. 4. Check whether busybox shell can be used or not by echoing.	174
	5. Remove all under /var/run, /dev, /tmp, /var/tmp 6. Copy /bin/sh to random file name 7. Append series of binaries to random file name of step 6 and make attacker's own shell 8. Using attacker's own shell, download binary. IP Address of malware download server can be seen in the command and port number cannot be seen in the command 9. Run binary	1,353
Bashlite	1. Check whether shell can be used or not by echoing "gayfgt" 2. Download shell script. 3. Using downloaded shell script, kill previously running malicious process, download malware binaries of different CPU architectures and block 23/TCP in order to prevent other infection. 4. Run all downloaded malware binaries.	606
nttpd	1. Check whether shell can be used or not by echoing "welcome" 2. Download binary to /tmp directory. 3. Run Binary.	3.2
KOS	1. Check whether shell can be used or not by echoing "$?K_O_S_T_Y_P_E" 2. List /proc/self/exe 3. Check all running process 4. Download malware binary using tftp to /mnt folder 5. Run Malware 6. Check CPU information	3.5

Figure 6 IoT Pot Patterns of Attack

```
…
def replace_bosybox(tn):
      tn.read_until(CMD_PROMPT, 1)
      tn.write('echo $(which busybox) > tmp_busybox; cp $(cat tmp_busybox)
$(cat tmp_busybox).' + DATETIME + '\n')
      tn.write('if [ ! -f "${mybusybox}.bin" ]; then cp $(cat tmp_busybox)
$(cat tmp_busybox).bin; fi\n')
      tn.write('echo \'#!/bin/sh\' > tmp_bb\n')
      tn.write('echo \'mybusybox=$(which busybox)\' >> tmp_bb \n')
      tn.write('echo \'BADFLAG=0  \'  >> tmp_bb \n')
      tn.write('echo \'string="$*" \'  >> tmp_bb \n')
      tn.write('echo \'words="telnet wget tftp" \'  >> tmp_bb \n')

      tn.write('echo \'for word in $words; do if [ "${string#*$word}" !=
"$string" ]; then return 0; else BADFLAG=1; fi; done \'  >> tmp_bb \n')
      tn.write('echo \'if [ $BADFLAG = 1 ]; then ${mybusybox}.bin "$@"; fi
\'  >> tmp_bb \n')
      tn.write('mv tmp_bb $(cat tmp_busybox); chmod +x $(cat
tmp_busybox)\n')
      print tn.read_until(CMD_PROMPT, 1)
```

Figure 7 Replace_busybox

```
...
def change_passwd_telnet(tn):
      p = random_gen()
      tn.write("passwd " + user + "\n")
      tn.read_until("(current) UNIX password: ")
      tn.write(password + "\n")
      tn.read_until("Enter new UNIX password: ")
      tn.write(p + "\n")
      tn.read_until("Retype new UNIX password: ")
      tn.write(p + "\n")
      targetDetails = "%s:%d:%s:%s:%s" % (target, port, proto, user, p,)
      log.info("Changed values: \t%s" % targetDetails)
...
def upload_run_script():
      ...
      with open(file_exec) as f:
         content = f.read()
      _execFile = file_exec.strip('.\\')
      # convert file contents to base64 and split into chunks to send
reliably over telnet
      content_serialized = split_by_length(base64.b64encode(content),
FILE_CHUNK)
      execFile = RUN_LOCATION + DATETIME + "_" + _execFile
      decodedFile = RUN_LOCATION + DATETIME + "_RUN_" + _execFile
      ...
      # write file in FILE_CHUNK sections
      for c in content_serialized:
         tn.write("echo \"" + c + "\" >> " + execFile + " \n")
         tn.read_until(CMD_PROMPT, 3)
      ...
      print tn.read_until(CMD_PROMPT, 3)
      # execute script on device
      tn.write("cd " + RUN_LOCATION + " && /usr/bin/nohup /bin/sh " +
decodedFile + " " + arg_str +
              " >/dev/null 2>&1 &\n")
  print tn.read_until(CMD_PROMPT, 3)
```

Figure 8 antimmirai.py

```
PS="/bin/busybox ps"
while true; do
	socket=$(grep /proc/net/tcp -e '[0-9]*: [A-Z0-9]*:[A-Z0-9]\{4\} [A-Z0-
9]\{8\}:0017' | tr -s ' ' | cut -d' ' -f 11)
	if [ ! -z "$socket" ]; then
	master_pid=$(find /proc/ -type l 2>/dev/null | grep /fd/ | xargs ls -la
2>/dev/null | grep $socket | head -1 | tr -s ' ' | cut -f 9  -d ' ' | cut -f 3 -d '/')
	name=$($PS aux | grep $master_pid | head -1 | tr -s ' ' | cut -d ' ' -f 4)
	$PS aux | grep $name | sed \$d | awk '{print $1}' | xargs kill -9 2>/dev/null
	fi
	sleep 2
done
```

Figure 9 secure.sh