Kennesaw State University Conference on Cybersecurity Education, Research & Practice

Kennesaw State University
Coles College of Business
Center for Information Security Education

Search

Enter search terms:

Search

in this collection

Advanced Search

Notify me via email or RSS

Faculty/Staff Authors

Author FAQ

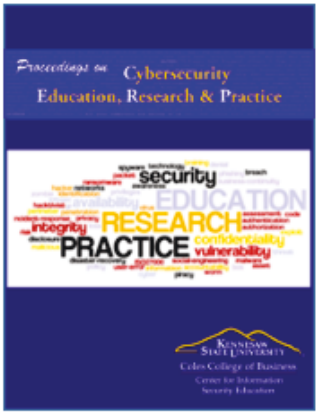
Submit to CCERP

Submission Style Guide

Links

CCERP 2016

ISSN: 2472-2898



2016 KSU CONFERENCE ON CYBERSECURITY EDUCATION, RESEARCH AND PRACTICE

This conference is sponsored in part by U.S. National Sciences Foundation Grant #1649587

The conference is organized into three tracks.

All student-authored papers should be submitted to the Student track, unless at least one author is not a student. If submitting for the NSF funded stipends (graduate workshop or undergraduate poster session, please email infosec [at] kennesaw [dot]edu and inform us as to which session you are applying for immediately after you submit your paper.

All curriculum development and instruction-focused papers should be submitted to the Pedagogy track.

All other papers, including cybersecurity research and industry best practice papers should be submitted to the Practice track.

Browse the contents of 2016 KSU Conference on Cybersecurity Education, Research and Practice:

Student Papers

Papers prepared primarily by students in the areas of information security, cybersecurity, or a related field.

Academic Papers - Practice

Papers should have practical relevance to faculty researching and teaching in information security and cybersecurity. All non-pedagogy papers should be submitted here, unless authored by students.

Academic Papers - Pedagogy

Papers should have practical relevance to the design, development, implementation, and best-practices in the teaching of information security/cybersecurity.

Show (#)

KSU Proceedings on Cybersecurity Education, Research and Practice (http://digitalcommons.kennesaw.edu/ccerp)

STUDENT PAPERS (HTTP://DIGITALCOMMONS.KENNESAW.EDU/CCERP/2016/STUDENT)

All papers primarily authored by students should be submitted here. Only papers authored exclusively by students will be considered for best student paper recognition. If you are applying for one of the 15 graduate workshop or one of the 15 undergraduate poster presentation slots (and associated stipend), please email infosec@kennesaw.edu immediately after submitting and inform us as to which session you are applying.

Student

Brain Betrayal: A Neuropsychological Categorization of Insider Attacks (http://digitalcommons.kennesaw.edu/ccerp/2016/Student/9)

Rachel L. Whitman, *University of Georgia*

Thanks to an abundance of highly publicized data breaches, Information Security (InfoSec) is taking a larger place in organizational priorities. Despite the increased attention, the threat posed to employers by their own employees remains a frightening prospect studied mostly in a technical light. This paper presents a categorization of insider deviant behavior and misbehavior based off of the neuropsychological foundations of three main types of insiders posing a threat to an organization: accidental attackers; neurologically “hot” malcontents, and neurologically “cold” opportunists.

Code Metrics For Predicting Risk Levels of Android Applications (http://digitalcommons.kennesaw.edu/ccerp/2016/Student/1)

Akond A. Rahman, *North Carolina State University*

Android applications pose security and privacy risks for end-users. Early prediction of risk levels that are associated with Android applications can help Android developers is releasing less risky applications to end-users. Researchers have showed how code metrics can be used as early predictors of failure prone software components. Whether or not code metrics can be used to predict risk levels of Android applications requires systematic exploration. The goal of this paper is to aid Android application developers in assessing the risk associated with developed Android applications by identifying code metrics that can be used as predictors to predict two levels of risk for Android applications. In this exploratory research study the author has investigated if code metrics can be used to predict two levels of risk for Android applications. The author has used a dataset of 4416 Android applications that also included the applications' 21 code metrics. By applying logistic regression, the author observes two of the 21 code metrics can predict risk levels significantly. These code metrics are functional complexity and number of directories. Empirical findings from this exploratory study suggest that with the use of proper prediction techniques, code metrics might be used as predictors for Android risk scores successfully.

Cover Text Steganography: N-gram and Entropy-based Approach (http://digitalcommons.kennesaw.edu/ccerp/2016/Student/16)

Sara M. Rico-Larmer, *Kennesaw State University*

Steganography is an ancient technique for hiding a secret message within ordinary looking messages or objects (*e.g.*, images), also known as cover messages. Among various techniques, hiding text data in plain text file is a challenging task due to lack of redundant information. This paper proposes two new approaches to embed a secret message in a cover text document. The two approaches are n-gram and entropy metric-based generation of stego text. We provide examples of encoding secret messages in a cover text document followed by an initial evaluation of how well stego texts look close to the plain texts. Furthermore, we also discuss several related work as well as our future work plan.

Hands-on labs demonstrating HTML5 security Concerns (http://digitalcommons.kennesaw.edu/ccerp/2016/Student/15)

Mounika Vanamala

The research is focused on the new features added in HTML5 standard that have strong implications towards the overall information security of a system that uses this implementation.A Hands-on Lab is developed to demonstrate how Web Storage and the Geo-location API of HTML5 can affect the privacy of the user.

Improvement and Maturity of the Information Security Risk Management Process (http://digitalcommons.kennesaw.edu/ccerp/2016/Student/13)

Angela Jackson-Summers, *Kennesaw State University*

Individuals' Concern about Information Privacy in AR Mobile Games (http://digitalcommons.kennesaw.edu/ccerp/2016/Student/11)

Dapeng Liu, *Virginia Commonwealth University*

Augmented Reality (AR) proves to be an attractive technology in mobile games. While AR techniques energize mobile games, the privacy issue is raised to be discussed. Employing social media analytics (SMA) techniques, this research makes efforts to examines Twitter postings of “PokemonGo” case and explores individuals’ attitudes toward privacy in AR games. In this research, we examine what are the privacy concerns of individuals in AR games and what are the individuals’ sentiments toward privacy. In the interesting case of PokemonGo, this paper suggests that individuals’ concerns about privacy are emphasized on six dimensions - collection, improper access, unauthorized secondary use, errors, post event reimbursement and proactive announcement. The findings could benefit AR game industry to identify privacy problem in discussion and to manage post privacy-event intervention.

Keywords: Information Privacy, Individuals’ Concern, AR Games, Social Media Analytics

Investigating Cyberbullying in Social Media: The case of Twitter
(http://digitalcommons.kennesaw.edu/ccerp/2016/Student/4)

Xin Tian, *Old Dominion University*

Social media has profoundly changed how we interact with one another and the world around us. Recent research indicates that more and more people are using social media sites such as Facebook and Twitter for a significant portion of their day for various reasons such as making new friends, socializing with old friends, receiving information, and entertaining themselves. However, social media has also caused some problems. One of the problems is called social media cyberbullying which has developed over time as new social media technologies have developed over time. Social media cyberbullying has received increasing attention in recent years as the media began shedding light on the devastating consequences that bullies can bring to their victims via social media. During the past few years, there has been a sharp rise in media reports regarding the use of social media to annoy, humiliate, intimidate, bully, and threaten others, with harmful consequences such as emotional distress, anxiety, depression and in some cases, suicidal tendencies. Therefore, it is imperative for researchers to investigate the phenomenon of social media cyberbullying.Thisstudy identifies public cyberbullying messages on Twitter and then specifically examines the diffusion of these cyberbullying messages through Twitters. Java programs were developed to gather Twitter cyberbullying messages using search API offered by Twitter and then these messages were analyzed in depth to understand how people retweet cyberbullying messages on Twitter.

Investigating Information Security Policy Characteristics: Do Quality, Enforcement and Compliance Reduce Organizational Fraud?
(http://digitalcommons.kennesaw.edu/ccerp/2016/Student/12)

Dennis T. Brown, *Kennesaw State University*

Occupational fraud, the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets, is a growing concern for all organizations. While the typical organization loses at least 5% of annual revenues to fraud, current methods of detection and prevention are not fully adequate to reduce increasing occurrences. Although information systems are making life easier, they are increasingly being used to perpetrate fraudulent activities, and internal employee security threat is responsible for more information compromise than external threats.

The purpose of this research is to examine how information security policy quality and enforcement impacts compliance and mediates organizational fraud levels in a sampling of small to medium-size firms. We will examine if (1) organizations with low (high) quality information security policy experience lower (higher) information security policy compliance; (2) organizations with strong (weak) enforcement of the existing policy experience lower (higher) levels of information security policy compliance; (3) if there is any significant interaction effect between information security policy quality and enforcement and (4) if perceived information security policy compliance is inversely related to reported organizational fraud.

Completion of this research will approach the fraud problem from a perspective that has not been studied previously and will inform current findings regarding the potential direct and indirect effects of information security noncompliance on organizational fraud by giving insights into the motivation leading to compliance versus noncompliance decisions encountered by employees in various organizational settings.

Investigating the Influence of Perceived Uncertainty on Protection Motivation: An Experimental Study (http://digitalcommons.kennesaw.edu/ccerp/2016/Student/7)

Ali Vedadi, *Mississippi State University*

IS users and organizations must take necessary measures to adequately cope with security threats. Considering the importance and prevalence of these issues and challenges, IS security research has extensively investigated a variety of factors that influence IS users' security intentions/behaviors. In this regard, protection-motivated behaviors are primarily based on individuals' personal cognitive evaluations and vigilance. In reality, however, many users reach security hygiene decisions through various non-rational and non-protection-motivated processes. Such users may not necessarily rely on their own cognitive appraisals and information processing, but proceed to make decisions without careful cognitive assessments of security threats and coping responses. One promising lens for assessing these behaviors that may not be informed by rational and personal assessments of threats and responses is Herd Theory, which describes the phenomenon in which individual decisions are often influenced by other users' decisions about their behaviors. Drawing on this theory, this study seeks to answer the following research questions by using an experimental design:. *In uncertain circumstances, are individuals more likely to cope with security threats by following the herd?*

IS Security Research Development: Implications For Future Researchers (http://digitalcommons.kennesaw.edu/ccerp/2016/Student/5)

Kane Smith, *Virginia Commonwealth University*
Chris Merritt, *Virginia Commonwealth University*

Security within the context of Information Systems has long been a concern for both academics and practitioners. For this reason an extensive body of research has been built around the need for protecting vital technical systems and the information contained within them. This stream of research, termed Information Systems Security (ISS), has evolved with technology over the last several decades in numerous different ways. This evolution can create a great deal of difficulty for researchers to identify under-represented areas of ISS research as well as ensure all relevant areas of concern are addressed. The purpose of this paper is threefold: First, our goal is to map the progression of ISS research from past to present. Second, conduct a review of ISS literature from the date of the last holistic literature review to present, identifying key security thematic presented in these works, grouping them categorically. Lastly, from this review we explain the thematic these works resolve to and based on these categories we discuss where ISS research currently stands.

The Role of State Privacy Regulations in Mitigating Internet Users' Privacy Concerns: A Multilevel Perspective (http://digitalcommons.kennesaw.edu/ccerp/2016/Student/14)

Tawfiq Alashoor, *Georgia State University*

In the U.S., there is no comprehensive national law regulating the collection and use of personal information. As a response to the high level of privacy concerns among U.S. citizens and the currently limited regulations, states have enacted their own privacy laws over and above the principles of Fair Information Practices (FIP). In this exploratory study, we draw upon the privacy literature and the Restricted Access/Limited Control (RALC) theory of privacy to study the privacy concerns phenomenon with a multilevel theoretical lens. We introduce and test three novel propositions pertaining to the impact of state level privacy regulations on privacy concerns. This combines consideration of individual differences as well as state level factors in predicting individuals' Internet privacy concerns. Overall, the results provide support for the role of state level privacy regulations in mitigating individuals' privacy concerns. We discuss the results, theoretical contributions, policy implications, and future research.

Towards A Comparison of Training Methodologies on Employee's Cybersecurity Countermeasures Awareness and Skills in Traditional vs. Socio-Technical Programs (http://digitalcommons.kennesaw.edu/ccerp/2016/Student/2)

Jodi Goode, *Nova Southeastern University*

Organizations, which have established an effective technical layer of security, continue to experience difficulties triggered by cyber threats. Ultimately, the cybersecurity posture of an organization depends on appropriate actions taken by employees whose naive cybersecurity practices have been found to represent 72% to 95% of cybersecurity threats and vulnerabilities. However, employees cannot be held responsible for cybersecurity practices if they are not provided the education and training to acquire skills which allow for identification of security threats along with the proper course of action. This work-in-progress study addresses the first phase of a larger project to empirically assess if there are any significant differences on employees' cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) based on the use of two security education, training, and awareness (SETA) program types (traditional vs. socio-technical) and three SETA delivery methods (face-to-face, hybrid, & online). In the first phase, a panel of subject matter experts (SMEs) will review SETA program topics and the measurement criteria for CCA and CyS per the Delphi methodology. The SMEs' responses will be incorporated into the development of two SETA program types with integrated vignette-based assessment to be delivered via three methods.

Towards a Development of a Mobile Application Security Invasiveness Index (http://digitalcommons.kennesaw.edu/ccerp/2016/Student/6)

Sam Espana, *Nova Southeastern University*

The economic impact of Mobile IP, the standard that allows IP sessions to be maintained even when switching between different cellular towers or networks, has been staggering in terms of both scale and acceleration (Doherty, 2016). As voice communications transition to all-digital, all-IP networks such as 4G, there will be an increase in risk due to vulnerabilities, malware, and hacks that exist for PC-based systems and applications (Harwood, 2011). According to Gostev (2006), in June, 2004, a well-known Spanish virus collector known as VirusBuster, emailed the first known mobile phone virus to Kaspersky Lab, Moscow. Targeting the Symbian OS, the worm spread via Bluetooth. Ten years later, Kaspersky Lab reported 884,774 new malicious mobile programs (Unuchek & Chebyshev, 2015).

On the one hand, during mobile application installations, users typically agree with the vendor's end-user license agreement (EULA) as a contract between the licensor and licensee. On the other hand, there is no easy way for users to monitor approved software functionality (i.e., automatic updates) as opposed to unapproved functionality (i.e., unwanted Bluetooth connectivity).

This paper presents, as the primary goal, the development of the Mobile Application Security Invasiveness (MASI) Index for assessing the level of invasiveness of covert application functionality. By assessing the MASI Index of an application, users should be able to score its invasiveness, classify it (i.e., non-invasive application or invasive application) and potentially uninstall it.

Towards a Model of Senior Citizens' Motivation to Pursue Cybersecurity Awareness Training: Lecture-Based vs. Video-Cases Training
(http://digitalcommons.kennesaw.edu/ccerp/2016/Student/3)

Carlene G. Blackwood-Brown, *Nova Southeastern University*

Cyber-attacks on Internet users, and in particular senior citizens, who have limited awareness of cybersecurity, have caused billions of dollars in losses annually. To mitigate the effects of cyber-attacks, several researchers have recommended that the cybersecurity awareness levels of Internet users be increased. Cybersecurity awareness training programs are most effective when they involve training that focus on making users more aware so that they can identify cyber-attacks as well as mitigate the effects of the cyber-attacks when they use the Internet. However, it is unclear about what motivates Internet users to pursue cybersecurity awareness training so that they can identify as well as mitigate the effects of the cyber-attacks when they use the Internet. This work-in-progress study will empirically investigate what motivates a specific group of Internet users, that is, senior citizens, to pursue additional cybersecurity awareness training, after initial training is conducted. Contributions from this study will add to the body of knowledge on how to motivate Internet users to pursue additional training in cybersecurity, and thus, aid in the reduction of the billions of dollars in losses accrued to Internet users as a result of cyber-attacks. Senior citizens will also benefit in that they will be better able to identify and mitigate the effects of cyber-attacks. The recommendations from this work-in-progress study will also be significant to law enforcement in reducing the number of cases relating to cybersecurity issues amongst senior citizens, and thus, free up resources to fight other sources of cyber crime.

Training Decrement in Security Awareness Training
(http://digitalcommons.kennesaw.edu/ccerp/2016/Student/8)

Tianjian Zhang

This study determines if there is a decremental effect following IT security awareness training. In most security policy compliance literature, the main focus has been on policy design. Studies that address security awareness training are seldom theory driven and even fewer are empirically based. To fill this gap, we draw from the theory of vigilance decrement as well as forgetting curves in psychology, and propose a classroom experiment showing that participants' IT security awareness decreases over a 45-day period since the training at day one. The result adds to the security policy compliance literature and suggests that some policy violations are due to the decrement in vigilance and security knowledge. The practical implications are that companies need to train their employees repeatedly overtime in order to maintain a high level of IT security policy compliance.

User Privacy Suffers at The Hands of Access Controls
(http://digitalcommons.kennesaw.edu/ccerp/2016/Student/10)

Chad N. Hoye, *University of West Florida*

With advancements in personal hand held devices, smaller more mobile computers, tablets, and the world's population connected with social media the threat to the user's privacy has been diminished. I will look at how access control policies have opened the proverbial door to user's privacy being attacked and threatened. You will see examples of how users have to divulge personal information to get better service and even be monitored while at work to prevent intrusions in to the company.

Brain Betrayal: A Neuropsychological Categorization of Insider Attacks

Rachel L. Whitman
University of Georgia, rlw35713@uga.edu

Abstract
Thanks to an abundance of highly publicized data breaches, Information Security (InfoSec) is taking a larger place in organizational priorities. Despite the increased attention, the threat posed to employers by their own employees remains a frightening prospect studied mostly in a technical light. This paper presents a categorization of insider deviant behavior and misbehavior based off of the neuropsychological foundations of three main types of insiders posing a threat to an organization: accidental attackers; neurologically "hot" malcontents, and neurologically "cold" opportunists.

Disciplines
Cognitive Psychology | Industrial and Organizational Psychology | Information Security | Management Information Systems

INTRODUCTION

Information Security (InfoSec) is no longer a minor concern of organizations. In today's social media-saturated environment, data breaches can easily become large, publicized affairs that deal immense, sometimes irreparable blows to an organization's reputation (Ponemon Institute LLC, 2011). With cyberattacks coming from all sides and news outlets on the prowl for the next sensational breach, InfoSec professionals have increasingly turned their attention to the potential risks posed by an organization's own employees. Insider threat is understandably a serious issue: the damage caused by employees or associates is rated as more severe, costly, and difficult to detect than that of outsiders (Software Engineering Institute [SEI], 2013). While the majority of cyberattacks still originate from non-insiders, employee attacks are still viewed with no small amount of trepidation (SEI, 2013). Most organizations report feeling vulnerable to internally-originated incidents and 93% are planning to increase or maintain their InfoSec budgets accordingly—though roughly seven to nine percent of the median annual $750k IT budget is already allocated to security (Vormetric Data Security, 2015; Filkins & Hardy, 2016). This expansion of cybersecurity spending indicates recognition of a vulnerability, but increased internal focus potentially comes at a cost to workplace trust, organizational cohesiveness, and, ultimately, productivity.

Research attempts to explore causes and possible preventative approaches to insider threat have been gaining traction. However, as Crossler et al. note, most of these efforts tend to be geared towards the technical side of the cybersecurity field—the focus of the research appeals to the firewall-wielding, computer-savvy CISO, seemingly at the expense of the more managerial-minded Information Security professionals. Crossler and his colleagues also point to a rather undefined classification approach to insider attacks that label threat behavior as either deviant or misbehavior, and call for a clearer separation and examination of the two categories (Crossler et al., 2012). Loch, Carr, and Warkentin's Four Dimensions of Information Systems Security provides a comprehensive classification scheme for categorizing threats by analyzing threat source, agent, motivating intent, and potential results, and refinement by Willison and Warkentin has expanded the category of intent to include a continuum of motives—from unintentional to fully malicious (Lock, Carr, & Warkentin, 1992; Willison & Warkentin, 2013).

While subsequent multidimensional approaches have sought to classify threats in orthogonal manners, thus extending the modularity and applicability of Loch et al.'s original classification scheme, these approaches—thanks to their intended all-encompassing applicability—are not specific to insider threat (Jouini, Rabai, & Aissa, 2014; Jouini, Rabai, & Khedri, 2015). Due to the extremely negative emotional and financial impacts associated with the collapse of the employee-employer trust dynamic, insider threat poses a significant enough risk to warrant its own classification scheme (Reina & Reina, 2015).

By adopting a neuropsychological approach to investigating insider threat behavior, we are able to better tease apart the categories of insider deviant and misbehavior as rooted in aggression and nonaggression, respectively. We also propose a subcategorization of insider deviant behavior based on the neurological arousal levels of the aggression type displayed, resulting in our final categories of accidental attackers, hot malcontents, and cold opportunists. A common approach to uniting psychology with other management-involved fields is to pose the motivation-concerned question of *why*: why do employees fall for email scams? Why do they attack organizations? Why don't they change their password on a regular basis? We have been seeking to understand why employees attack their organizations, but perhaps it is time to ask how.

With the application of a neurologically-rooted system of categorization, we not only gain unique insight on the problem of insider threats and attacks, but we are able to surpass previously motivation-limited approaches to understanding such behavior on a psychological level. Armed with this information, Information Security professionals will be able to better understand, prepare for, and circumvent such attacks.

DANGEROUS INSIDERS

Using a traditional motive-based perspective, risks posed by employees can initially be broken down into two major groups: insiders that bear an intent to harm their organization, and those that do so accidentally. As previously mentioned, Crossler et al. classify these categories of behavior as insider deviant behavior and misbehavior, respectively (Crossler et al., 2012). The latter half, bearing no ill intent other than a possible aversion to following good security habits, requires no further categorization and such misbehaviors will be grouped together for the purpose of this approach, as most unintentionally risky behaviors can be traced to distraction or a general lack of awareness. Insiders that intend to harm their employers, however, require deeper analysis, as deviant behavior essentially amounts to acts of aggression.

It likely comes as no surprise that the neurological activity behind a lapse in attention is leagues away from that of a purposeful, aggression-based attack, but it is important to note that not all acts of aggression are cut from the same cloth. Motivation and context play a large role in determining how the body will process aggression in everyday life, and the same is true of deviant employee behavior. While both vengeance-driven sabotage and the purposeful misuse of user privileges for financial gain both seem to be intentional, deviant acts of an aggressive nature, they are displays of two very physiologically different types of human behavior. It is the difference between spitefully hurling your boss' prized decorative vase across the room, and secretly selling it on your local Free and For Sale Facebook page (whereas in this scenario, an accidental attacker might simply send the piece toppling with a stray elbow).

With these differences accounted for, we wind up with three categories of insider attacks: accidental, non-attentive, non-aggressive insiders; neurologically "hot" malcontents aiming to cause harm; and neurologically "cold" opportunists seeking to cut themselves a piece of organizational pie.

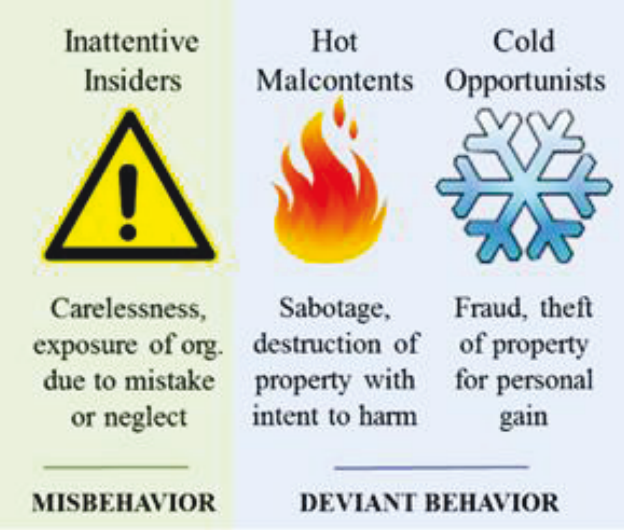


Figure 1: Proposed categories include "hot" anger and "cold" calculation in the deviant category, and inattention-based threat in the misbehavior section

Accidental Attackers

Just as the road to a familiar destination is paved with good intentions, so is the path to insider threat lined with non-malicious motives. Here defined by a lack of intent to harm an organization, unintentional insider threat can include accidental disclosure of classified information, careless treatment of physical data storage devices, and falling prey to often-obvious, sometimes-subtle phishing emails that even well-trained, cautious employees may respond to when bogged down with overwhelming amounts of correspondence (CERT Insider Threat Center [CERT], 2014). From a neurological perspective, unintentional insider threat behavior arises primarily from a lapse in attention—that is, a temporarily diverted level of consciousness. Any consequential breach of security is entirely unintended, and it is this complete lack of malice lends the title of accidental attacker to employees in this category.

Though the popularity of multitasking suggests otherwise, attention appears to be a limited resource, and employees can only spend so much before they begin to operate in the red. Though the connotations associated with words such as "careless" and "inattentive" contain negative implications, causes contributing to unintentional insider threat are varied and many, and the label of inattentive insider is not meant to be a judgment of an employee's responsibility or lack thereof. Whatever the circumstances surrounding an accidental attacker—excess amounts of stress imposed by a heavy workload, a lack of sleep, the presence of workplace distractions such as a noisy coworker—the end result is the same: a lack of attention and diminished or misdirected state of consciousness.

It may seem that the category of inattentive insiders contains mostly small workplace sins: phishing gullibility, a misplaced USB drive, or bad browsing habits. These seemingly small events stack up, though, as accidental data exposure is the most common cyber incident amongst insiders (SEI, 2013).

It is worth noting that intention once again plays an important role in distinguishing accidental threat. An intentional disregard for safe employee practices, though similar in results to a lack of attentiveness, falls under cold threat rather than inattentiveness. For example, insiders that violate guidelines for workplace behavior in order to illegally download music display a willful disregard for the expected employee behaviors. This intent to ignore codes of conduct places them under the third category—that of cold opportunists—as he or she is choosing to break the rules for the enjoyment that stands to be gained from such behavior. Inattentive insiders are categorized by their lack of attention, and willful ignorance fails to meet this qualification.

Hot Malcontents

Deriving its name from the active state of the sympathetic nervous system, "hot" insider attacks spawn from motives rooted in anger—and, by extension, aggression. One of the more overpowering human emotions, anger is able to muddy one's ability to reason, cause extreme short-sightedness, and turn an otherwise logical person into a raving lunatic (DeSteno & Piercarlo, 2011). Unlike negligence or inattentiveness, anger is characterized by intense arousal of the sympathetic nervous system—the same system that is responsible for the fear-induced fight or flight response (Carlson, 2013). While the fight or flight response is more commonly associated with fear, anger and fear share a number of biological characteristics—heart rate elevation, an increase in blood pressure, and a generally heightened state of awareness—and anger-driven insider aggression similarly runs on such responses (Ax, 1953).

Hot malcontents possess an additional neurological edge in that this category is essentially exclusively concerned with revenge-oriented insiders. While anger is certainly a dominating emotion in these instances, it has been shown that acts of vengeance activate not just the fight and flight response, but the brain's pleasure-tied reward pathways as well (de Dominique et al., 2004). The activation of these pathways make revenge more than a simple release of anger: it is a desirable, physiologically incentivized behavior. This neural intoxication makes hot malcontents a heated risk indeed.

The profile of the angry insider is well-cited archetype of the InfoSec community: an irate employee, upon discovering that they are to be demoted, fired, or otherwise cast from their spot on the organizational ladder, takes it upon themselves to alleviate their feelings of distress by relieving their former employer of valuable data or equipment. One way that hot malcontent threats differ from those of cold opportunists is that these attacks are most notably reactionary. Home Depot's Ricky Joe Mitchell, for example, caused former employer EnerVest nearly one million dollars in damages to office equipment and the company network after learning he was to be dismissed from the organization (Gallagher, 2014).

The defining characteristics of this category of insider attack are thus that they are aggressive in nature (qualifying them as deviant behavior), reactionary, and hold harming the organization as the primary goal of their behavior.

Cold Opportunists

In contrast to the heated, anger-driven nature of hot insider attacks, "cold" aggression shows much less arousal of the jittery, high-strung sympathetic nervous system. Fraud, exploitation, intellectual theft—these are all deviant behaviors that display aggression towards an organization, but they lack the neurological fire that behaviors of hot malcontents possess. Similar to acts of predation, insider attacks in this category instead fall under the jurisdiction of the calmer, more analysis-friendly parasympathetic nervous system.

This "rest and digest" division of the autonomic nervous system—which governs the unconscious activities that keep us alive and running—is responsible for some of the least aggressive activities known to humankind, such as sleep (Carlson, 2013). In certain situations, however, it can serve as a platform from which acts of aggression may be carried out. The most notable of these examples, predation, is generally defined as occurring when a member of one species engages in aggressive or violent behavior against a member of another species (Carlson, 2013). In the context of human behavior, we may presume to expand this definition to include not only activities such as hunting, but circumstances in which individuals seek to better their stations in life at the expense of others. In the absence of the adrenaline-soaked mindset that accompanies the fight or flight response, the focus is less on immediate survival (or vengeance, in the case of our hot malcontents) and more on personal advancement. Since the mind is not overwhelmed with emotion and is more capable of logical, long-term planning, attacks in this category can be highly complex, orchestrated events that pose massive risk towards an organization.

As the name suggests, cold opportunists are proactive rather than reactive: instead of negatively responding to an unfavorable HR decision, they act out of self-interest to take exploit their current situation, often financially. In the case of William G. Sullivan, Senior Database Administrator for Certegy Check Services, the potential gain in monetary advantages was enough to motivate Certegy Check Service's Senior Database Administrator to download and sell the personal records of eight and a half million customers—a breach of monumental scale (Kendall, 2007). Unlike hot malcontents, cold opportunists are not inherently against their employer; they are merely for themselves.

It is in this category that we may see the greatest variety of threat, as while financial incentives are the largest motivator of intentionally threatening insiders, espionage is steadily on the rise, and intellectual property theft is tied with accidental data exposure as the leading insider cyber incident (Verizon, 2016; SEI, 2013). Any ideological attacks conducted on an organization by an insider would similarly fall under the umbrella of cold opportunism, so long as they are proactive in nature. The defining qualifications of the cold opportunist branch of deviant insider behaviors are as follows: that the attack be an aggressive assault on an organization or its assets, that it be proactive in nature, and that it possess a self-serving intent on the part of the threat agent.

TRUST AND TRAITORS

When considering the multitude of ways in which employees pose serious risk to an organization, employees might ironically seem to be too risky for an organization to employ. The age-old and often-debated tug-of-war between the feasible and the ideal requires little discussion, but it is worth nothing the positive effects that trust in the workplace often beget. We spend much time focusing on the multitude of ways in which employees cannot be trusted, and for good reason. It is clear that our society is moving forward into an increasingly uncertain state. Between highly publicized security breaches like that of Target and Home Depot, and public information leaks that are only increasing in frequency, the concept of trust may come across as foolish notion.

However, trust does not exist in a workplace for the sole purpose of being broken: it serves to enhance performance and has a massive potential to help the organization. If an employer can foster and maintain an environment of trust in the workplace, not only will it reap the benefits of a harmonious, united workforce—it will have a leg up on the competition.

These benefits are both intuitive and well-documented. Increased levels of organizational trust lead to increased participation and engagement in employee work, and an environment in which workers are trusted to be able to competently fulfill their duties can lead to higher retention of talented individuals—whose expertise the organization stands to greatly benefit from (Reina & Reina, 2015). The Leader-Member Exchange Theory (LMX) from the Industrial/Organizational Psychological schools of thought revolves entirely around the formation of strong relationships between superiors and subordinates, and studies have found that high levels of trust in this dynamic are associated with positive work performance (Chen, Lam, & Zhong, 2012). Trust is a cornerstone of human interaction, one that cannot be struck from the workplace.

A Need for Control

As technology has grown smaller, portable, and even wearable, it has increased the spread of the workplace. Employees often have work laptops, USB drives with sensitive information, or their professional emails accessible even when not on the premises. While this expansion of the workplace indicates the diminishing separation of work and home—often at the expense of the domicile—it also poses a problem for information security professionals. Namely, that employees are both taking technology home and bringing their own personal devices to work.

The rise of supplying and utilizing personal technology in a productive environment is not limited to industry (Elementary schools even have programs such as BYLD that encourage students to "Bring Your Learning Device" and incorporate cell phones into curriculum), but it is causing some anxiety for IT decision makers. According to a 2015 survey by Vormetric, the vast majority of these professionals are concerned with their lack of control over mobile devices in the workplace. This worry, unfounded or not, is drawing attention when things like high-volume data storage remain pressingly vulnerable (Vormetric Data Security, 2015).

Though the increased attention pointed toward mobile devices indicates an elevated desire for control in an environment with innumerable variables, increasing security presence could have unintended negative effects. It is documented that while individuals who are not confident of their skill sets both benefit from and appreciate close monitoring, those who are skilled tend to resent such close attention—not only that, but their performance actually decreases in response (Aiello & Kolb, 1995). Though insiders pose some of the greatest threats to organizations, holding them under constant scrutiny would likely decrease both morale and performance, and in a worst-case-scenario could actually serve to drive away skilled employees.

The resulting conundrum is a classic one for InfoSec professionals. On one hand, the need for a balance for reasonable security measures. On the other, the need for effective workplace trust—especially since employee performance is correlated with their supervisor's perception of their ability (Dockery & Steiner, 1990). Both are necessary for maximum organizational efficiency, and it might seem that the answer lies in some variation of "too hot, too cold, just right." This is certainly a viable approach, and as every organization is a unique entity, it is up to the CISO to gauge what levels of security are appropriate for the situation. At the end of the day, cyber security is in the business of keeping the organization protected so that it may perform its business with confidence.

However, since we've gone to the trouble of classifying types of insider threat according to their physiology and categories of aggression, we can further extend our understanding into supplying general courses of action to prevent such occurrences. We've asked *how* instead of *why*, and answering this question is the first step in understanding *how not*.

IMPLICATIONS

Since our three categories of insider threat are essentially divided based on their types of aggression (or lack thereof), we will analyze the implications accordingly. Despite the differing complex forces of human behavior at play, the three categories of insider threat can be combated with a similar psychological approach. In all regards, it boils down to a matter of perception crafting.

The human brain is already in the business of synthesizing reality. It is capable of transducing and translating wavelengths of light into vivid, recognizable colors, it turns the compression and rarefaction of air into comprehensible language, and it regularly takes rhythmic utterances and extracts from them meaningful information. The brain has often been portrayed as nature's greatest supercomputer, but its remarkable processing power can be attributed in part to the fact that it takes shortcuts—as evidenced by the lengthy list of human biases to be found. Confirmation biases, stereotyping, hindsight bias—these often be the result of the brain attempting to "fill in the gaps" in an effort to save time and keep us alive. And because we only ever perceive what our brains feed us, we fall prey to these biases time and time again. Perception governs our world. Whether it is used knowingly, accidentally, or seldom at all, it is one of the greatest tools in the InfoSec toolbox.

Averting Accidents

"Accidents happen," certainly, but when working for a business that wants results twice as good in half the time, it hardly makes for an acceptable excuse when an employee falls for a phony email and winds up infecting half the network with a virus. Luckily, a lack of attention is easily and intuitively addressed through education, training, and no small amount of promotional merchandise. Training programs have been documented to reduce the risk of unintentional insider threat (UIT), and creating a culture of mindfulness within the workplace will help draw attention to good browsing habits (CERT, 2014). If a lack of attention or awareness is the main cause of unintentional insider threat, the immediate goal should be to draw attention to the problematic behaviors.

To further deter UIT, employees must perceive their careless activity as harmful to the organization, and, by extension, themselves. Reframing the organization's interests as being the individual worker's is a long-held, upstanding approach to encouraging desired behaviors. While fully harnessing a person's incredibly powerful intrinsic motivation ("I want this") remains out of reach, it is another matter entirely to attempt to convince someone that a behavior is in their best interest ("I should want this"). Doing so is hailed as one of the most effective ways to influence behavior (Carnegie, 1936), and InfoSec professionals can harness this approach in several ways. For example, promoting the idea that good employees practice good security incentivizes desirable habits in individuals who want to be exemplary workers. Framing desired organizational behaviors as beneficial to employees turns the activities from chores into self-rewarding habits.

While awareness posters and other promotional material reminding employees of acceptable organizational behaviors is certainly a step in the right direction, it loses its value if it is posted and then allowed to fallow. New additions to an environment tend to draw the eye, but once the mind has accepted an item (a poster, in this case) as part of the surrounding landscape, it is expected to be there, and thus is paid little attention, as the brain can and often does safely assume it will continue to occupy that space. Promotional material should therefore be cycled through on a regular basis, in order to keep the message of conscientiousness fresh in the minds of employees. With carefully-designed materials and a pointed effort to improve awareness, our accidental attackers stand a much better chance of recognizing and avoiding risky employee misbehavior.

Cooling Tempers

To prevent "hot malcontents" from figuratively (or perhaps literally) setting fire to an organization's assets, the goal is to expand the perception of belonging to the organization.

Since the aggression behind these types of insider attacks is fueled by the same mechanisms that react when an individual is faced with a threat to safety (the fight or flight-based sympathetic nervous system), the counteraction to best prevent such behavior would be to avoid triggering the system in the first place. Completely avoiding such arousal is beyond the scope of our ability, however, and as such we must again turn to crafting perception.

We tend to view antagonists as being either against us or for themselves, and it is in an organization's best interests to avoid the former. If an employee perceives that the organization is out to get them, he or she is probably much more likely to take news of their firing/demotion/layoff negatively than if the organization is simply struggling to survive. Framing any potentially upsetting firing decisions in the light of the organization trying to remain afloat may help in this regard. However, employers should hesitate before adopting an overly formal letter of discontinued employment, as this might be seen as a complete disregard for an employee's contributions to the company (Reina & Reina, 2015). Courtesy and appreciation are paramount in these tense situations. If there is no way to avoid conflict, though, it is advised that a close eye be kept on any vulnerable assets.

Luckily, patterns of aggression can often be traced throughout an individual's life, and an organization that conducts background checks on potential employees would do well to take any indications of such behavior into account. Rogue network administrator Terry Childs of San Francisco infamy, for example, spent time in prison for aggravated assault years before he seized control over the city's FiberWAN network (Venezia, 2008).

Deterring Opportunists

It must first be noted that there are some individuals who will resist deterrence by even the most proactive of organizational measures. However, several patters of risk behavior can be applied to insider threat scenarios, allowing for a better understanding of what factors might succeed in staving off cold opportunists. In the context of risks made for personal gain, perception is both a powerful player and a useful tool, especially considering the more complex and logically conceived behaviors in this category.

Psychologists David DeSteno and Piercarlo Valdesolo describe the manner in which violence against others is justified: through a dehumanization of the opposing force and a breaking down of the ways in which an individual can relate to their newfound enemy (DeSteno & Valdesolo, 2011). The enemy becomes "other," making them unlike ourselves and thus leaving no place for empathy, which is reserved for those whom we can relate to. This disconnect enables individuals to commit behaviors that would otherwise require a state of extreme emotional arousal to engage in. An individual can literally think themselves out of committing a morally reprehensible act—and do so quite often. This is a pattern that sees repetition throughout much of history, from colonial slavery to the Holocaust, and it is a longstanding testament to the power of perception.

Part of this is because of how perception mediates the relationship between risk behavior and outside environmental influences. Individuals who perceive their circumstances as undesirable repeatedly tend to underestimate the risks of their decisions (Sitkin & Pablo, 1992). To rephrase in the context of cyber security, an unhappy employee who has more to gain by abusing their access for fraudulent purposes is more likely to view the risks of engaging in such behavior as less than they actually are, thus increasing the chances of an insider incident. One approach to combating this would again be to pay careful attention to fostering a strong, united workplace. The majority of activities that break workplace trust are small incidents that accumulate over time, so an effort to ensure that emails are responded to promptly, appropriate employees are consulted for their opinions, and staplers are not stolen can help dissipate some of the damage done to trust in the workplace (Reina & Reina, 2015).

Visibly flaunting the organization's InfoSec department could also potentially help deter cold opportunists by promoting the perception of the organization's systems as well-guarded. Since attacks in this category are made without the hotheaded sympathetic arousal of Hot Malcontents, reason plays a much larger role in the decision to attempt to turn against one's employer. If the organization frequently advertises the fact that their assets are carefully maintained, the risks of being caught may very well outweigh the potential advantages to be gained from fraud or thievery. Subtly flaunting the strength of an organization's security can have other benefits, too—a CISO can cultivate an image through normal, awareness-promoting activities within the business. Practicing good security therefore doesn't only increase within-organizational awareness, it can deter insiders and help create a better working environment as well.

CONCLUSIONS

While neuropsychology and other brain-related subjects may still seem like a distant, laboratory-limited field of study, it is currently rapidly expanding. This era has been dubbed "The Century of the Brain" by many a scientist, and understanding how neurophysiological pathways influence and play into the behaviors we encounter every day can give twenty-first century businesses an edge. Though the field of applied neuropsychology could stand more attention, the secrets of human behavior are nevertheless being slowly unraveled, and it is up to the InfoSec professionals of the future to weave these new understandings into our organizations.

As it applies to insider threat, neuropsychology can help further define and classify employee misbehavior and insider deviant behavior into physiologically-rooted categories. While accidental attackers unintentionally expose their organization through any number of careless misbehaviors, deviant behaviors house the more malevolent, aggression-related attacks. Neurologically hot malcontents react to negative events with the intent to destroy organizational property, while the category of cold opportunists allows for a separation of aggressive events in which the employee holds his or her personal interests as the highest priority rather than the destruction of the organization.

Armed with a better understanding of how employees are psychologically able to pose a threat to their employer, CISOs may take another step on the long road toward a broader utilization of modern understandings of human behavior. Psychology and management are tightly intertwined. This will only become truer as our knowledge of both fields expands.

ACKNOWLEDGMENTS

Many thanks to Dr. Whitman for his helpfulness, and to the KSU Conference on Cybersecurity Education, Research and Practice for the opportunity to submit undergraduate research.

REFERENCES

Aiello, J. R., & Kolb, K. J. (1995). Electronic performance monitoring & social context: Impact on productivity & stress. *Journal of Applied Psychology, 80*(3), 339-353.

Ax, A. F. (1953). The physiological differentiation between fear and anger in humans. *Psychosomatic Medicine, 15*(5), 433-442.

Carlson, N. R. (2013). Emotion. In *Physiology of Behavior* (347-400). Edinburgh Gate, Harlow: Pearson.

Carnegie, D. (1936). *How to win friends and influence people*. D. Carnegie and A. R. Pell. New York, NY: Pocket Books.

CERT Insider Threat Center (2014). Unintentional insider threats: Social engineering. Technical Report. CERT Division.

Chen, Z., Lam, W., & Zhong, J. (2012). Effects of perceptions on LMX and work performance: Effects of supervisors' perception of subordinates' emotional intelligence and subordinates' perception of trust in the supervisor on LMX and, consequently, performance. *Asia Pacific Journal of Management, 29*(3), 597-616.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2012). Future directions for behavioral information security research. *Elsevier Computers & Security, 32*, 90-101.

de Dominique J. F. Q., Fischbacher, U., Treyer, V., Schellhammer, M., Schnyder, U., Buck, A., & Fehr, E. (2004). The neural basis of altruistic punishment. *Science, 305*(5688), 1254-1258.

DeSteno, D., & Piercarlo V. (2011). *Out of character*. New York, NY: Crown Publishers.

Dockery, T. M., & Steiner, D. D. (1990). The role of the initial interaction in leader-member exchange. *Group and Organization Studies, 15*, 395–413.

Filkins, B., & Hardy, G. M., (2016). *IT security spending trends.* Technical Report: SANS Institute.

Gallagher, S. (2014, September). Home Depot's former security architect had history of techno-sabotage. *Ars Technica*.

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classificatiopn of security threats in information systems. *Procedia Computer Science, 32*, 489-496.

Jouini, M., Rabai, L. B. A., & Khedri, R. (2015). A multidimensional approach towards a quantitative assessment of security threats. *Procedia Computer Science, 52*, 507-514.

Kendall, S. (2007, November). Admin to plead guilty in theft of 8.5M records from database. *CSO Online*.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly, 16*(2), 173-186.

Ponemon Institute LLC (2011). *Reputation impact of a data breach*. Executive Summary: Experian Data Breach Resolution.

Reina, D., & Reina, M. (2015). *Trust and betrayal in the workplace* (3rd ed.). Oakland, CA: Berrett-Koehler Publishers, Inc.

Sitkin, S. B., & Pablo, A. L. (1992). Reconceptualizing the determinants of risk behaviour. *Academy of Management Review, 17*(1), 9-38.

Software Engineering Institute (2013). *US state of cybercrime survey: How bad is the insider threat?* PowerPoint slides: Carnegie Mellon University.

Venezia, P. (2008, July). Why San Francisco's network admin went rogue. *InfoWorld*.

Verizon (2016). *Data breach investigations report*. Technical Report.

Vormetric Data Security (2015). *Vormetric insider threat report: Trends and future directions in data security global edition.* Technical Report.

Willison, R. & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1-20.

Code Metrics For Predicting Risk Levels of Android Applications

Akond A. Rahman
North Carolina State University, aarahman@ncsu.edu

Abstract
Android applications pose security and privacy risks for end-users. Early prediction of risk levels that are associated with Android applications can help Android developers is releasing less risky applications to end-users. Researchers have showed how code metrics can be used as early predictors of failure prone software components. Whether or not code metrics can be used to predict risk levels of Android applications requires systematic exploration. The goal of this paper is to aid Android application developers in assessing the risk associated with developed Android applications by identifying code metrics that can be used as predictors to predict two levels of risk for Android applications. In this exploratory research study the author has investigated if code metrics can be used to predict two levels of risk for Android applications. The author has used a dataset of 4416 Android applications that also included the applications' 21 code metrics. By applying logistic regression, the author observes two of the 21 code metrics can predict risk levels significantly. These code metrics are functional complexity and number of directories. Empirical findings from this exploratory study suggest that with the use of proper prediction techniques, code metrics might be used as predictors for Android risk scores successfully.

Disciplines
Information Security | Software Engineering | Technology and Innovation

SUMMARY

Android applications can pose security and privacy risks for end-users. Early prediction of risk levels that are associated with Android applications can help Android developers is releasing less risky applications to end-users. Researchers have showed how code metrics can be used as early predictors of failure prone software components. Whether or not code metrics can be used to predict risk levels of Android applications requires systematic exploration. The goal of this paper is to aid Android application developers in assessing the risk associated with developed Android applications by identifying code metrics that can be used as predictors to predict two levels of risk for Android applications. This research paper focuses on answering the following research question to achieve this goal: RQ: What code metrics can be used as significant predictors to predict different levels of risk for Android applications?

In this paper the author has evaluated how code metrics such as number of lines, and McCabe's complexity can be used as predictors to predict multiple level of risk for Android applications. In this exploratory research study the author has investigated if code metrics can be used to predict two levels of risk for Android applications. The author has used a dataset of 4416 Android applications that also included the applications' 21 code metrics. By applying logistic regression, the author observes two of the 21 code metrics can predict risk levels significantly. These code metrics are functional complexity and number of directories.

In this exploratory research study the author has observed when all code metrics are combined in a logistic regression model, two specific code metrics are significant predictors. The author acknowledges that one type of regression model is not sufficient to predict multiple levels of risk for Android applications. The author observes the opportunity for future research in this direction, e.g. using other techniques such as principal component analysis to determine the significant predictors. Furthermore, the author observes the scope of applying a wide range of statistical learners to correctly predict the levels of risk. Sampling techniques such as over and under sampling can also be used to evaluate the performance of such prediction models.

Empirical findings from this exploratory study suggest that with the use of proper prediction techniques, code metrics might be used as predictors for Android risk scores successfully. The author observes the opportunity of applying statistical learning techniques on the used dataset as well as other data sources.

Cover Text Steganography: N-gram and Entropy-based Approach

Sara M. Rico-Larmer
Kennesaw State University, slarmer@students.kennesaw.edu

Abstract
Steganography is an ancient technique for hiding a secret message within ordinary looking messages or objects (*e.g.*, images), also known as cover messages. Among various techniques, hiding text data in plain text file is a challenging task due to lack of redundant information. This paper proposes two new approaches to embed a secret message in a cover text document. The two approaches are n-gram and entropy metric-based generation of stego text. We provide examples of encoding secret messages in a cover text document followed by an initial evaluation of how well stego texts look close to the plain texts. Furthermore, we also discuss several related work as well as our future work plan.

Disciplines
Information Security | Management Information Systems | Technology and Innovation

INTRODUCTION

Steganography is a popular approach to hide a given secret message within an ordinary document (known as cover media). The embedded message within a cover document is known as stego document. A systematic approach is applied at the sender side to generate the stego document, while the secret message gets extracted at the receiver side. The entire approach is known as stego system.

Steganographic techniques are divided into several categories based on the employed approach [6]. For example, a substitution system would add a secret message in redundant text present in a file, whereas a statistical method would capture the statistical properties from a text file in order to encode information. The cover document can be of three types: text, image and video.

This work focuses on embedding a secret message into a text document. Generally, it is a challenging task as text documents have little or no redundant information to hide a secret message compared to images or videos. In this project, we focus on embedding a secret message in a cover document of type text. We denote it as cover text steganography.

Current text-based steganography approaches (e.g., Garg (2011), Kim (2003), Nagarhill 2014, Low et al. (1995)) assume that a cover document is huge and the secret message is smaller in size. In practice, the cover document may be much smaller. A popular steganography technique on text cover document is to change the format by adding a space or invisible characters. The generated stego text reads as misspelled words in text, variation of fonts. This would fool an ordinary reader thinking misspellings or extra spaces. Format based approach may apply various fonts sizes, gaps among lines, or paragraphs.

In this paper, we propose two simple approaches to generate stego text: N-gram and Entropy. We provide examples of the ideas.

The paper is divided as follows. Section 2 provides an overview of some related work. Section 3 introduces N-gram and Entropy-based approaches with example of stego-text generation. Section 4 concludes and provides a future work plan.

RELATED WORK

Garg (2011) proposed to embed a secret message in HTML document. The idea is that HTML tag attributes often come with pairs (e.g.,) and the order of the pairs does not impact on the HTML document rendering process at the browser. Thus, they generate a set of tag attribute pairs and

alter their sequences to represent binary zero or one (e.g., align preceding width imply 1, where align present after width means zero). The approach works fine as long as HTML document is large enough to fit a secret message. If the secret message has a large length and HTML document does not have enough pairs of tag and attribute from the built in table, then the approach may not work well.

Kim, Moon, and Oh (2003) grouped adjacent words and generated statistics of white space. The embedding of the secret message involves modifying the statistics among adjacent words in a group. Nagarhill [3] proposed to embed a secret message through emotics by mapping alphabets and numbers with emotics available by SMS messaging application in mobile phone.

Low et al. (1995) proposes word shifting method where words are shifted horizontally and by changing the distance between the words the information is hidden. This leads to the strategy that marks a text line both vertically using line shifting and horizontally using word shifting.

Interested readers can see an extensive survey of Bennett et al. (2004) covering most known cover text-based stego text generation approaches.

PROPOSED APPROACH

N-GRAM ANALYSIS-BASED STEGANOGRAPHY

N-gram approach is used to generate possible close enough words for a given word. If the length of a given word is N, the approach systematically generates strings (subwords) from 1 to N-1 characters (Suen 1979). There are automatic tools available (e.g., Frequency Analysis (2016)) to generate N-gram for a given word. N-gram techniques are widely used for speech recognition, spelling correction, information extraction, etc. (N-gram (2016)).

In our proposed approach, we rely on n-gram analysis of wording to insert an embedded message. For a given word of length N (N>2), we generate words of length N-1. Then, we choose the first subword and place a space between the subword and remaining character in ordinary text to encode binary zero. For example, the word “TEST” has length 4, and it will have the following two subwords generated by a tool from (Frequency Analysis (2016)) as shown in Figure 1.

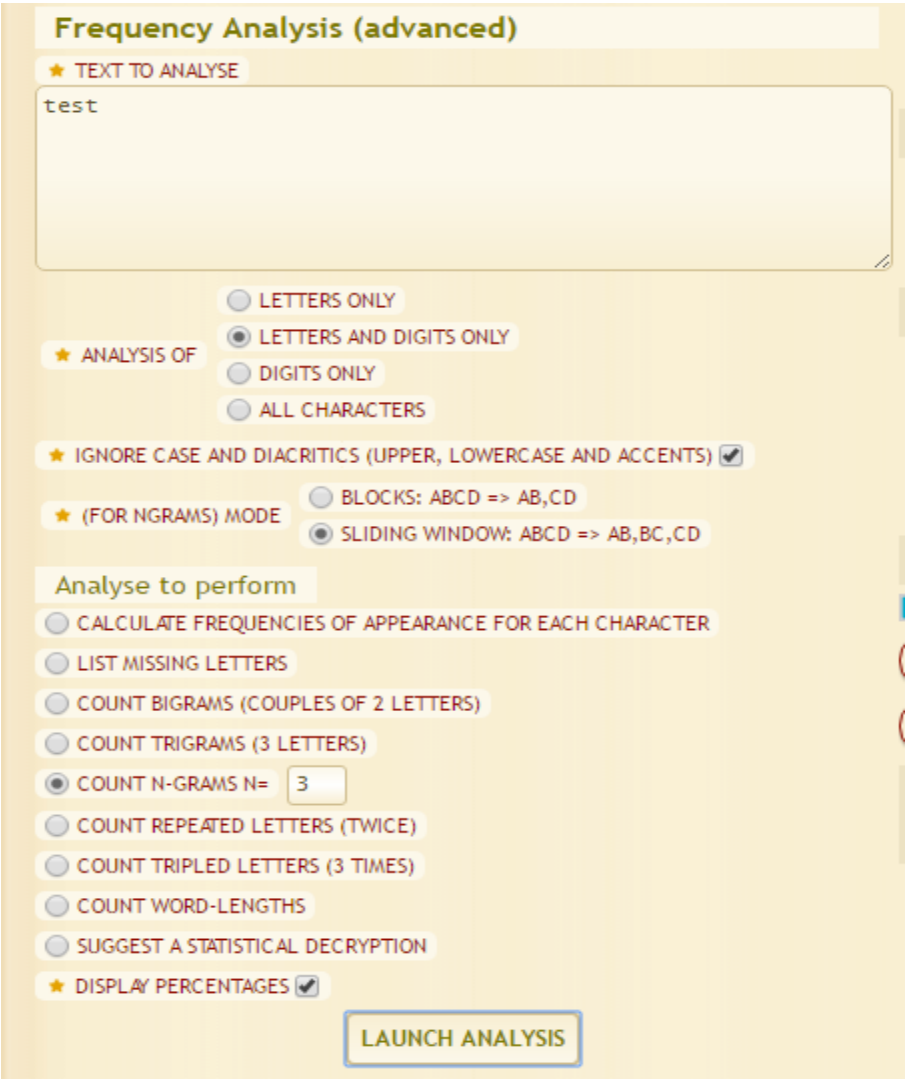


Figure 1: Example of Trigram for the cover text "TEST"

Table 1: Example of secret message encoding in cover text TEST

Secret message	Stego text
0	T EST
1	TES T

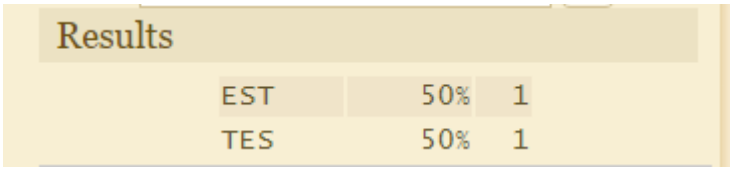


Figure 2: Result of Trigram for the cover text "TEST"

To encode the secret message 0, the stego text will be "T EST", where we added a space between "EST" and the beginning character "T" (first row of Table 1). We choose the last element of the generated subword (TES from Figure 1) of length N-1 to encode binary 1. Thus, a sender can encode a secret message up to the length of the number of words (as long as a character is at least 3 characters). The receiver needs to know the N-gram generator tool link to recover the secret text.

ENTROPY BASED STEGANOGRAPHY

Entropy (H) is a popular metric from information theory proposed by Shannon [9]. It calculates the amount of randomness present in a message. The formula shown in Equation (i) is commonly used to compute entropy.

Let us assume that Q is a set of symbols (unique characters) found in a given word present in cover text. Here, q_i is the occurrence of i^{th} character of a given word found in cover text. Let us consider that $p(q_i)$ is the occurrence of probability of q_i^{th} element. Then, the entropy of Q is

$$H(Q) = -\Sigma qi * \log_2 P(qi) \ldots \ldots (i)$$

To encode a secret message using entropy-based technique, we find two successive pair of words and compare their entropy level. To encode zero, we place the word having lower entropy at the front whereas, to encode one, we place the word having higher entropy at the front. If the entropy of two successive words are same, we skip the pair of words and move to the next.

Let us assume the cover text is "Comparing inverted files and signature files for searching a large lexicon" and secret message to be encoded is "11010". Table 2 shows each of the words (top row) of the cover text and the corresponding entropy level (bottom row). There are available open source tools to compute entropy (see for example, Shannon Entropy Calculator (2016)).

Table 2: Words and entropy level

Comparing	inverted	files	and	signature	files	for	searching	a	large	lexicon
3.17	2.75	2.32	1.58	3.12	2.32	1.58	3.17	0	2.32	2.81

Table 3: Stego text generation example

Comparing	inverted	files	and	files	signature	searching	for	a	large	lexicon
1		1		0		1		0		

Table 3 shows encoding of the secret message "11010" based comparison of entropy level for two successive word pairs in cover text. For example, the

entropy level of "Comparing" and "inverted" is 3.17 and 2.75, respectively. So, to encode "1", we keep the order as is (the word having higher entropy is already at the front). The last word ("lexicon") is an orphan and in this case to be ignored by the receiver. The sender would require mentioning the size of the secret message to the receiver.

EVALUATION

We calculate Levenshtein Distance (LD) between plain text and stego text. The LD algorithm computes the least number of operations (substitution, insertion, and deletion) performed at character level to modify plain text to stego text [12]. We apply an online tool to measure the LD between plain cover text and stego text [11].

Table 4: Secret message and plain text

Test#	Secret	Plain text										
1	1101011100	Comparing	inverted	files	and	signature	files	for	searching	a	large	lexic
2	1101011100	Normally	the	system	probes	the	monitors	and	fills	in	the	valu
3	1101011100	Email	enables	you	to	communicate	with	users	on	the	local	syste
4	1101011100	The	keys	back	up	and	correct	the	shell	command	line	
5	1101011100	The	nature	of	value	differs	for	different	types	of	organizations	
6	1101011100	Usually	formal	approval	will	solidify	the	sponsors	of	the	project	
7	1101011100	The	focus	will	be	on	the	managerial	and	business	decisions	
8	1101011100	Typical	projects	have	six	to	ten	designers	submitting	several	designs	
9	1101011100	Literally	thousands	of	programmers	have	worked	on	Apache	over	the	years
10	1101011100	Some	critics	believe	poor	design	is	more	common	than	good	desig

Table 5: Stego text based on entropy and Levenshtein Distance (LD)

Test#	Stego text											LD
1	Comparing	inverted	files	and	signature	files	searching	for	a	large	lexicon	9
2	Normally	the	probes	system	the	monitors	fills	and	in	the	values	20
3	Enables	email	you	to	with	communicate	users	on	the	local	system	21
4	Keys	the	back	up	and	correct	shell	the	command	line	command	23
5	Nature	the	value	of	for	differs	different	types	of	organizations		21
6	Formal	usually	approval	will	the	solidify	sponsors	of	the	project		23
7	Focus	the	will	be	on	the	managerial	and	business	decisions		12
8	Projects	typical	have	six	to	ten	submitting	designers	design	several		39

9	Thousands	literally	programmers	of	have	worked	Apache	on	the	over	years	36
10	Critics	some	believe	poor	is	design	more	common	good	than	design	27

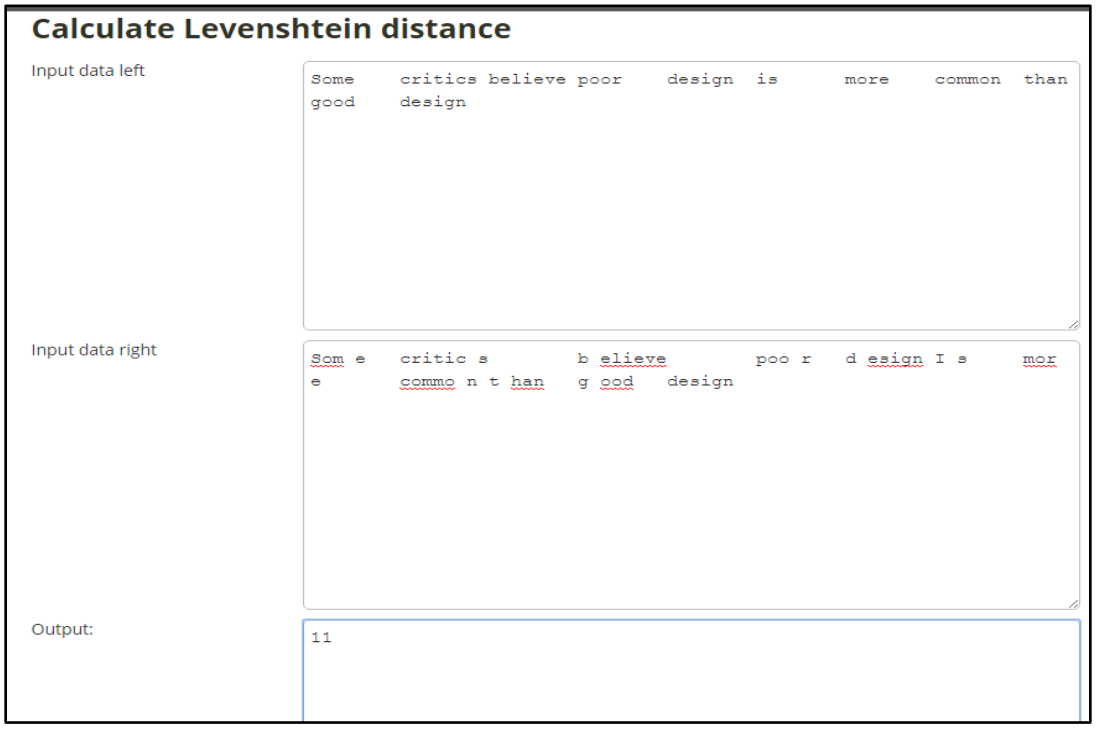


Figure 3: Screenshot of computing LD for N-gram based steganography

The higher the distance, the more dissimilar the two given strings are. Table 4 shows 10 original texts. We encode the secret message "1101011100" (column 2). Table 5 shows the generated stego text based on entropy. The last column of Table 5 shows LD for entropy-based stego text. Table 6 shows the generated stego text using N-gram technique. The last column of Table 6 shows LD.

Table 6: Stego text based on N-gram and Levenshtein Distance (LD)

Test#	Stego text											LD
1	Comparin g	inverte d	f iles	an d	s ignature	file s	fo r	searchin g	a	l arge	lexicon	18
2	Normall y	th e	s ystem	probe s	t he	monitor s	an d	fill s	I n	t he	values	12
3	Emai l	enable s	y ou	t o	c ommunicate	wit h	user s	o n	t he	l ocal	system	10
4	Th e	key s	b ack	u p	a nd	correc t	th e	shel l	c ommand	l ine		10
5	Th e	natur e	o f	valu e	d iffers	fo r	differen t	type s	o f	o rganizations		11

6	Usuall y	forma l	a pproval	wil l	s olidify	th e	sponsor s	o f	t he	p roject		10
7	Th e	focu s	w ill	b e	o n	th e	manageria l	an d	b usiness	d ecisions		10
8	Typica l	project s	h ave	si x	t o	te n	designer s	submittin g	severa l	design s		10
9	Literall y	thousand s	o f	programmer s	h ave	worke d	o n	Apach e	o ver	t he	years	10
10	Som e	critic s	b elieve	poo r	d esign	I s	mor e	commo n	t han	g ood	design	11

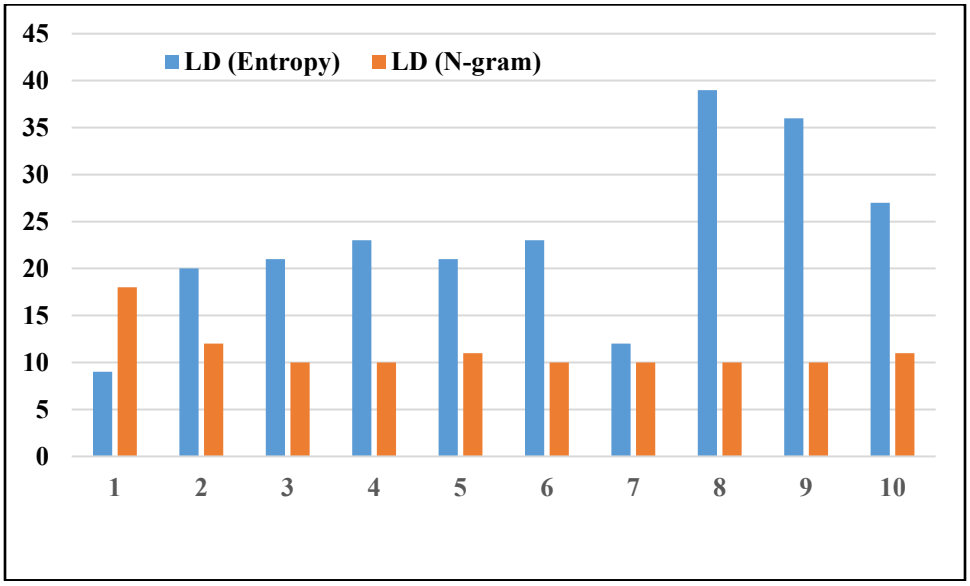


Figure 4: Leveshtein Distance between plain text and Stego Text

Figure 4 shows the comparison of LD between Entropy and N-gram based technique. We find the LD is lower for N-gram compared to Entropy-based technique. N-gram would be the preferred technique to generate stego text for small volume of texts. Table 7 shows the average and standard deviation for Entropy and N-gram based technique.

Table 7: Average and standard deviation of LD for Entropy and N-gram

	Entropy	**N-gram**
Avg.	23.1	11.2
Stdev.	9.279009	2.485514

CONCLUSION

Steganography comprises a set of art to hide a secret message in an ordinary looking document. Though most works focused on hiding information in image or video files, text file poses the challenge of discovering redundant information to hide secret text. To overcome the limitation of some of the existing text-based steganography techniques, we propose to apply N-gram and entropy metric-based generation of stego text to hide a secret message. We show examples of hiding secret messages and performed an initial evaluation to compare between entropy and N-gram based technique. The early results indicate N-gram is better than entropy-based technique. In the future, we plan to compare with larger text files. We also plan to measure the effectiveness steganography-based approaches using other distances such as Jaro-Winker.

REFERENCE

[1] M. Garg. (2011). A Novel Text Steganography Technique Based on Html Documents, *International Journal of Advanced Science and Technology*, Vol. 35, October, 2011, pp. 129-138. http://www.sersc.org/journals/IJAST/vol35/11.pdf

[2] Y. Kim, K. Moon, and I. Oh. (2003). A Text Watermarking Algorithm based on Word Classification and Inter word Space Statistics. *Proc. of the 7th International Conference on Document Analysis and Recognition (ICDAR)*, 2003, pp. 775-779.

[3] T. Nagarhill. (2014). A New Approach to SMS Text Steganography using Emoticons, *International Journal of Computer Applications*, pp. 1-3. Accessed from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.662.4948&rep=rep1&type=pdf

[4] S. Low, N. Maxemchuk, J. Brassil, L. O'Gorman. 1995. Document Marking and Identification Using Both Line and Word Shifting, *Proc. of 14th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, Vol.2, pp. 853-860. Accessed from http://netlab.caltech.edu/publications/InfocomID95.pdf

[5] Frequency Analysis Tool, 2016 Accessed from http://www.dcode.fr/frequency-analysis

[6] Krista Bennett. (2004). Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text, CERIAS Tech Report 2004-13, Purdue University, USA.

[7] N-gram, All our N-gram belong to you. (2006). Accessed from https://research.googleblog.com/2006/08/all-our-n-gram-are-belong-to-you.html

[8] C. Suen. (1979). n-Gram Statistics for Natural Language Understanding and Text Processing, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol 1, Issue 2, Feb 1979, pp. 164-172. http://dl.acm.org/citation.cfm?id=2053409

[9] T. Cover. (2006). *Elements of information theory*, 2nd Edition. Wiley-Interscience.

[10] Shannon Entropy Calculator. (2016) Accessed from http://www.shannonentropy.netmark.pl/

[11] Levenshtein Distance Calculator, Accessed from http://www.unit-conversion.info/texttools/levenshtein-distance/

[12] The Levenshtein Algorithm, Accessed from http://www.levenshtein.net/

Hands-on labs demonstrating HTML5 security Concerns

Mounika Vanamala
vanamala.mounika7@gmail.com

Abstract
The research is focused on the new features added in HTML5 standard that have strong implications towards the overall information security of a system that uses this implementation.A Hands-on Lab is developed to demonstrate how Web Storage and the Geo-location API of HTML5 can affect the privacy of the user.

Disciplines
Information Security | Management Information Systems | Technology and Innovation

SUMMARY

The research is focused on the new features added in HTML5 standard that have strong implications towards the overall information security of a system that uses this implementation. The built-in security support offered by features like Cross Origin Resource sharing, Web Storage (either Local Storage or session Storage), Geolocation, Web Sockets advantage over the capabilities offered by HTML4.

HTML5 provides new features to web applications but also introduces new security issues. Consequently, through adding those new features the evolution of the current web standards to HTML5 introduces also new security vulnerabilities and threats. New HTML5 features open innovative ways to attackers for launching their attacks. These new vulnerabilities, threats and attack possibilities are addressed in this paper. Every part of the specification has an own subsection dealing with security. This paper covers the points that need to be well thought-out when implementing the corresponding parts. The vulnerability which can result from this feature and how to securely implement it by the browser manufacturers is described.

A Hands-on Lab is developed to demonstrate how Web Storage and the Geolocation API of HTML5 can affect the privacy of the user. The main security concern with Local Storage is that the user is not aware of the kind of data that is stored in Local Storage. The user is not able to control storage respectively access to data stored in Local Storage. The new threats introduced by local storage like Disclosure of Confidential Data and User tracking are discusses in this paper.

The HTML5 Geolocation API provides the possibility of identifying the user's physical location based on GPS position. Prior to HTML5 it was only possible to determine the position of the user through plugins such as Java Applets. With the Geolocation API mainly privacy issues are associated. Every website is able to determine the position of the user which can be used by web application providers for user identification and tracking. This breaks the security requirement of Identity protection.

Improvement and Maturity of the Information Security Risk Management Process

Angela Jackson-Summers
Kennesaw State University, jacksan30144@yahoo.com

SUMMARY

With alarming rates of increasing information security threats and growing information security concerns among IT executives, this proposed study is designed to address the maturity and effectiveness of information security risk management (SRM). SRM is an organizational, continuous process that involves integration among other organizational processes. SRM also includes controls serving as countermeasures, policies, safeguards, and procedures that work to address security risks. As facets of SRM, maturity refers to the completeness and capability of continuous improvement, and effectiveness regards the level of usefulness of process methods. To help strengthen existing SRM organizational processes, this study aims to address the following questions: How can organizations strive to mature SRM? How can organizations improve SRM effectiveness?

Given the intrusive nature of SRM, the research methods to be used in past SRM studies have been designed with caution. An interview-based approach using the resource-based view theory and a capability maturity model will be used in this study. Interviews of three (3) to five (5) Chief Information Security Officers (CISO), or persons in senior management like roles, will be conducted. While a small number of study informants have been met with criticism in the past research, research rigor can be applied to a small sample rendering rich results. Using the laddering and critical incident techniques, planned interview questions derived from Spears and Barki (2013) and the ISACA RiskIT Process Model Framework (ISACA, 2009) will be used.

The interview data will be collected, analyzed, and interpreted to address SRM effectiveness. Also, the interview data will be used to address SRM maturity. In addressing SRM maturity, the Software Engineering Institute's (SEI) Capability Maturity Model Integration for Services (CMMI-SVC) framework is adopted, because of its use for integrated process improvement assessments. CMMI-SVC is comprised of twenty-four process areas of which the Risk Management (RSKM) model encompasses three maturity levels to organizational improvement. The three maturity levels are defined as 1 (Initial), 2 (Managed), and 3 (Defined). Textual analysis of the interview data will be performed and applied to the RSKM model. The study's findings will be verified and prepared for reporting.

The study's results will be captured and presented. Planned contributions from this study include building upon the existing body of knowledge in the areas of SRM, and the resource-based view theory. Also, the use of the CMMI-SVC framework will serve as an alternative capability maturity model approach for

academic researchers and practitioners when considering processes that are integrated among other processes.

Individuals' Concern about Information Privacy in AR Mobile Games

Dapeng Liu
Virginia Commonwealth University, liud22@vcu.edu

Abstract
Augmented Reality (AR) proves to be an attractive technology in mobile games. While AR techniques energize mobile games, the privacy issue is raised to be discussed. Employing social media analytics (SMA) techniques, this research makes efforts to examines Twitter postings of "PokemonGo" case and explores individuals' attitudes toward privacy in AR games. In this research, we examine what are the privacy concerns of individuals in AR games and what are the individuals' sentiments toward privacy. In the interesting case of PokemonGo, this paper suggests that individuals' concerns about privacy are emphasized on six dimensions - collection, improper access, unauthorized secondary use, errors, post event reimbursement and proactive announcement. The findings could benefit AR game industry to identify privacy problem in discussion and to manage post privacy-event intervention.

Keywords: Information Privacy, Individuals' Concern, AR Games, Social Media Analytics

Disciplines
Information Security | Management Information Systems | Technology and Innovation

Summary

Augmented Reality (AR) proves to be an attractive technology in mobile games. While AR techniques energize mobile games, the privacy issue is raised to be discussed. While big data presents to the web users the electronic social media such as Twitter, which provides information on human sentiments, attitudes, or concerns, this research employs social media analytics (SMA) techniques, examines Twitter postings of "PokemonGo" case and explores individuals' attitudes toward privacy in AR games.

The purpose of the paper is to examine what are the privacy concerns of individuals in AR games and what are the individuals' sentiments toward privacy. In the interesting case of PokemonGo, this paper suggests that individuals' concerns about privacy are emphasized on six dimensions - collection, improper access, unauthorized secondary use, errors, post event reimbursement and proactive announcement.

Our results enhance our understanding of privacy concerns as previously identified. The findings could benefit AR game industry to identify privacy problem in discussion and to manage post privacy-event intervention. In this case, the results also suggest that while that PokemonGo has noticeable privacy problems, the public show very little emphasis on privacy and much more emphasis on the entertaining part of the game.

Investigating Cyberbullying in Social Media: The case of Twitter

Xin Tian
Old Dominion University, xtian@odu.edu

Abstract
Social media has profoundly changed how we interact with one another and the world around us. Recent research indicates that more and more people are using social media sites such as Facebook and Twitter for a significant portion of their day for various reasons such as making new friends, socializing with old friends, receiving information, and entertaining themselves. However, social media has also caused some problems. One of the problems is called social media cyberbullying which has developed over time as new social media technologies have developed over time. Social media cyberbullying has received increasing attention in recent years as the media began shedding light on the devastating consequences that bullies can bring to their victims via social media. During the past few years, there has been a sharp rise in media reports regarding the use of social media to annoy, humiliate, intimidate, bully, and threaten others, with harmful consequences such as emotional distress, anxiety, depression and in some cases, suicidal tendencies. Therefore, it is imperative for researchers to investigate the phenomenon of social media cyberbullying.Thisstudy identifies public cyberbullying messages on Twitter and then specifically examines the diffusion of these cyberbullying messages through Twitters. Java programs were developed to gather Twitter cyberbullying messages using search API offered by Twitter and then these messages were analyzed in depth to understand how people retweet cyberbullying messages on Twitter.

Disciplines
Information Security | Management Information Systems | Management Sciences and Quantitative Methods | Technology and Innovation

SUMMARY

Cyberbullying messages are retrieved from twitter and were analyzed. The analysis results did not find significantly strong relationship between the negative sentiments and the number of retweets. However, an interesting finding is found regarding the top 50 messages with retweets. The results are pronounced and showed that support the hypothesis 1: *The more negative a Twitter cyberbullying message exhibits, the more often it will be retweeted.* That means the cyberbullying message with more negative words typically spreads more often. The speed of retweeting for negative sentiment messages is faster than that of positive sentiment messages. The Hypothesis 2 is also supported. The mean of the number of retweets in is 164,683. Such a large number indicates that the retweeting behavior may have a significant impact on the victims who are suffered from the harassment. Although social media is a useful tool to help people communicate with others, it could become a tool utilized by bullies to hurt other people. As bullying on social media is particularly harmful to the adolescent (Gilkerson, 2012), more studies on bullying prevention is needed.

Educating adolescent about cyberbully is so important because it can effectively prevent and stop cyberbullying from happening and worsening. One recent research find violence tendency is positively related to cyberbullying perpetration (Sari and Camadan, 2016). Goodboy and Martin (2015) found that of the personnel traits, psychopathy emerged as the unique predictor of cyberbullying. They suggest that personality traits are important predictors of computer-mediated behavior. To reduce the spreading and development of cyberbullying, educators should be proactive to recognize the characteristics of cyberbullying messages, develop relevant mechanisms and policies to identify cyberbullying messages as early as possible and address the implications caused by cyberbullying.

This case study shows that the more negative cyberbullying messages, the more retweets will happen and negative messages spread faster than positive messages. The results have some implications for social media providers, educators, parents, students, and school policy makers. For social media providers such as Facebook and Twitter, they can use this methodology to determine if there is a need to eliminate some of the negative tweets that cause so many retweets because such messages could potentially hurt young kids. Twitter could develop a new filter and require user-identity verification to limit the bullying. Social media sites still do not have enough action to address harassment on the site. Educators from middle school and high school should let their students know the consequence of cyberbullying and teach them how to identify and deal with the cyberbullying messages. Parents and students should be educated about cyberbullying. Policy makers need to be proactive to develop relevant mechanisms and policies to reduce the happening of cyberbullying. As for future research, I plan to mine the contents in these tweets

through machine learning and data mining techniques in order to better identify how content characteristics (e.g., topics, URL and hashtag) and network characteristics (e.g., friends/followers or not) are related to retweet behavior.

REFERENCES

Gilkerson, L. (2012). Bullying Statistics: Fast Facts About Cyberbullying. Available at http://www.covenanteyes.com/2012/01/17/bullying-statistics-fast-facts-about-cyberbullying/

Goodboy, A. K., & Martin, M. M. (2015). The personality profile of a cyberbully: Examining the Dark Triad. *Computers in Human Behavior*, 49, 1-4.

Sari, S. V., & Camadan, F. (2016). The new face of violence tendency: Cyber bullying perpetrators and their victims. *Computers in Human Behavior*, 59, 317-326.

Investigating Information Security Policy Characteristics: Do Quality, Enforcement and Compliance Reduce Organizational Fraud?

Dennis T. Brown
Kennesaw State University, dennistedbrown@gmail.com

Abstract
Occupational fraud, the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets, is a growing concern for all organizations. While the typical organization loses at least 5% of annual revenues to fraud, current methods of detection and prevention are not fully adequate to reduce increasing occurrences. Although information systems are making life easier, they are increasingly being used to perpetrate fraudulent activities, and internal employee security threat is responsible for more information compromise than external threats.

The purpose of this research is to examine how information security policy quality and enforcement impacts compliance and mediates organizational fraud levels in a sampling of small to medium-size firms. We will examine if (1) organizations with low (high) quality information security policy experience lower (higher) information security policy compliance; (2) organizations with strong (weak) enforcement of the existing policy experience lower (higher) levels of information security policy compliance; (3) if there is any significant interaction effect between information security policy quality and enforcement and (4) if perceived information security policy compliance is inversely related to reported organizational fraud.

Completion of this research will approach the fraud problem from a perspective that has not been studied previously and will inform current findings regarding the potential direct and indirect effects of information security noncompliance on organizational fraud by giving insights into the motivation leading to compliance versus noncompliance decisions encountered by employees in various organizational settings.

Disciplines
Accounting | Information Security | Management Information Systems | Technology and Innovation

SUMMARY

Fraud reduces every organization's ability to reach its full potential. It is a major risk businesses face, and is increasingly difficult to detect and prevent. Fraud is a latent crime, with a true, complete impact is difficult to comprehensively measure. Global business costs resulting from fraud exceeded USD$2.9 trillion or five percent annually as of 2010. Fraud impacts society to such a degree that it has effectively reduced overall consumer and investor confidence in core business processes.

The purpose of this research is to examine the impact of information security policy quality and enforcement on information security policy compliance and ultimately on organizational fraud using General Deterrence Theory (GDT) and the Theory of Planned Behavior (TPB). Past research has linked information security policy quality and enforcement to information security policy compliance; however, any potential relationship between information security policy compliance and fraud has not been studied, although many of the accounting and behavioral "Red Flags" associated with fraud are linked to information security and policy compliance.

Multiple methods of fraud detection and prevention have been explored to address increasing trends of organizational fraud. These methods include expanded traditional audits (including more appropriate analytical procedures), automated approaches, data analytics, data visualization, meta-learning frameworks, data mining, and the Analytic Hierarchy Process. Current approaches and potential solutions have not fully met expectations and require significant improvement to stem rising losses.

Completion of this research will accomplish several key objectives. First, this study will approach the increasing fraud problem from a totally different perspective that has not been studied previously. It will also expand the body of organizational fraud knowledge by giving insights into the motivation leading to compliance versus noncompliance decisions encountered by employees in various organizational settings. It will also give organizations increased insight into prevention and mitigation strategies for this increasingly common and damaging threat.

Investigating the Influence of Perceived Uncertainty on Protection Motivation: An Experimental Study

Ali Vedadi
Mississippi State University, ali.vedadi@gmail.com

Abstract
IS users and organizations must take necessary measures to adequately cope with security threats. Considering the importance and prevalence of these issues and challenges, IS security research has extensively investigated a variety of factors that influence IS users' security intentions/behaviors. In this regard, protection-motivated behaviors are primarily based on individuals' personal cognitive evaluations and vigilance. In reality, however, many users reach security hygiene decisions through various non-rational and non-protection-motivated processes. Such users may not necessarily rely on their own cognitive appraisals and information processing, but proceed to make decisions without careful cognitive assessments of security threats and coping responses. One promising lens for assessing these behaviors that may not be informed by rational and personal assessments of threats and responses is Herd Theory, which describes the phenomenon in which individual decisions are often influenced by other users' decisions about their behaviors. Drawing on this theory, this study seeks to answer the following research questions by using an experimental design:. *In uncertain circumstances, are individuals more likely to cope with security threats by following the herd?*

Disciplines
Information Security | Management Information Systems | Technology and Innovation

SUMMARY

Information System (IS) assets are subject to diverse threats to security and privacy, including malware infection, data loss, compromised passwords, and identity theft, which are detrimental to organizational infrastructure, often leading to challenges to confidentiality, integrity, and data availability. In this regard, IS users and organizations alike must take necessary measures to adequately cope with the threats. Considering the importance and prevalence of these issues and challenges, IS security research has extensively investigated a variety of factors that influence IS users' security intentions/behaviors including threat appraisal, coping appraisal, fear appeals, subjective norms, and security-related self-efficacy.

Protection Motivation Theory (PMT) suggests that after receiving fear-arousing stimuli, individuals undergo two primary appraisal stages – threat appraisal and coping appraisal – that may contribute to protection motivation and intention to engage in responses recommended by the fear arousing stimuli such as fear appeals. A fear appeal initially triggers a threat-appraisal process in which the message recipient cognitively assesses his or her susceptibility or vulnerability to the stated threat, and then assesses the severity of that threat. Then, in the coping-appraisal stage, a person's response efficacy, perceived response cost, and self-efficacy determine the subsequent coping behavior. It should be noted that protection-motivated behaviors are primarily based on individuals' personal cognitive evaluations and vigilance. In reality, however, many users exhibit security hygiene-related behaviors through various non-rational and non-protection-motivated processes.

One promising lens for assessing these behaviors is Herd Theory, which describes the phenomenon in which individual decisions are often influenced by other users' decisions about their behaviors. Some of the IS users pay more attention to threats, enabling the proximal users (those with less security-related awareness and skills) to be less vigilant without decreasing their level of security. This has been found to guide individual behaviors in many contexts, but it has not yet been investigated in the context of responding to information security threats. Accordingly, we seek to answer the following research question: *In uncertain circumstances, are individuals more likely to cope with security threats by following the herd?*

According to Herd Theory, the processes of discounting one's own beliefs and the imitating of others when adopting new technologies or behavioral practices are prompted mainly by the observation of prior adoptions and uncertainty-related perceptions regarding the adoption of new technologies. IS security literature has been silent on how herd behavior can be substituted for

the traditional coping appraisal, or under what circumstances an individual faced with these environmental influences might respond according to the processes described by Herd Theory or by PMT. The ultimate goal of this study is to determine whether herd behavior can be a better theoretical lens than PMT in predicting and explaining home users' coping with security threats in highly uncertain circumstances. We employ a 2x2 experimental design and analyze data using covariance-based SEM (AMOS vs22). Overall, this paper aims to provide insights on how herd behavior can influence protection-motivation behaviors.

IS Security Research Development: Implications For Future Researchers

Kane Smith
Virginia Commonwealth University, smithkj6@vcu.edu

Chris Merritt
Virginia Commonwealth University, merrittcd@vcu.edu

Abstract
Security within the context of Information Systems has long been a concern for both academics and practitioners. For this reason an extensive body of research has been built around the need for protecting vital technical systems and the information contained within them. This stream of research, termed Information Systems Security (ISS), has evolved with technology over the last several decades in numerous different ways. This evolution can create a great deal of difficulty for researchers to identify under-represented areas of ISS research as well as ensure all relevant areas of concern are addressed. The purpose of this paper is threefold: First, our goal is to map the progression of ISS research from past to present. Second, conduct a review of ISS literature from the date of the last holistic literature review to present, identifying key security thematic presented in these works, grouping them categorically. Lastly, from this review we explain the thematic these works resolve to and based on these categories we discuss where ISS research currently stands.

Disciplines
Information Security | Management Information Systems | Technology and Innovation

Comments
Summary Version

SUMMARY

Security within the context of Information Systems has long been a concern for both academics and practitioners. For this reason an extensive body of research has been built around the need for protecting vital technical systems and the information contained within them. This stream of research, termed Information Systems Security (ISS), has evolved with technology over the last several decades in numerous different ways. This evolution can create a great deal of difficulty for researchers to identify under-represented areas of ISS research as well as ensure all relevant areas of concern are addressed. It is for this reason this work exists, to discern where our field has been, where it is currently at and prognosticate where we believe it should be heading in order to maximize its valuable contributions in Information Systems Security. This is not the first effort in this regard as previous researchers have done the same, looking holistically at the entire field of ISS; however the first review of this kind occurred by Baskerville (1993) and the last by Siponen & Oinas-Kukkonen (2007) with two others between them (Dhillon & Backhouse 2001 and Siponen 2005). For this reason it is now important to again evaluate the current state of ISS research and make a call towards under-researched areas of this field.

The body of knowledge regarding ISS research has continued to evolve since the work of Baskerville (1993), Dhillon & Backhouse (2001), and Siponen (2005). These three works were comprehensive assessments of the "current" state of information systems security research, and each prognosticated the future directions of research in the field. An extensive review of current Information Systems Security Research (ISS research moving forward) uncovered two additional holistic reviews of ISS research, McFadzean et al. (2006) and Siponen & Oinas-Kukkonen (2007), which are extensions of Dhillon & Backhouse (2001) and Siponen (2005) respectively. Since Siponen & Oinas-Kukkonen (2007), all additional literature reviews in ISS research have only been focused on specific streams of research within the field instead of all-encompassing assessments of the direction of ISS research. Therefore the purpose of this paper is threefold: First, our goal is to map the progression of ISS research from Baskerville (1993) to present by describing their assessment of the field at the time and then visions for the future. Second, we conduct a review of ISS literature from 2007 (the date of the last holistic literature review) to present 2016 and identify the key security thematic presented in these works, grouping them categorically. Lastly, from this review of ISS literature from 2007 to present we explain the thematic these works resolve to and then discuss based on these categories where ISS research currently stands. Using this current standing as a launching point, we are then able to address where gaps, potential opportunities for new research, exist and can be

exploited by new researchers in our field. The aim of this work is to ultimately make a call back to holistic research practices so that under-researched areas of Information Systems Security can be developed to the benefit of the field as a whole.

The Role of State Privacy Regulations in Mitigating Internet Users' Privacy Concerns: A Multilevel Perspective

Tawfiq Alashoor
Georgia State University, talashoor1@gsu.edu

Abstract
In the U.S., there is no comprehensive national law regulating the collection and use of personal information. As a response to the high level of privacy concerns among U.S. citizens and the currently limited regulations, states have enacted their own privacy laws over and above the principles of Fair Information Practices (FIP). In this exploratory study, we draw upon the privacy literature and the Restricted Access/Limited Control (RALC) theory of privacy to study the privacy concerns phenomenon with a multilevel theoretical lens. We introduce and test three novel propositions pertaining to the impact of state level privacy regulations on privacy concerns. This combines consideration of individual differences as well as state level factors in predicting individuals' Internet privacy concerns. Overall, the results provide support for the role of state level privacy regulations in mitigating individuals' privacy concerns. We discuss the results, theoretical contributions, policy implications, and future research.

Disciplines
Information Security | Management Information Systems | Privacy Law

Comments
Keywords:

State privacy regulations, privacy concerns, surveillance, behavioral outcomes, multilevel analysis

Only an abstract and summary are pushed in the Proceedings.

SUMMARY

Digital innovation has resulted in increased convenience for customers and greater market reach for organizations. But, it has also increased the risk of consumers' privacy exposure as information is easily collected, transferred, shared, and searched, leading to elevated concerns for privacy among Internet users. Privacy concerned users are less likely to divulge personal information, provide accurate information, accept the technology, and use online shopping and other online services. While mitigating these concerns is important for streamlining the digital innovation, many organizations do not have robust plans to counter privacy exposure and employees often lack awareness of how to handle personal customer data. As a result, governmental interventions—in the form of enacting legislation on online privacy—are imperative in order to preserve individuals' privacy rights and alleviate their concerns.

In the U.S., there is no comprehensive online privacy law that addresses the collection and use of Internet users' personal information through digital channels. In the past two decades, however, states have enacted further legislations and laws over and above the Fair Information Practices (FIP) principles supported by the general federal privacy laws. State level actions to this end are seen as a response to the high level of privacy concerns among U.S. citizens and the currently limited federal regulations. For instance, some states have imposed many requirements on governmental and corporate websites to describe data gathering and to ensure other privacy practices. Such form of regulation is aimed at protecting the privacy of individuals of those states. Yet, there is a lack of clarity as to how effective these state regulations have been in mitigating individuals' privacy concerns. In this exploratory study, we pose the question: How do state privacy regulations affect individuals' concerns for privacy and behavioral outcomes?

We draw upon the privacy literature and the Restricted Access/Limited Control (RALC) theory of privacy to develop three novel propositions, arguing for the multilevel nature of the privacy concerns phenomenon. The RALC theory suggests that information privacy can be achieved in a situation through norms, policies, and laws that have been formulated to protect individuals (e.g., Internet users) in that situation (e.g., an Internet activity). In two survey studies, we provide empirical support for the role of state level privacy regulations in

mitigating users' privacy concerns. Such findings provide critical policy implications, especially to state legislators and governors. States that have made little progress in passing privacy laws in order to provide protection to their citizens are strongly recommended to consider taking this issue into consideration. A succinct conclusion from this study is that individuals residing in states with a higher number of privacy laws tend to be less concerned about surveillance practices and Internet privacy. These associations are insightful because they carry over to affect behavioral outcomes, such as online purchasing behaviors, that have significant impact on the national economy. We conclude the paper with avenues for future research needed to corroborate the tentative conclusions drawn from this exploratory study.

Towards A Comparison of Training Methodologies on Employee's Cybersecurity Countermeasures Awareness and Skills in Traditional vs. Socio-Technical Programs

Jodi Goode
Nova Southeastern University, jp1587@nova.edu

Abstract
Organizations, which have established an effective technical layer of security, continue to experience difficulties triggered by cyber threats. Ultimately, the cybersecurity posture of an organization depends on appropriate actions taken by employees whose naive cybersecurity practices have been found to represent 72% to 95% of cybersecurity threats and vulnerabilities. However, employees cannot be held responsible for cybersecurity practices if they are not provided the education and training to acquire skills which allow for identification of security threats along with the proper course of action. This work-in-progress study addresses the first phase of a larger project to empirically assess if there are any significant differences on employees' cybersecurity countermeasures awareness (CCA) and cybersecurity skills (CyS) based on the use of two security education, training, and awareness (SETA) program types (traditional vs. socio-technical) and three SETA delivery methods (face-to-face, hybrid, & online). In the first phase, a panel of subject matter experts (SMEs) will review SETA program topics and the measurement criteria for CCA and CyS per the Delphi methodology. The SMEs' responses will be incorporated into the development of two SETA program types with integrated vignette-based assessment to be delivered via three methods.

Disciplines
Information Security | Management Information Systems | Technology and Innovation

SUMMARY

Concern over cybersecurity breaches continues to grow as organizations gain a greater understanding of the financial impact, loss of company information assets, and harm to business reputation that can transpire from cyber threats. Employees' naive cybersecurity practices have been found to represent 72% to 95% of cybersecurity threats and vulnerabilities to organizations. This revelation has initiated research concentrated on technological solutions to secure systems, motivation of attackers, profile aspects, and loss which can result from the impact of breaches. However, focus on technical aspects alone against cyber threats is not enough. Organizations, which have established an effective technical layer of security, continue to experience difficulties triggered by cyber threats.

As technology becomes increasingly critical for achieving business objectives, state of the art security systems can provide a false sense of protection to organizations. Research must encompass the human-centric lens, as employees are often the potential targets or unintentional facilitators in cyber-attacks. Previous research has found raising employee awareness of security policies, as well as the implementation of security education, training, and awareness (SETA) programs to be beneficial in mitigating cybersecurity threats. SETA programs can be used to empower employees, who are often cited as the weakest link in information systems security due to limited knowledge and lacking skillsets.

This study will seek to address the lack of theoretically grounded empirical studies related to the design and effectiveness of SETA programs and will explore the differences in cybersecurity countermeasures awareness and cybersecurity skill based on SETA program type and delivery method. The first phase of this work-in-progress study will develop a validated measurement tool to properly assess the cybersecurity countermeasures awareness and cybersecurity skill level of employees due to the limitations of construct measurement in previous research. To address this need, the first four specific research questions of this work-in-progress study will focus on use of the Delphi methodology to determine subject matter experts' approved measurement criteria for cybersecurity countermeasures awareness and cybersecurity skill, as well as the development of two SETA programs with integrated vignette-based assessment. Additional research questions and hypotheses will be addressed in the second and third phases of the study which are considered future research.

Towards a Development of a Mobile Application Security Invasiveness Index

Sam Espana
Nova Southeastern University, espana@nova.edu

Abstract
The economic impact of Mobile IP, the standard that allows IP sessions to be maintained even when switching between different cellular towers or networks, has been staggering in terms of both scale and acceleration (Doherty, 2016). As voice communications transition to all-digital, all-IP networks such as 4G, there will be an increase in risk due to vulnerabilities, malware, and hacks that exist for PC-based systems and applications (Harwood, 2011). According to Gostev (2006), in June, 2004, a well-known Spanish virus collector known as VirusBuster, emailed the first known mobile phone virus to Kaspersky Lab, Moscow. Targeting the Symbian OS, the worm spread via Bluetooth. Ten years later, Kaspersky Lab reported 884,774 new malicious mobile programs (Unuchek & Chebyshev, 2015).

On the one hand, during mobile application installations, users typically agree with the vendor's end-user license agreement (EULA) as a contract between the licensor and licensee. On the other hand, there is no easy way for users to monitor approved software functionality (i.e., automatic updates) as opposed to unapproved functionality (i.e., unwanted Bluetooth connectivity).

This paper presents, as the primary goal, the development of the Mobile Application Security Invasiveness (MASI) Index for assessing the level of invasiveness of covert application functionality. By assessing the MASI Index of an application, users should be able to score its invasiveness, classify it (i.e., non-invasive application or invasive application) and potentially uninstall it.

Disciplines
Digital Communications and Networking | Information Security | Management Information Systems | Risk Analysis | Technology and Innovation

Comments
The author is a Ph. D. in Information Systems (DISS) student at Nova Southeastern University with Dr. Yair Levy as doctoral research advisor

SUMMARY

Mobile device users should be concerned about downloading certain applications due to the possible application's invasive behavior. This proposed research will define an invasive mobile application as an application that is nonnative to the host operating system under consideration and whose introduction causes, or is likely to cause, economic harm (i.e., productivity loss), system harm (i.e., security breach) or harm to humans (i.e., privacy violation). Hence, its *invasiveness* is defined as the degree of harm or the potential to cause harm to the device, its operating system, applications, system security and/or user's privacy.

This proposed study will seek to develop a mobile application security invasiveness (MASI) index. The MASI Index will be used to analyze a set of mobile applications and score each application's invasiveness from a score of zero (0) when the application demonstrated no invasiveness, to an accumulated score of 100 when the application demonstrated a high degree of invasiveness. The main research question that this study will address is: How will the 100 most highly reviewed mobile applications running on Android, iOS, and Windows operating systems, be classified on the MASI Index?

Towards a Model of Senior Citizens' Motivation to Pursue Cybersecurity Awareness Training: Lecture-Based vs. Video-Cases Training

Carlene G. Blackwood-Brown
Nova Southeastern University, cb2136@nova.edu

Abstract
Cyber-attacks on Internet users, and in particular senior citizens, who have limited awareness of cybersecurity, have caused billions of dollars in losses annually. To mitigate the effects of cyber-attacks, several researchers have recommended that the cybersecurity awareness levels of Internet users be increased. Cybersecurity awareness training programs are most effective when they involve training that focus on making users more aware so that they can identify cyber-attacks as well as mitigate the effects of the cyber-attacks when they use the Internet. However, it is unclear about what motivates Internet users to pursue cybersecurity awareness training so that they can identify as well as mitigate the effects of the cyber-attacks when they use the Internet. This work-in-progress study will empirically investigate what motivates a specific group of Internet users, that is, senior citizens, to pursue additional cybersecurity awareness training, after initial training is conducted. Contributions from this study will add to the body of knowledge on how to motivate Internet users to pursue additional training in cybersecurity, and thus, aid in the reduction of the billions of dollars in losses accrued to Internet users as a result of cyber-attacks. Senior citizens will also benefit in that they will be better able to identify and mitigate the effects of cyber-attacks. The recommendations from this work-in-progress study will also be significant to law enforcement in reducing the number of cases relating to cybersecurity issues amongst senior citizens, and thus, free up resources to fight other sources of cyber crime.

Disciplines
Information Security | Management Information Systems | Technology and Innovation

SUMMARY

Evidence from research indicates that significant financial losses have been accrued to governments, organizations, and Internet users because of limited awareness of cybersecurity countermeasures among the Internet users. Cyber-criminals can launch attacks on Internet users via attack vectors such as unsecured wireless networks and phishing attacks. This results in billions of dollars in fraudulent revenue to the cyber-criminals at the expense of Internet users who are not aware of those types of attacks.

Senior citizens are one of the most vulnerable groups of Internet users who are prone to cyber-attacks, and within the last decade, there has been a significant increase in Internet use among American senior citizens. A report from the Pew Research Center indicates that senior citizens had the greatest rate of increase in Internet usage (107% increase) over all the other age groups that were surveyed between 2000 and 2015. However, while using the Internet, senior citizens are being targeted and exploited, with one in five American senior citizen being a victim of financial fraud, costing more than $2.6 billion per year. Phishing attacks pose serious threats to the private lives of these Internet users, including, but not limited to compromising of confidential information, and identity theft. One of the common fears of senior citizens is identity theft, and coupled with their limited awareness of cybersecurity countermeasures, they feel overwhelmed, frustrated, and demotivated when they use the Internet. After being victims of identity theft, some senior citizens suffer devastating effects, ranging from loss of all their life savings, feelings of shame for being victims, and exacerbated illnesses to include premature death. Therefore, cybersecurity awareness is essential for them as a countermeasure strategy to combat the cyber-attacks that they face.

In spite of the losses caused by cyber-attacks, and the attempts at providing cybersecurity awareness, it appears that it is still unclear about what motivates Internet users to pursue cybersecurity awareness training so that they can identify as well as mitigate the effects of new upcoming cyber-attacks. This work-in-progress study answers the call from several researchers to increase the awareness of cybersecurity countermeasures of Internet users so that they can stay up-to-date on the available cybersecurity tools and procedures that can protect their personal data, as well as themselves whenever they use the Internet. This will be done by empirically assessing a model of some contributing factors (cybersecurity awareness, computer self-efficacy, and perceived risk of identity theft) on the

motivation of senior citizens to pursue additional cybersecurity awareness training. Groups of senior citizens will receive cybersecurity awareness training using different delivery methods. Measurements of each contributing factor will be taken before the training as well as after, up to a period of four weeks. The measurements will then be statistically analyzed, and discussed. A better understanding of the types of cybersecurity awareness countermeasure training that can contribute to the motivation of Internet users to pursue training to reduce the effects of cyber-attacks will be provided.

Training Decrement in Security Awareness Training

Tianjian Zhang
tj.zhang@okstate.edu

Abstract
This study determines if there is a decremental effect following IT security awareness training. In most security policy compliance literature, the main focus has been on policy design. Studies that address security awareness training are seldom theory driven and even fewer are empirically based. To fill this gap, we draw from the theory of vigilance decrement as well as forgetting curves in psychology, and propose a classroom experiment showing that participants' IT security awareness decreases over a 45-day period since the training at day one. The result adds to the security policy compliance literature and suggests that some policy violations are due to the decrement in vigilance and security knowledge. The practical implications are that companies need to train their employees repeatedly overtime in order to maintain a high level of IT security policy compliance.

Disciplines
Information Security | Management Information Systems | Technology and Innovation

Comments
This is a work in progress.

Keywords: security awareness, training, vigilance decrement, forgetting curve.

SUMMARY[1]

Information security breaches have been a major issue for organizations. According to the 2011 Computer Crime and Security Survey by the Computer Security Institute (CSI), 41.1% of organizations experienced computer security breaches within the past year.

Many of the breaches are of non-malicious nature. The recent Ernst & Young's Global Information Security Survey suggests that careless or unaware employees is considered the leading security vulnerability. However, the same survey also reveals that at least 30% of the organizations have no security awareness training program. Other surveys suggest the percentage may be higher.

While the industry has recognized the lack of security awareness training, academia has yet to shift more focus towards awareness training. Most security policy compliance literature focus on the mechanism behind employees' intentions to comply. Studies that do address security awareness training are seldom theory driven and even fewer are empirically based. To fill the gap, we draw from the theory of memory retention in psychology, and propose a classroom experiment to show that *participants' IT security awareness decreases over time following the security awareness training*. This study suggests that even those with training programs do not necessarily prepare employees to deal with security issues in the long run.

Participants of the study are from three different sections of an introductory class in information systems in a large mid-western public university. Security knowledge will be measured by security awareness quiz results. On day 1, participants took an in class quiz (pretest) on security training. A week after the pretest, a lecture on security awareness was delivered by the course instructor to serve as the security awareness training. Immediately after the lecture, participants took quiz (posttest 1). Depending on which of the three class sections the students are in, participants will take a third in class quiz (posttest 2) 15, 30 or 45 days after posttest 1. We expect posttest 2 scores to be lower than that of posttest 1, and the difference to be positively related to the number of days in between. We will use repeated measures ANOVA to analyze the data. Prior studies have shown the amount of time it takes for knowledge to tend to 0 ranges from one to three weeks.

[1] Data collection is in process.

The longer time interval in this pilot study is to ensure we capture the decrement. Further studies will adjust the interval length accordingly.

Limitation of the study includes the use of student sample, and not measuring the effect of repeated training on knowledge retention. The latter is partly due to the time cost of repeated training in a classroom. The study will add to the security policy compliance literature suggesting that some policy violations are due to the decrement in security knowledge. The practical implications are that companies need to train their employees repeatedly over time in order to maintain a high level of IT security policy compliance.

User Privacy Suffers at The Hands of Access Controls

Chad N. Hoye
University of West Florida, cnh22@students.uwf.edu

Abstract
With advancements in personal hand held devices, smaller more mobile computers, tablets, and the world's population connected with social media the threat to the user's privacy has been diminished. I will look at how access control policies have opened the proverbial door to user's privacy being attacked and threatened. You will see examples of how users have to divulge personal information to get better service and even be monitored while at work to prevent intrusions in to the company.

Disciplines
Information Security | Management Information Systems | Social Psychology | Technology and Innovation

INTRODUCTION

With advancements in personal hand held devices, smaller more mobile computers, tablets, and the world's population connected with social media the threat to the user's privacy has been diminished. I will look at how access control policies have opened the proverbial door to user's privacy being attacked and threatened. You will see examples of how users have to divulge personal information to get better service and even be monitored while at work to prevent intrusions in to the company.

ACCESS CONTROLS

When pulling up to the front gate of a military instillation there will be a guard standing there ready to check your ID to verify that you have the proper credentials to be allowed on to the installation. The guard acts as a control point for the base verifying that you have permission to access the installation. The security guard is a type of physical access control and we are here to talk about digital controls that are implemented inside of the systems and networks where people try and access information for many different purposes. Basic access control policies include a username and password that will be entered to verify the user identity and permissions for system usage. We as a collective of data specialist and security professionals have come to the realization that these most basic controls are not viable anymore to protecting sensitive governmental and corporate information.

That's is why there are more in depth access control policy methods such as: Mandatory Access Control (MAC), Role Based Access Control (RBAC), Discretionary Access Control (DAC), and Rule Based Access Control (RBAC) (Infosec Institute, 2012). Looking at security and the ability of control within the systems, mandatory access control is by far the most restrictive for the user. The user has no privileges or control over the systems within the computers or devices that would allow them to set access to certain data or programs. Everything is controlled by an administrator and that administrator is the one that provides the privileges for each user on their devices. The MAC method is very administrator intensive and demanding since they are the only ones that can set the privileges for each user in the system.

Within MAC there is a model called Bell-LaPadula named after its authors and creators (Infosec Institute, 2012). The US government and many other governments are famous for using this model in the form of *Top Secret* and other levels of security for their data and information. There is complexity to how the model sets up it access to certain documents by not allowing a person at a certain security level to access information at a higher level but can obtain and read information at a lower security level. As an example Jamie, who has a Tier 2 *Top Secret* security clearance,

has composed a document and saved it to her company's server. Blake, only having a *Secret* level security clearance will be unable to access or read the document. In turn if Blake has written something and saved it on the same server Jamie, having a high security level, would be able to access the file and read through it. Jamie would also be able to write into the document that Blake has created. The US Government has added changes to this model to make it more secure and to not allow for the misuse use of data by implementing a *need to know* basis for being able to access information of the same security level or lower as the user. Meaning that if the user has no reason for accessing the data then they will not be given permission to access it mitigating internal theft and someone being able to access data that is not part of their defined job.

Fine-grained and context-based access control policies are much better at providing data and information confidentiality, integrity, and availability, also known as CIA. Context-based access controls also known as CBAC use an intelligent firewall that filters TCP and UDP packets based on application layer protocol session information (Context-based Access Control, 2016). Where *Fine-Grained* access control policies allow the user to only access theirs companies information during certain working hours (Brossard, 2011). The challenge with these two types of control policies is and will always be the internal threat, the user having authorization to access organizational proprietary and sensitive data for misuse and worst case theft. In 2014 the US Fraud Retail Survey found and identified that employee theft was the biggest cause of loss to retailers (Leinbach-Reyhle, 2015). Although that survey was on a retail market the same can be said about any company and its corporate structure. To improve these control policies extended access control models have been proposed, including time-based access control models, location-based access control models, purpose-based access control models, and attribute-based access control models that restrict data accesses with respect to time periods, locations, purpose of data usage, and user identity attributes (Nabeel, Shang, and Bertino), respectively.

USER PRIVACY

Access control policies secure and provide confidentiality, integrity, and availability for an organizations or governments data and information but what about the user's personal information that is being collected and stored while he or she is using the system. With the growing amount of social media sites in use by people all around the world, maintain privacy for the user is a precious commodity. Facebook allows the user to dictate what he or she will have displayed on their page just as a company puts access controls on their systems. These controls can range from allowing a certain post to be viewed by the user's friends only or by the entire world if they so choose. Not only is a user's personal information being used for public viewing on social media but is now being used for all sorts social engineered

processes. Ranging from the advertisements that are displayed on the webpages being viewed to data inputted into algorithms that will predict what pictures to display on the users Instagram account.

All around the world we as a collective people amass 2.5 quintillion bytes of data every day being spread across massive networks of computers increasing the attack surface of the entire system (CSA, 2012). As people make searches, order items off retail websites, and post news updates to their Facebook page data is being collected about them and stored. How is this data being used and for what purpose?

Alan Westin defines privacy as "the ability for people to determine for themselves when, how, and to what extent, information about themselves is communicated to others (Westin 1968)." Abiding by this outlook of privacy, users are giving up control of their personal information at an alarming rate and most don't know it is happening. Social media sites such as Facebook, Twitter, Instagram, and many others have privacy controls that allow the user to dictate how much of their privacy they are willing to sacrifice to the general public of the world. I use the term sacrifice because it is just that. Most of these controls are very vague and hard to interpret and makes it difficult for the user to ascertain what information he or she is making public or private. And being that no two social media sites are going to have the same privacy controls it is doubly difficult adjusting the settings between different websites and trying to maintain these controls as a user can be very difficult.

Social media sites might allow the user to control what they want to share but once the user's personal information is out there in the world wide web there is no getting it back. In 2009 Carnegie Mellon Researchers were able to identify people by their social security numbers using just public records from the internet. Using people's social media pages and governmental records that are public they could correctly identify one out of 20 complete social security numbers born in Delaware in 1996 (Nabeel, Shang, and Bertino). Social Security Numbers being linked to a person's identity make them very valuable to that person. Having your identity stolen is not only a violation of a person's privacy but also to their security in being able to protect their identity.

PRIVACY VS CONTROL

So if someone can so easily use social media and public records to reconstruct a person's S.S.N so easily what's to stop them from trying to make that person do something that they wouldn't normally do. Having access controls implemented and monitoring the user's online behavior allows for internal threats to be prevented or flagged for later inspection. Internal threats are not always intentional decisions and can originate from misuse of the company's data or from a third party through and internal source that is unaware of the intrusion.

No matter intentional or unintentional organizations and governments are always trying to mitigate and lessen the amount of data loss that is due to the internal threat. They mitigate this threat with the use of the access control policies that we were talking about earlier. But on top of those policies because of *Social Media* sites and the abundance of scams, organizations and governments are going a step further to protect their precious data. But at what cost are they doing this? At the cost of the user's privacy?

On a person's profile page, they might have certain information set to allow only friends to view the information, but what is to stop a friend from divulging information about that user to another person. Because of Social media users are targets for specialized spear-phishing attacks and socially engineered scams that are designed to retrieve and ascertain sensitive and personal information that is then later used against that user and in attacks towards the organization. And there lies the dilemma of trying to balance control and user privacy. On one hand you want to prevent unauthorized access and theft of data and on the other hand maintain the privacy of the user's personal information.

Companies with the use of Context-Based access controls are able to watch what it's users are looking at and saying on the world wide web while using their systems. With the data that company collects on its users it is able to construct its own profile of its users. This collection of data and profiles allows the company to spot and track anomalies in its user activity. The company now has a viable way to monitor its users by looking into their personal life to keep its own information safe. When properly implemented content-based access control policies can reduce the improper data accesses and the opportunity of insiders to steal information from the company. As an employee of such a company you are giving up privacy rights to continue your working for said company and some people don't even know that it is happening to them.

With 91% of the worlds adults owning and using a smartphone or tablet (Rainie, 2013) for work and personal use, access control policies need to be more flexible and adapting to change. That is why the models for location-based, time-based, and attribute-based models are so important now. With these control policy models users are able to be mobile and work from their personal devices on corporate data without threat of data loss in the company.

Attribute-based allows for the user to identify himself or herself to the company's system to ask for permission to access it. With every smartphone containing GPS chipset, that most users use for directions, the company's system can then ascertain the user's location and check it against it authorized locations for acceptance. Then comes, time-based access controls, is the user trying to access the system during a pre-determined time of day that is within the company's guidelines. With all three access control models plus context-based implemented, the

company's data is a lot more protected. These controls give the company an abundance of control over its user's privacy to maintain security of data.

At the same time access control policies alone are not always sufficient at protecting and preventing against internal threats. A user might have legitimate permission to access a certain spreadsheet from his company's server from his personal smartphone while he not in the office. But when that user accesses and downloads the spreadsheet instead of adding to it during his normal business hours, the system will detect the anomaly and flag the event for inspection. The access controls were implemented in the system but were only able to flag a misuse and not able to prevent the misuse of the data.

MAKING PEACE

So how do we balance the scales of user privacy with the control of an organizations personal and proprietary data? Playing devil's advocate looking at both sides there is pluses and minus for both sides. It is a give and take scheme in that both are trying to protect the privacy of the user and the data of the organization. On the one hand there are access controls that provide a security blanket for the organization to protecting its data but the user in the organization gives up some of their privacy to help the organization maintain its security. If the user wants to maintain their personal information, it limits how much control the organization can provide for maintaining the security of data.

I propose a model that works with all previously discussed models of access control but implements notifications that notifies the users of what information is being used and for what purpose. When a user is notified about what information that he or she is about to give up they have to the choice to continue or decline to continue. Not only should the notice list what information is being requested but there should also be a statement about who will be receiving the data and for what purpose it will be used. At this point the user is dictating their own privacy model and allowing the organization to use their information for future purposes.

For example, if Jamie is using her tablet from home to access her company's server to retrieve a spreadsheet, the system would notify her that her location, time stamp, and open applications on her tablet will be monitored to identify any anomalies or possible attacks if any were to transpire during her use of the server. If Jamie does not want to allow the company access to her tablet to monitor it while she is accessing their system, then she can simply decline the request and access the document during the normal working hours at her workplace. Two fold Jamie's privacy and the company's data has been maintained and nothing was sacrificed or given up without consent from either party. The same can be done if Jamie was given a work tablet and if she wants to look at her social media sites on that tablet then she will be notified by the system that if she wants to view those sites that she

will be allowing the company to monitor her sites and also be collecting data off them.

The other way that it can work is when a user is at work and they have access to both company data and personal data via social media. Blake is worried about his friend who just lost his mother in a tragic accident, so he visits his friends Facebook page to write and post message expressing his condolences. The system will then notify Blake that if he wants to continue that he will be allowing the company to gain access to his Facebook profile and be able to monitor what he is posting and reading. There is also a disclaimer in the notification that if he continues that the company will be storing any data from his personal profile and may use it later to monitor his online presence. Blake chooses to continue and allow the company to monitor and store data about his online presence through social media allowing them to look for anomalies in his behavior and Blake willing gave them the permission to do this and was given the opportunity to not proceed.

When it comes to the usage of the personal information that the user is willing to give up, the notice should be written in such a way that the user can understand and ascertain exactly what it is being used for. For instance, when entering your likes and dislikes on Facebook there would be a description of what those likes and dislikes will be used for, i.e. targeted advertising on your profile page and certain people's postings as they pertain to the likes that you've set.

Ultimately the access control policies have to be malleable to allow for change and modeling to each individual user instead of an umbrella standpoint. There will still have to be a leveling as to not allow for a user to have access to data that is not intended for their eye but from the stand point that the control can be flexible to allow for changes. People are ever changing and so is the world that we live in. Technology is growing at a rapid rate and changing how people connect with and use data and to protect it and people's personal information the two have to work together cohesively as one.

REFERENCES

1. **Access Control: Models and Methods.** (2012) *Infosec Institute http://resources.infosecinstitute.com/access-control-models-and-methods/*
2. **Nicole Leinbach-Reyhle** (2015), New Report Identifies US Retailers Lose $60 Billion a Year, Employee Theft Top Concern, Forbes Magazine, http://www.forbes.com/sites/nicoleleinbachreyhle/2015/10/07/new-report-identifies-us-retailers-lose-60-billion-a-year-employee-theft-top-concern/#3c863ed31cd9
3. **Context-based Access Control.** (n.d.). *Wikipedia.* Retrieved July 1st 2016, from https://en.wikipedia.org/wiki/Context-based_access_control
4. **David Brossard. (**2011), Coarse-grained vs. fine-grained access control – part I. Identity & Access Management. http://www.webfarmr.eu/2011/05/coarse-grained-vs-fine-grained-

access-control-part-i/

5. **Cloud Security Alliance**. *Top Ten Big Data Security and Privacy Challenges. 2012. https://www.isaca.org/Groups/Professional-English/big-data/GroupDocuments/Big_Data_Top_Ten_v1.pdf*
6. **Nabeel, M., Shang, N., Bertino, E**.: Privacy preserving policy based content sharing in public clouds. IEEE Trans. Knowl. Data Eng. (to appear)
7. **Lee Rainie.** Cell Phone Ownership Hits 91% of Adults. Pew Research Center. http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/
8. **Alan Westin.** Privacy and Freedom (fifth edition) New York, USA: 1968