Man-At-The-End Attacks: Analysis, Taxonomy, Human Aspects, Motivation and Future Directions

Article *in* Journal of Network and Computer Applications · November 2014

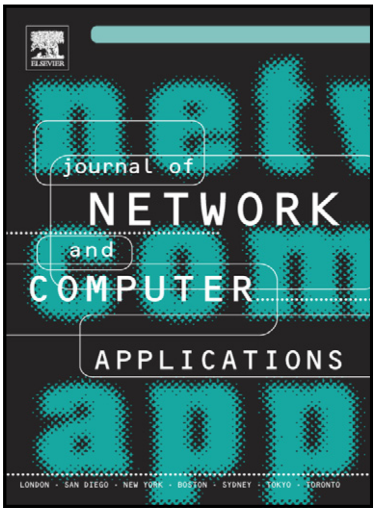
DOI: 10.1016/j.jnca.2014.10.009

Adnan Akhunzada
Technical University of Denmark
137 PUBLICATIONS **2,115** CITATIONS
SEE PROFILE

Mehdi Sookhak
Illinois State University
74 PUBLICATIONS **3,241** CITATIONS
SEE PROFILE

Nor Badrul Anuar
University of Malaya
199 PUBLICATIONS **10,039** CITATIONS
SEE PROFILE

Abdullah Gani
University of Malaya
274 PUBLICATIONS **15,791** CITATIONS
SEE PROFILE



www.elsevier.com/locate/jnca

Man-At-The-End Attacks: Analysis, Taxonomy, Human Aspects, Motivation and Future Directions

Adnan Akhunzada, Mehdi Sookhak, Nor Badrul Anuar, Abdullah Gani, Ejaz Ahmed, Muhammad Shiraz, Steven Furnell, Amir Hayat, Muhammad Khurram Khan

PII: S1084-8045(14)00237-9
DOI: http://dx.doi.org/10.1016/j.jnca.2014.10.009
Reference: YJNCA1322

To appear in: *Journal of Network and Computer Applications*

Received date: 26 May 2014
Revised date: 8 October 2014
Accepted date: 23 October 2014

Man-At-The-End Attacks: Analysis, Taxonomy, Human Aspects, Motivation and Future Directions

Adnan Akhunzada[a], Mehdi Sookhak[a], Nor Badrul Anuar[a], Abdullah Gani[a], Ejaz Ahmed[a], Muhammad Shiraz[a], Steven Furnell[b], Amir Hayat[c] and Muhammad Khurram Khan[d]

[a]Centre for Mobile Cloud Computing Research (C4MCCR), Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia

[b]Information Security & Network Research Group, School of Computing, Communications and Electronics, University of Plymouth, Plymouth, United Kingdom

[c]Applied Security Engineering Research Group, Dept. of Computer Science, COMSATS Institute of Information Technology, Pakistan

[d]Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia

Emails: a.adnan@siswa.um.edu.my, m.sookhak@ieee.org, badrul@um.edu.my, abdullahgani@ieee.org, imejaz@siswa.um.edu.my, muh_shiraz@um.edu.my, sfurnell@plymouth.ac.uk, amir.hayat@comsats.edu.pk, mkhurram@ksu.edu.sa

Abstract

Man-At-The-End (MATE) attacks and fortifications are difficult to analyze, model, and evaluate predominantly for three reasons: Firstly, the attacker is human and therefore, utilizes motivation, creativity, and ingenuity. Secondly, the attacker has limitless and authorized access of the target. Thirdly, all major protections stand up to a determined attacker till a certain period of time. Digital assets range from business to personal use, from consumer devices to home networks, the public Internet, the cloud, and the Internet of Things—where traditional computer and network security are inadequate to address MATE attacks. MATE is fundamentally a hard problem. Much of the extant focus to deal with MATE attacks is purely technical; though, security is more than just a technical issue. The main objective of the paper is to mitigate the consequences of MATE attacks through the human element of security and highlighting the need for this element to form part of a holistic security strategy alongside the necessary techniques and technologies. This paper contributes by taking software protection (SP) research to a new realm of challenges. Moreover, the paper elaborates the concept of MATE attacks, the different forms, and the analysis of MATE versus insider threats to present a thematic taxonomy of MATE attack. The ensuing paper also highlights the fundamental concept of digital assets, and the core protection mechanisms and their qualitative comparison against MATE attacks. Finally, we present state-of-the-art trends and cutting-edge future research directions by taking into account only the human aspects for young researchers and professionals.

Keywords

Man-At-The-End, Software Protection, Information Security, Digital Rights Management, Digital Assets, Distributed Software Systems

1 Introduction

Any security system, no matter how intelligent, well-designed, properly configured, thoroughly deployed, and meticulously maintained, will have to rely on people. The most stimulating and overarching issue in security is the human element – and dealing with it is perhaps one of the biggest challenges we face today. Trying to design information security solutions without due consideration of the complex human nature may prove to be an Achilles heel, “If the human factor is not considered, information security might be just an illusion” (Svensson, 2013).

Technological advancements and innovations make the armory more and more impressive but according to Schneier a high degree of security was in our hands. He further argues that if you think technology can resolve your security problems, then you neither understand the problems nor the technology (Frangopoulos et al. , 2013). Despite the implied focus upon technology, it is increasingly recognized that mere technology cannot provide a complete solution; however, what has only started to receive extensive recognition relatively recently is the role and importance of people as part of the solution (Furnell and Clarke, 2012).

Despite technological progression, the problem of Man-At-The-End (MATE) attacks is primarily harder (and, under very general circumstances, difficult to resolve) than other, more common studied problems in security. The reason behind this is the very liberal attack model that software protection (SP) researchers and practitioners must cope with: it is presumed that an all-powerful adversary who has complete access to our software and hardware, can examine, utilize his or her capabilities, modify, and probe it at will (Ceccato et al. , 2013, Falcarin et al. , 2011, Gu et al. , 2011). Fundamentally, a MATE attack happens in a setting where an adversary gains physical access to a device and compromises it by tampering or inspecting the hardware itself or the software it contains (Jakubowski et al. , 2011). MATE attacks, therefore, essentially encompass an adversary gaining an advantage by violating software or hardware under their control, directly or via a remote connection also known as Remote Man-At-The-End (RMATE) (Collberg, Collberg et al. , 2011). Protection mechanisms against MATE attacks are recognized as anti-tamper techniques, digital asset protection, or, more commonly, software protection (Falcarin, Collberg, 2011).

Due to the powerful attacks launched in a MATE scenario, we typically do not expect any technique in SP to hold off an attack for indefinite period of time (Collberg, Davidson, 2011). Subsequently, no piece of software, no matter how well protected, is likely to survive unscathed for a long period of time. However, an attractive opportunity for MATE attackers is, in-fact, todays open environments, where the attackers prey on every single line of code, and commercial off-the-shelf systems include a plenitude of unpatched and known software vulnerabilities (Broadhurst and Chang, 2013). Moreover, in this dynamic world where digital content mainly relies on software for its storage, consumption, creation, and distribution, it’s becoming an essential obligation that we protect digital assets by continuously upgrading the protections in their associated software. However, today, an increasing number of applications are vulnerable to MATE attacks, and there is a need for comprehensive SP techniques that deliver a nontrivial level of security against determined attacks by skilled adversaries (Jakubowski, Falcarin, 2011). Besides, firewalls are classic solutions to mitigate the threat of remote attackers (i.e., Man-In-The-Middle) who try to break into software systems; however, these typical approaches do not help defending software systems when the attacker is MATE (Ceccato, Di Penta, 2013) and is equally hard to define and measure the MATE attacker’s capabilities (Collberg, Davidson, 2011, Falcarin, Collberg, 2011).

The literature available on MATE is very limited. To the best of our knowledge, this is the first effort that studies MATE in detail. The paper elaborates the concept of MATE attacks, its different forms, and its analysis and characteristics. Moreover, we devise MATE attacks taxonomy by critically analyzing and reviewing the previous taxonomies in different fields of information systems and security. Furthermore, we present three elements in properly securing digital assets, i.e. SP, hardware-based software protection and MATE. However, the bygones of SP research are only based on two elements hardware and, software based protection and some of the latest expert’s opinion put forward the co-design of hardware and software (Gu, Wyseur, 2011); where MATE assessment has been addressed indirectly. Directly addressing the MATE, however, in the security chain has largely been neglected. The paper highlights the need for human aspects to form part of a holistic security strategy alongside the necessary techniques and technologies in SP research. The paper elaborates the concepts of digital assets and review efforts that endeavor to mitigate MATE attack consequences. MATE attacks and their role and effectiveness on high-value digital assets are studied. We contribute by taking SP research to a whole new realm of challenges and present the state-of-the-art trends and future directions researchers should explore while addressing MATE attacks. These novel directions directly take into account the human aspects, i.e. mental capabilities, skills and expertise, different security-related and cross-cultural behavior, curiosity, fear, direct MATE aspects on software resilience, and finding the actual behavior of MATE. Exploring these future research challenges could have high impact and provide greater insight in properly addressing MATE attacks. This in turn enhances the defense capabilities of high-value digital assets with improved extant techniques and leads to innovate and develop state of the art next-generation security tools and technologies (to properly secure distributed software systems and digital assets).

The remainder of this paper is organized as follows. Section 2 describes MATE attacks in detail that includes the concept of MATE attacks, the different forms, and the characteristics and analysis of MATE versus insider threats. Critical analysis and a comprehensive taxonomy of MATE attacks are also devised in this section. Section 3 elaborates the fundamental concept of digital assets; the core protection mechanisms and their qualitative comparison against MATE attacks, and its two broad categories of software and hardware-based software protection. State-of-the-art new trends and future research directions are presented in Section 4. Finally; paper is concluded in Section 5.

2 Man-At-The-End Attacks

In July 2011, the Digital Asset Protection Association (DAPA) is launched to address challenges particular to MATE attacks. The key task for DAPA is to create awareness of the seriousness of MATE attacks among politicians, software developers, government agencies, and the general public (Collberg, Davidson, 2011). Protection mechanisms against MATE attacks are variously acknowledged as digital asset protection or more commonly SP; therefore, the concept of MATE attacks primarily comes from the area of digital asset's protection (DAP) or SP research (Falcarin, Collberg, 2011). Figure 1 depicts the attack in a MATE scenario, where the digital assets, be it media or software, is protected by asset sentries (hardware or software entities that monitor and guard the asset itself). What makes it different from other types of computer security scenarios is that the asset sentry and the digital asset are both under the control of the adversary.

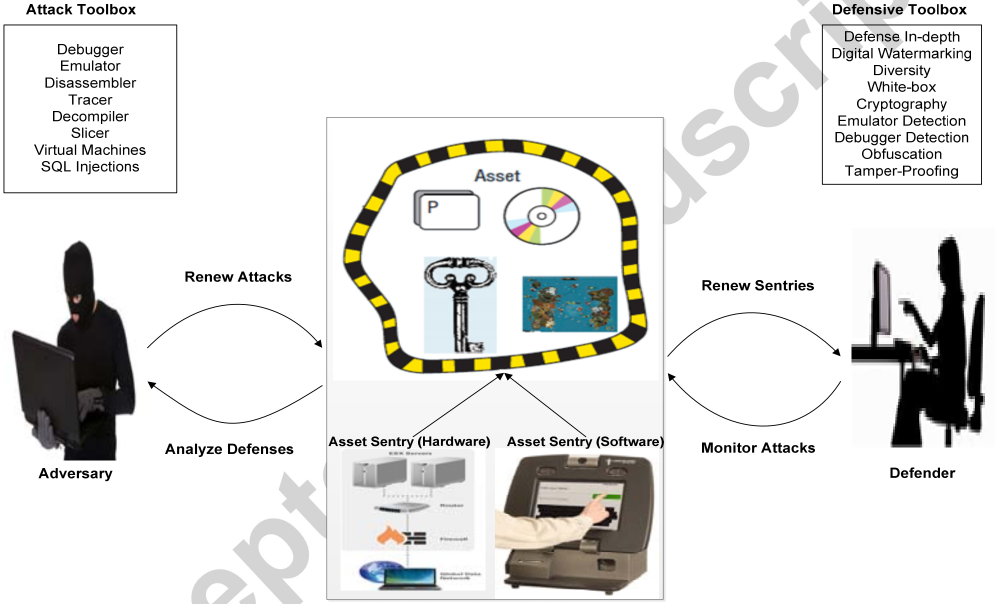


Figure 1: MATE adversary having full access to analyze and utilize their capabilities in circumventing digital asset protections

The defender has procedures for monitoring attacks and tools for constructing and updating sentries, whereas the adversary has a set of tools and techniques for analyzing, modifying, and disabling the sentries. However, both the adversary and defender have equal access to analyze the system. The attacker's curiosity always increases to defeat the digital asset protection by all means; while the defender adds defense-in-depth and diversity to make sure that every single asset sentry is different, making it more problematic for the adversary to build attacks that are effective on entire classes of sentries.

In standard practice, it might seem that encrypting transmitted documents would be enough to ensure the integrity and confidentiality of data. This, however, essentially disregards MATE-style attacks that target the endpoints of data transmission (Collberg, 2011). This problem becomes even more serious when using mobile or other portable devices, such as PDAs and laptops, placed outside in an environment which is not physically secured. Moreover, in a real scenario, a disgruntled system administrator might be legally add new malicious users, run backup scripts that would destroy user sensitive data and could modify and update critical database entries. Such MATE attackers are partially trusted and might have the capability to conceal their tracks, for instance, by modifying log files, which makes such attacks, particularly even more challenging to counter (Collberg, Davidson, 2011).

2.1 Different Forms of MATE Attacks

MATE attacks can take several forms where the adversary has physical and authorized access to the attack target. In this section, we briefly describe some forms of MATE attacks from the literature. In one type of MATE attack, while conducting a tampering attack at an individual level (Martinez et al. , 2013), a MATE adversary disrupts the integrity of a piece of software under his control, possibly by altering it in ways the software vendor did not expect. In addition, cheating massively in multi-player online games by modifying client software (Falcarin, Collberg, 2011, Jeng and Lee, 2013). Moreover, to launch a reverse-engineering attack (Tang et al. , 2013), one can disrupt the vendor's privacy rights by tracing intellectual property from the software, such as designs, algorithms, or implementations. Similarly, a cloning attack (Shan et al. , 2013) violates copyright laws by creating and issuing illegitimate copies of the software. However, on a national level, example attack scenarios include compromises of smart meters to launch denial of service attacks in the electric power grid which could possibly cause countrywide blackouts (Qin et al. , 2013). Moreover, in wireless sensor networks used for monitoring military combat zones, a compromised sensor node by a MATE adversary might refuse to forward data received from other sensors or can insert wrong data into the system. Furthermore, tampering of computers in order to gain access to medical records, secret military documents or documents containing intellectual property and other sensitive digital information; violation of the Internet protocols to gain an unfair share of network bandwidth, (Falcarin, Collberg, 2011). Besides, to craft personal exploit code using the publicly available exploit codes and encode it so that it may not be recognized by antivirus software (Svensson, 2013).

2.2 MATE versus Insider Threats

MATE attacks essentially take place in a setting where an adversary has physical access to a device in order to compromise it by inspecting or tampering with the hardware device itself or the software it contains (Jakubowski, Falcarin, 2011). From this perspective, insider attacks are a particularly insidious form of MATE attack since the adversary is considered to be a trusted individual within an organization and has authorized access to ensure certain activities (Collberg, Davidson, 2011, Jang-Jaccard and Nepal, 2014). However, MATE attacks are slightly different as they take the concept of deperimeterization (Goyal, 2014, Pieters and van Cleeff, 2009), i.e. it necessarily neither falls within the organizational perimeter nor under the hierarchical control of the organization. Nowadays, big-businesses and enterprises outsource application management and enter into partnerships, subcontract different services running data centers, have their assets managed remotely and have point-of-sale systems supported, owned and maintained by third-party vendors. IT solutions crossway's numerous partners who are engaged in joint product development. The prevalent nature of open-source application software's, proprietary system software's and distributed software systems. MATE attacks, therefore, do not fall under the hierarchical control of an organization, and no one of the organizations in isolation has complete control over the threats they represent (Pieters and van Cleeff, 2009). MATE attacks actually add a new layer of complexity to the existing insider attacks, which is one of the hard problems of information security as declared by the U.S. department of homeland security (Axelrod and CISM, 2008). There are, however, certain common characteristics between insider and MATE attacks, but are not exclusively of the same nature. Moreover, MATE attacks by definition require a certain level of skills and expertise (Collberg, Davidson, 2011, Falcarin, Collberg, 2011, Jakubowski, Falcarin, 2011) in-order to compromise software or hardware under their own control; whereas, a simple human error causing a threat or visiting a malicious website are also considered as insider threat (Greitzer et al. , 2014). MATE attacks are deliberately done and the motive of the attack is always malicious (Falcarin, Collberg, 2011, Gu, Wyseur, 2011). However, in case of insider threats the major part causing damage is unintentional e.g., human error, and the motive of the attack could be intentionally beneficial (without obvious intention to harm) (Bureau, 2013, Greitzer, Strozer, 2014, Valacich et al. , 2013, Warkentin and Willison, 2009, Whitman, 2003). According to (Farahmand and Spafford, 2009), insiders have a better risk perception as compared to MATE since one factor affecting risk perception is actually understanding of the risks themselves, reflected in knowledge and experience with the practices employed by the organization. However, in a MATE scenario, risk perception varies with the situation. Insider attacks tend to be more cautious for the reason that insiders have, in principle, more to lose in terms of their jobs and other benefits (Wall, 2013). However, MATE attacks do not necessarily subject to these kinds of circumstances. Auditing insider attacks is possible as organizations have deployed fine grained access to the logged information. However, due to the prevalent and deperimeterized nature of the MATE attacks, auditing and accountability are complex and research oriented issues (Pieters and van Cleeff, 2009). Access rights revocation and update is normally very straight forward for insiders within a specific organization (Adeyemi et al. , 2013); however, MATE is either not subject to such kind of circumstances or due to the involvement in different working processes of different partners, revocation and update of access rights is too difficult. Traditional insider attacks always use direct paths and detection and prevention rate of suspicious insider attack behavior is high as screening is done typically before hiring, and continuous social interaction makes it possible (Flynn et al. , 2013). MATE attacks, however, use both direct and indirect paths to get access therefore; the reduced and sporadic social interaction makes it difficult to detect their suspicious behavior. Examples of such circumstances include accessing open source software's and third party proprietary software's. Authorization and identity management is comparatively easier as authorizations are granted typically on a need-to-know basis with enforced policies (Maloof and Stephens, 2007), however, digital identification of MATE attackers is complex as authorizations are granted usually on a worst-case, partner basis. Security policies are enforced by the organization and insiders are bound to comply with those policies, while security assurance can easily be done through awareness campaigns, and implementation of other internal controls (Farahmand and Spafford, 2013). However, in a MATE attack scenario, MATE is often abided by a third party security policy that actually provides access to the corresponding digital assets and security governance is mostly assured via legal contracts, reputation, and certifications. According to best security practices, the level of access granted and approved privileges are subject to risk assessment ; however, it may be impractical to perform risk assessment on individual basis (Fenz et al. , 2013) . The concept of MATE attacks originates and mainly lies in the area of SP research. Keeping in view the pervasive nature of different variety of software's and SP primitives against MATE attacks, clearly shows that MATE is entirely a different entity and does not fall necessarily under the broad category of insiders. MATE, however, are a not a sub-set of insiders but rather a discrete set of individuals that falls somewhere between insiders and outsiders, therefore, having some of the mutual characteristics of the two categories.

Table 1 summarizes the results of our analysis. It clearly shows that there are certain in-common characteristics; however, both the attacks are not exclusively of the same nature.

Table 1: MATE VS. Insider threats

Characteristics	MATE Attacks	Insiders Attacks
Organizational controls	MATE attacks are not liable to the direct enforcement of organizational controls. However, in some cases they are subject to the security policies and contracts of a third-party that provide access to the corresponding digital assets. Implementing such controls on MATE attackers in practice, however, faces various challenges.	Insider attacks are always subject to organizational controls as insiders are strictly bound to one of the means of organizational controls, for example, access control, physical controls, separation of duties and other hierarchical controls like supervision and review procedures.
Organizational boundaries	MATE attacks do not necessarily fall under a specific organizational boundary due to the pervasive and distributed nature of software and software systems. These attacks slightly form a potential part of a new concept of deperimeterization.	Insider attacks always fall under the boundaries of a specific organization.
Authorized access	Since IT projects engage various partners in joint product development, therefore, most of the time MATE have full access to the system development. The access granted in some cases over a high-value digital asset is also made in- order to accomplish a contract between different business partners. According to best security practices, for example, ISO 27001-27002, the level of access granted and privileges approved are subject to risk assessment; in contrast, it is increasingly recognized by these security guidelines that it may be impractical to perform the assessment of risk on an individual basis. Subsequently, contracts become elusive, and the required level of detailed information typically not maintained.	Insiders are always subject to direct authorized access under the organizational controls.
Level of expertise	MATE attacks by definition involve a certain level of expertise in order to compromise software or hardware under their control, and that makes MATE different from a simple end-user. Therefore, an attack launched in a MATE scenario by a system administrator is entirely different from the one launched by a lay man.	Insider attacks do not necessarily requisite certain level of expertise. A simple human error causing an attack or simply visiting a malicious site is also considered an insider attack.
Intentionality	MATE attacks are always intentional and are deliberately done.	The cause of insider attacks may be accidental.
Motive	Motive of MATE attacks is always malicious.	The motive of the insider threats could be intentionally beneficial (i.e. without obvious intention to harm).
Risk perception	MATE attacks risk perception varies and are subject to different situations since factors affecting risk consequences is actually based on understanding of the risks themselves, and the in-depth knowledge of the scope of the attack.	Risk perception of the insider attacks is high since one factor affecting risk it is the understanding of the risks themselves, reflected in knowledge and experience with best practices employed by the organization.
Cautiousness	The level of cautiousness is low as compared to insider attacks as MATE is not subject to the direct enforcement of controls of the organization.	Insider attacks are subject to more cautiousness because they have, in principle, more to lose their jobs and other relevant benefits.
Auditing	Due to the prevalent nature of the MATE attacks the information logged, have a tendency to be coarse-grained and the essential auditing may need information logged by other business partners; however, other partners may refuse and keep the information confidential.	Auditing is always possible as the organization alone has the potential access to most of the logged information of all the insiders.
Access rights revocation and update	MATE particularly involves different working processes and due to indirect access rights, the access rights revocation and update problem becomes even more complicated.	The problem of revocation and update of access rights regarding insiders is very easy and straight forward within a specific organization.
Control of access paths	Typically, it may be the case that organization deputies another party to carry-out their services, and that party subcontract another party (third party) without informing the primary organization and this series of legal indirect access makes MATE attacks harder and even more complicated. Obviously, the possibility of indirect access paths increases the risk of asset's misuse. However, there are situations where MATE has a direct and full access; examples include accessing open-source software and other freely available source codes to craft their own one, etc.	Traditional insider attacks mostly use direct paths to access the organizational assets.
Screening and monitoring	The chances of MATE attack suspect behavior detection are limited due to the in-direct enforcement of controls. However, abridged and infrequent social interaction makes it hardly possible.	The chance of monitoring and detection of suspicious insider attack behavior is high as usually screening is before hiring and constant social interaction makes it easily possible.
Authorizations and	Normally the access authorizations are made on worst-case,	The chance of asset's misuse is very limited for the

identity management	partner basis without exclusive identification of the individual. Therefore, the digital identifications of MATE attackers are a bit complex.	reason that access authorizations are typically made on a need-to-know, individual basis and with maximum enforcement of assured duty policies.
Security policies	MATE attackers often use software and hardware that comply with the security policies of a third party to access the organization's assets; hence it is difficult to ensure their compliance with security policies enforced by the organization.	Organizations use corporate-supported hardware and software configured in a standard way, and subject to (automatic) patch management procedures adopted by the organization; therefore, the organization enforces security policies that insiders have to comply with.
Security assurance	In case of MATE, security governance is assured often by means of certifications, reputation, and legal contracts; however, contracts are often under-specified and; therefore, contract violations are hard to define, and hereafter difficult to detect.	In case of insiders, organizations have detailed information about how to ensure security: for example, through awareness campaigns, and enforcement of internal controls, etc.

2.3 MATE Attack Taxonomy

Most of the previous taxonomies do consider security perimeters; however, MATE attacks, mainly against digital assets call for a new concept of deperimeterization (Pieters and van Cleeff, 2009). Furthermore, as organizations become deperimeterized, the situation becomes more complicated.

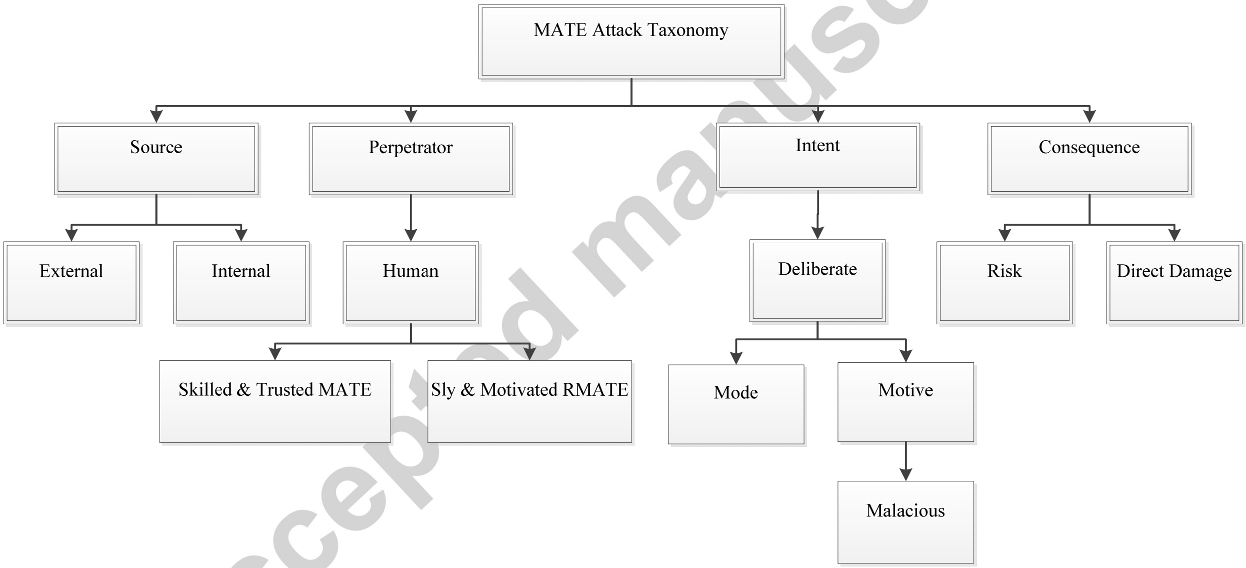


Figure 2: Man-at-the-End Attack Taxonomy

We review briefly different classifications and taxonomies of security threats to figure out the basis for our taxonomy of particular conceptualizations of MATE attacks. Since there are no previous publicly available studies on MATE attacks, therefore, we have been through various information system (IS) security threats and classifications.

In the literature of information system (IS) security, one way of classifying threats are a four-dimension model (Loch et al. , 1992). We use the same four main dimensions on the top level to categorize MATE attacks and these dimensions are the sources, perpetrator, the intent and the consequences. The source mainly comprises of hardware, software or any other high-value digital assets internal or external to the organization in question. It may be any proprietary software or any device placed in or outside a physically secured environment, since MATE primarily involves in compromising either software or hardware under their control. The perpetrator in our taxonomy is MATE, the one who carries out attacks and the primary characteristic of the attacker is that he or she must be a human; therefore, a perpetrator is indicated as human. However, we further categorize the human element into two main classes. This further categorization of human element also acts as MATE attacker taxonomy, which is actually an extraction from the IBM three classes' taxonomy (Svensson, 2013), proposed for the designers of a security system. These classes are: (a) *Skilled and trusted MATE*: They are educated human resource having specialized technical expertise. They have varying degrees of understanding of different parts of the system and know sophisticated tools and mechanisms for different analysis. They have full access to a machine, including arbitrary ability to observe and modify code and data and can debug and patch code, modify data at runtime, hook APIs, read and alter files, change system binaries, etc. (b) *Sly and motivated RMATE*: They are highly intelligent but may have inadequate information of the different parts of the system and are having access to reasonably sophisticated tools. They constantly try to take benefit of exploiting an existing weakness in the system, instead of trying to create their own one. They are capable of assembling groups of experts with complementary and related skills sponsored by great funding agencies and may use first class adversaries as part of the attack team. In this category the attacker is logging in over a network instead of using the machine locally. This class is also known as Remote Man-At-The-End as mentioned earlier. In figure 2, you can clearly see that the third dimension is intentionality. This very element refers to whether MATE behavior is intentional or unintentional (accidental). The intentionality dimension is detailed in (Im and Baskerville, 2005); with further classifications in (Stanton et al. , 2005). As mentioned earlier that all MATE attacks are purely deliberately done, therefore, it is further divided into two sub-dimensions: motive and mode. Mode actually denotes a person's fundamental approach of how to create a threat; however, the motive of a deliberate threat in case of MATE attacks is always malicious (i.e. with obvious intention to harm or damage security); and it might be vandalism, espionage, or fraud. The paper further explores that behavior could also involve either low or high technical expertise and actually denotes to the degree of IS knowledge and skills that an individual would need to accomplish the behavior in question (Magklaras and Furnell, 2005). MATE possesses a certain level of expertise, and it is the main factor behind the mode dimension of the taxonomy. Creating an approach to compromise the entire system security requires technical skills and deeper understanding in comparison to sending spam emails. This very dimension is also interrelated to the roles that workers play in a work setting. The output of MATE attack actually refers to the consequence dimension of the taxonomy. However, this very dimension is further divided into two: risk and direct damage. Subsequently, MATE attack could either pose a threat or cause direct damage to the system. Direct damage can cover many aspects but are not limited to: modification, disclosure, destruction, or denial of service and it may be more noticeable because it is directly observable. On the contrary, risks may not appear; and there is an equal chance of no damage at all, which actually leads to uncertainty in terms of consequence.

The purpose of the MATE attack taxonomy is to draw a complete picture of this particular attack, starting from its creation to its termination, and describe all the major element involve in launching a MATE attack. Further, it help in discussing the major characteristics of the attacker and the two types of MATE attackers, the intent of the attacker, the motivation behind the attack, and the consequences of the attack. The authors view's that the taxonomy gives help in understanding, evaluating, analyzing and modelling MATE attacks.

3 Core Protection Mechanisms against MATE Attacks

Since protection mechanisms against MATE attacks are variously acknowledged as digital asset protection (DAP) or more commonly SP, hence, there is an essential need to elaborate the fundamental concept of digital assets. A digital asset can precisely be everything ranging from a media file e.g., mp3, pdf, jpg, or movie to a password, or a computer program — any of the myriad of digital objects we create, rent, distribute, sell, and buy in the course of our daily modern lives (Collberg, 2011). It does include, broadly, digital content e.g., media, monetary tokens, virtual goods, and decryption keys used for accessing encrypted assets.

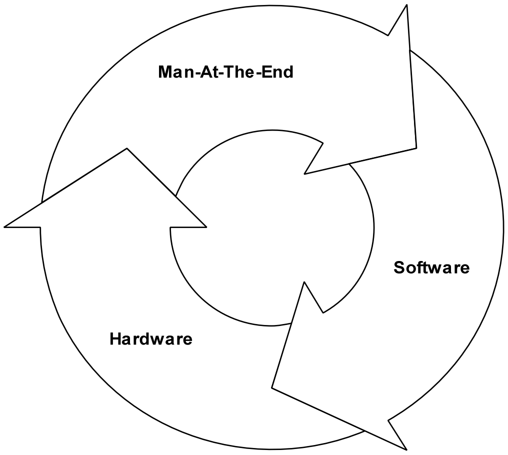


Figure 3: Three fundamental factors involve in properly securing the digital assets

The digital asset protection's mechanisms against MATE attacks are mainly based on either software or hardware- based protection and some of the latest expert's opinion put forward the co-design of hardware and software (Gu, Wyseur, 2011), where ultimately MATE assessment has been addressed indirectly. Obviously, it will improve the gap and make the armory more impressive with more implied focus on technology, but technology alone cannot deliver a complete solution as said earlier. Figure 3 is showing a security chain which primarily comprises of three elements involve in properly securing digital assets, i.e. MATE, software and hardware. MATE directly, however, in the security chain has largely been neglected to make it part of the security strategy alongside the necessary techniques and technologies in DAP Process. The following reasons will address that "why MATE in the security chain has largely been neglected".

1. The former research's focus, which is predominantly based on providing technical solutions to protect against MATE attacks (Collberg, Davidson, 2011, Falcarin, Collberg, 2011, Gu, Wyseur, 2011, Jakubowski, Falcarin, 2011). However, it is increasingly recognized that technology alone is unable to deliver a complete solution (Frangopoulos, Eloff, 2013, Furnell and Clarke, 2012)
2. The complexity of MATE attacks, which are difficult to analyze, model, and evaluate predominantly for three reasons: (a) the attacker is human and therefore, utilizes motivation, creativity, and ingenuity, (b) the attacker has limitless and authorized access of the target, (c) all types of defense stand up to a determined attacker till a certain period of time (Collberg, Davidson, 2011).
3. The wide acknowledgement of the fact that security is a humanoid issue has only started to receive more extensive recognition relatively recently. The role and importance of people as part of the solution is now an established fact (Furnell and Clarke, 2012).
4. The rapid evolution of digital threat landscape, deperimeterization and open environments (Goyal, 2014, Pieters and van Cleeff, 2009), where MATE attackers prey on every line of code, and commercial off-the-shelf systems include a plenitude of known and unpatched software vulnerabilities. Subsequently, no piece of software or digital assets, though, well protected, is likely to survive unscathed in the wild for a long period of time (Broadhurst and Chang, 2013).
5. Human troubles are more now than it used to be and a higher fraction of threats are aggressively targeting end users and it would not be illogical to propose that the user community of security is now effectually everybody (Furnell and Clarke, 2012).

3.1 Software versus Hardware based Software Protection

A MATE adversary can attack both software and hardware. Software protection can be a double-edged sword like many other indispensable technologies, particularly with malware progressively resilient to reverse engineering and eradication (Jakubowski, Falcarin, 2011). SP preferably in different categories of applications must be committed to dynamic development, deployment, maintenance with regular updates across the applications. Moreover, security must be agile and rapidly deployable in order to engage flexible and dynamically renewable SP mechanisms. However, the whole story of SP primitives against MATE attacks, moves around the four basic categories, i.e. code obfuscation, tamper-proofing, watermarking and birth marking with their sub-categories (Falcarin, Collberg, 2011, Gu, Wyseur, 2011, Jakubowski, Falcarin, 2011). Software defenses must achieve two objectives, resist the disabling of protections and resist fallouts that deliver the information or competencies the attacker needs, like their hardware counterparts. Moreover, SP has the drawback of fighting against the learning curve: opponents simply can get direct and limitless access to the implementation, acquire more information during its life cycle, and have a large diversity of tools at their disposal. Furthermore, SP is easier to update (Gu, Wyseur, 2011, Jakubowski, Falcarin, 2011) across different applications. Subsequently, it provides improved safety from diversified, obfuscated, and continuously updated software across their applications. However, a hardware fortification is very expensive for commodity devices but comprehensive enough to provide durable security. Similarly, hardware protection has a much higher learning curve. Keeping in view the prior characteristics of SP, it is by nature dynamic, however, hardware-based fortifications are by definition, static (Collberg, 2011), it means that once a device has been released in the field protected by hardware, and adversaries have destabilized the protection, renewing the protection is not viable until the next product release cycle. The core benefit of hardware-based software protection is that both data and protected code, such as algorithms and keys are not directly observable. Though, the static defenses is perhaps best summed up in the words of General Patton: “Fixed fortifications are a monument to the stupidity of man” (Weir, 2007).

Replacing hardware-supported protections with SP is perhaps a well-known mistake. Since SP is essential to make sure the end-to-end system security if hardware-supported fortifications are used. On the other hand, vulnerabilities found in hardware can have a much more overwhelming consequence and can be very costly and hard to repair. Hardware only protection techniques can be used to enhance the security of software only protection schemes and creating software defenses without a durable hardware foundation is similar building a fortress on sand (Gu, Wyseur, 2011). Skilled adversaries always focus on weak spots and one way to disable or bypass hardware protection is the manipulation of software being hosted. However, despite the implied focus on technology, the integration of a hardware/software co-design is the need of future security. Though, currently both hardware and software based protections are not well integrated and we cannot predict how much it will improve the content security until we try (Falcarin, Collberg, 2011, Gu, Wyseur, 2011).

Table 2: Software based Vs. Hardware based protection schemes.

No.	Characteristics	Software Based protection	Hardware Based protections
1	Nature	Dynamic	Static
2	Maintenance Cost	Low	High
3	Development Cost	Low	High
4	Learning Curve	High	Low
5	Resistible Level	Low	High
6	Access to Implementation	Direct & unlimited	Indirect and limited
7	Exploitable	High	Low
8	Durability	Low	High
9	Renewable	Easy	Demanding
10	Deploy-ability	Easy	Demanding
11	Diversity of Exploitable Tools	High	Low

The core protection mechanisms against MATE attacks are purely technical (SP defenses) or technological (hardware-based defenses) and lacks incorporating the direct human aspects of MATE. However, despite the implied focus on technology, mere technology cannot deliver a complete solution as said earlier. Further, we take the SP research to a whole new realm of challenges and present the human aspects as people represent the significant part of the problem more particularly in MATE attacks.

4 New Trends and Future Directions

Human troubles are more now than it used to be (Furnell and Clarke, 2012), and it has been acknowledged that people represent substantial part of the problem and that security is a humanoid issue. Although current users are more insecure and vulnerable than their counterparts of the past, and it would not be illogical to propose that the user community of security is now effectually everybody. In spite of the implied focus upon technology and technical aspects, attaining security is more than just a technical and technological issue, and progressively necessitates the active involvement and contribution of people to design well-secured, deployed, configured, maintained and updated systems. IT infrastructure spreads across all systems starting from a system administrator down to the owners of simple devices; all need to have their actions and decisions that are having a huge impact on the privacy and security of their device and information. Whilst humans imply a crucial element in attaining security, unfortunately, they are often likely to be the point of failure. The fundamental cause for such discrepancy is that the identification of human aspects requires a deeper understanding and in various ways, a more complex issue to approach within the scope of security and associated threats (Furnell and Clarke, 2012). This section onwards discusses the new trends and future directions, merely taking into account the human aspects, that need to form part of the solution together with the necessary techniques and technologies in DAP process. It will take SP researchers to a whole new realm of challenges, and the authors strongly feels that exploring these issues could provide greater insight into the problem of MATE attacks and could have a high impact on the overall DAP protection process. Fig 4 below depicts future trends and direction of MATE attacks.

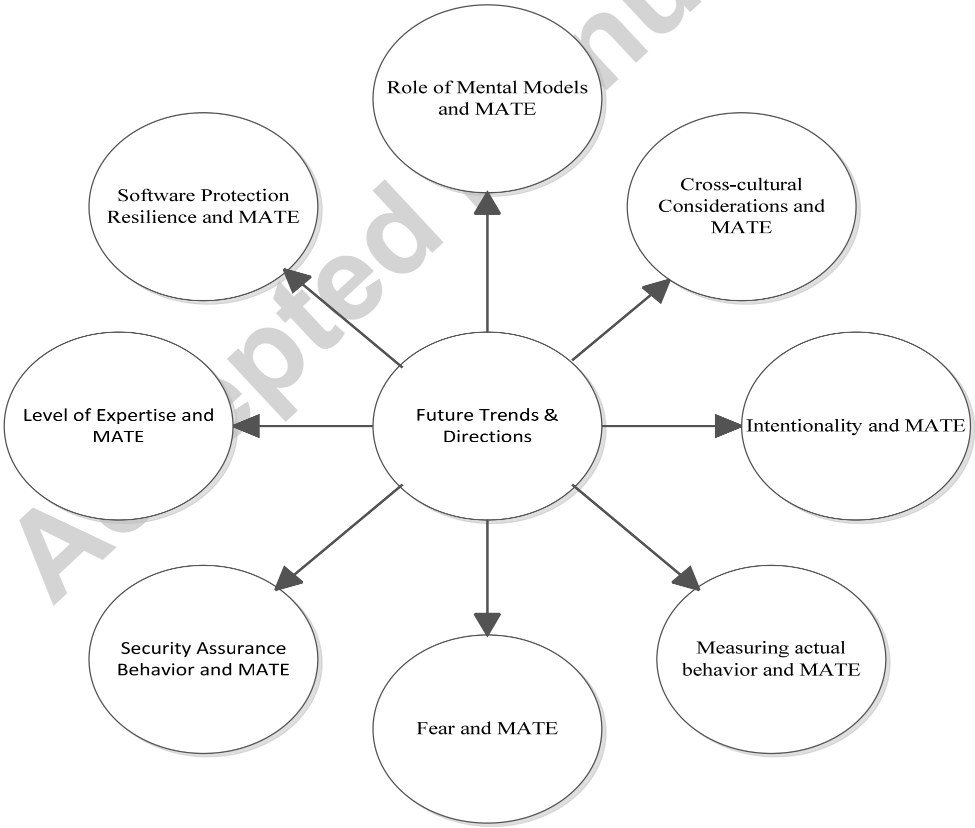

Role of Mental Models and MATE
Software Protection Resilience and MATE
Cross-cultural Considerations and MATE
Level of Expertise and MATE
Future Trends & Directions
Intentionality and MATE
Security Assurance Behavior and MATE
Fear and MATE
Measuring actual behavior and MATE

Figure 4: MATE future trends and directions

4.1 Role of Mental Models and MATE

In the reviewed literature, there is no research that has examined the mental processes that are instrumental to being a MATE. Irrespective of what type of MATE a human is, finding system weaknesses entails logical reasoning and the aptitude to systematically think through possible actions, alternatives, and possible conclusions. Launching a MATE attack is a cognitive activity that involves exceptional technical and reasoning capabilities and this combination of reasoning and systematic thinking implies the use of mental models. A mental model can be thought of as a MATE's internal representation and it helps to describe, explain, and foresee system attributes and behavior. Scottish psychologist Kenneth Craik (Craik, 1967) popularized the concept of mental models when he postulated that the mind creates a 'small-scale model' of realism that allows it to visualize possible actions with various alternatives.

A number of extant studies focus on the technological and sociological aspects of the hackers and their activity (Jordan and Taylor, 1998, Lakhani and Wolf, 2003). To the best of our knowledge, the understanding of individual and social cognition, including the faculties for processing information, applying knowledge, changing preferences, and making decisions, within MATE communities is severely limited. Taking this cognitive psychology approach offers us the opportunity to understand how the MATE mind interprets reality, how they make decisions, and how the thoughts of attackers interact with language. Understanding how MATE attackers think could provide greater insight into understanding the strategies for the future conflicts.

Some of the work done in hacking field on mental model theory provides the understanding of how hackers process information. It was, however, the work of scholars (Corritore and Wiedenbeck, 1991, Dreyfus and Dreyfus, 2005, Gomes and Mendes, 2007, Mayer, 1981, Soloway and Ehrlich, 1984) that applied the concepts of mental model's theory to computer programming and systems analysis (CP&SA). However, the work of (Dreyfus and Dreyfus, 2005) that provided insight into understanding that how expertise is achieved, and by definition MATE attackers are experts. Sociological studies on hackers, scholars (Jordan and Taylor, 1998), (Lakhani and Wolf, 2003), and (Bratus, 2007) suggested that the theories of flow and self-efficacy are instrumental to a hacker. Such theories identify factors such as expertise, curiosity and inquisitiveness, problem solving, systems thinking, self-efficacy, dialectic reasoning, visual comprehension and memory as the major contributing factors that influence the way hackers acquire, maintain and use mental models and are equally important to be applied thoroughly to MATE attackers. Additionally, we believe that a cognitive framework of MATE attackers can provide substantial insights into understanding how to protect digital assets, innovate, and develop the next-generation security tools and technologies. These frameworks will represent the foundational concepts of the MATE attacker's thought processes.

Table 3 shows the models, theories and frame works that are instrumental to MATE alongside their application to other two categories of hackers and computer programming and systems analysis (CP&SA). The theories are composed of sociological theories of flow and self-efficacy with their identified factors, and the mental model theory. The table also shows cognitive frame works and its applicability. However, the table clearly shows that only the expertise dimension of sociological theories of self-efficacy is made applicable to hackers and the application of mental model theory to hacker and CP&SA. Though, none of these studies are applied to MATE.

Table 3: Un-explored areas of MATE in-comparison to hackers and CP&SA in sociological studies and mental modelling

No	Model, Theories and Frame Works		Categories		
			Hacker	MATE	CP&SA
1	Sociological theories of flow and self-efficacy with their identified factors	Expertise	✓	Un-explored	Un-explored
2		Curiosity	Un-explored	Un-explored	Un-explored
3		problem Solving	Un-explored	Un-explored	Un-explored
4		Systems Thinking	Un-explored	Un-explored	Un-explored
5		Self-efficacy	Un-explored	Un-explored	Un-explored
6		Dialectic Reasoning	Un-explored	Un-explored	Un-explored
7		Visual comprehension and memory	Un-explored	Un-explored	Un-explored
8	Mental Model Theory		✓	Un-explored	✓
9	Cognitive Frame Works		Un-explored	Un-explored	Un-explored

4.2 Cross-cultural Considerations and MATE

Cross culture research is mainly considered for the reason of the digital dependencies around the world. The key limitation is that majority of the studies are conducted in western cultures while ignoring the rest of the world. Cross-cultural studies lacks considering the hackers community, security violations, IT security compliance, MATE and so forth. However, Culture has a direct impact on and is predominantly an essential consideration. However, some of its applications in other IT perspectives are shown in (Lowry et al. , 2011, Srite and Karahanna, 2006a, Zhang and Lowry, 2008, Zhang et al. , 2007).

A number of fundamental concepts are reviewed from the literature to illustrate and clarify how these could affect the behavior of MATE. Uncertainty avoidance is an imperative aspect of the cultural studies. It is the degree of threat (subject to uncertain and unknown situations) felled by the members of a specific culture (Zhang and Lowry, 2008). Examples of low uncertainty-avoidance countrywide cultures include Singapore and Denmark whereas Japan is an example of a high-uncertainty avoidance culture. To avoid uncertainty, it is to be expected that an end-user of a high uncertainty avoidance culture is less likely to be victimized for phishing emails while societies exposed to a low uncertainty avoidance culture are more likely to fall prey to a phishing attack. Individualism and Collectivism are another important cultural aspect. Individualism describes the loose connections between the members of a culture; on the other hand, Collectivism describes the unity among individuals, the strong and cohesive groups of the members of a culture based on absolute loyalty (Zhang and Lowry, 2008). For instance, China is a highly collectivistic culture whereas United States (US) is the prominent example of extremely individualistic nationwide culture. Clearly, People living inside such cultures could have either positive or negative impact on MATE behavior.

Another important cultural aspect is Power distance. It is the degree of expectance and acceptance about unequal distribution of power found in fewer influential members of an organization or institution within a country (Zhang and Lowry, 2008). The reason is that a high-power distance culture is more gladly willing to comply with comprehensive policies; whereas, members of a low-power distance culture are often subject to pick-and-choose which policies they feel they should obey. Confucian dynamism is another cultural aspect. It represents the time orientation dynamics that is long-term and short-term orientations of a culture (Zhang and Lowry, 2008). Certainly, it could have dramatic effects on MATE behavior since IT management with a long-term vision would concentrate more on improving the IT security with promising architecture, advanced policies and profound planning in comparison to those with short-term vision or orientation. Cultural Theory of risk is another important theory that help describes the social conflict over risk and would be of greater interest to use this theory for the prediction of MATE risk perception about violations of security (D'Arcy et al. , 2009).

Last but not least, the impact of culture has on MATE would be to measure the identified differences found (D'Arcy and Herath, 2011) in individuals and individuals of a specific area inside each country having great variation in their particular traits (Srite and Karahanna, 2006b). Furthermore, better insight about MATE could be provided by assessing the attributes together with their cultural trait on an individual basis.

The following list summarizes and highlights the main cultural considerations and its application to MATE. List of important cultural considerations:

- Uncertainty avoidance culture
- Power distance culture
- Confucian dynamism
- Individualism and Collectivism
- Cultural Theory of risk
- Individual Cultural attribution
- Individuals of a specific area within a country having great variation in their particular traits

4.3 Software Protection Resilience and MATE

Code obfuscation is a largely adopted solution and is intended to obstruct code understanding. Code understanding, however, cannot be completely impeded. The level of obfuscated code understanding can be measured by the time and cost penalty that the defensive mechanisms impose on the attacker and assessing these penalties is obviously an important problem. Despite largely adopted solution, its assessment has been addressed indirectly either by using internal metrics or taking the point of view of code analysis, e.g., considering the associated computational complexity.

There are no publicly available user studies on code obfuscation that compare different obfuscation techniques and measure how long it takes to understand and change obfuscated code from the point of view of a MATE attacker (Ceccato, Di Penta, 2013). The only study we found so far is (Ceccato, Di Penta, 2013) which studies family of experiments devoted to quantifying and comparing the effectiveness of code obfuscation, as a countermeasure against code tampering. This paper is having many limitations as suggested by the authors. However, future conducted experiments are well-preserved for other types of focus (e.g., professional developers) and when changing the domain and the complexity of the systems/tasks. The question that how long it takes to measure and understand the obfuscated code by MATE will provide greater insight into building robust and durable obfuscation techniques. Secondly, comparing different code obfuscation techniques and finding their time complexity from a human perspective is another major issue. Last, but not least, to assess the combined effect of different obfuscation techniques: this is another topic of interest for future studies.

Future research work will be dedicated to controlled experiment in different contexts like, tamper-proofing (TP), watermarking and birth-marking to analyze how long MATE takes to understand it along with their time complexities while rendering the actual strength of the corresponding technique. Moreover, a good opportunity to explore this very way is the hybrid techniques we often use such as obfuscation and TP (Jakubowski, Falcarin, 2011). Future studies may explore and uncover the combined effect of these techniques as well to provide greater insight and state of the art new extremely resilient techniques against MATE attacks.

Table 4 shows the unexplored areas of SP primitives from direct MATE perspectives. It highlights that the only study conducted so far is carried out in obfuscation while considering direct MATE aspects. This controlled experiment is having limitations and is conducted by the student’s category; however, professionals (MATE having high expertise) in the research has largely been neglected. Though, there is a tangible need to conduct more focused studies to explore the strength of each SP scheme, the combined effect of two techniques in the same main categories like obfuscation and TP etc. Moreover, the hybrid techniques like the integration of obfuscation and TP as discussed earlier in section 3 should also be explored to come up with best techniques and solutions.

Table 4: Un-explored area of software protection resilience against MATE

No	Research Perspectives		*Software Protection Schemes*			
			Code-obfuscation	***Tamper-Proofing***	***Water-Marking***	***Birth-Marking***
1	Research Studies Conducted		✓	Un-explored	Un-explored	Un-explored
2	Controlled Experiments	Programmers/Professionals	Un-explored	Un-explored	Un-explored	Un-explored
		Students	✓	Un-explored	Un-explored	Un-explored
3	Finding Time Complexities		Un-explored	Un-explored	Un-explored	Un-explored
4	Combined Effect		Un-explored	Un-explored	Un-explored	Un-explored
5	Hybrid Techniques		Un-explored	Un-explored	Un-explored	Un-explored

4.4 Level of Expertise in Security-related Behavior and MATE

The expertise level related to behavior have not been considered in the reviewed studies (D'Arcy, Hovav, 2009). Moreover, to measure human capabilities engaged in a behavior is a challenge in many cases. Though, MATE attacker needs a certain level of skills and knowledge, e.g. password cracking involves technical expertise in IS (D'Arcy, Hovav, 2009); and would definitely require more effort which may discourage the individual engaging in that particular behavior. Keeping in view these arguments (D'Arcy and Herath, 2011), computer self-efficacy or IS expertise may be an aspect to describe the behavior related to security. Furthermore, the roles that MATE play in a work setting may be a significant factor as IS specialists are primarily involved in enforcing policies while end-users are simply policy followers. Consequently, the reasons for violation of their own policy they create, may be entirely different from the reasons of violations of simple end-users (Albrechtsen and Hovden, 2009). Role of actors must be taken into account while addressing MATE attacks and hence there is a need for more evaluative studies. Role of actors have some influence on their behavioral decisions and subsequently may impact MATE intentions of engaging in a real behavior.

The analysis here is that some dependent variables must be considered while describing MATE behavior. Examples include IS expertise and MATE role in a setting. Moreover, future studies may consider some undesirable behavior indicated by (D'Arcy and Herath, 2011) and (Guo et al. , 2011). However, synthesizing the divergent conceptualizations of behavior related to security is one of the many challenges in behavioral InfoSec research (Crossler et al. , 2013). We hope that future work on divergent conceptualization frameworks on MATE behavior can provide more about understanding the concept of MATE attacks.

Table 5 highlight MATE related behavior through its two main categories. The different characteristics of MATE-related behavior are shown in order get a clear idea. Future research work may stimulate theory development and research of MATE related behavior while incorporating the characteristics of MATE to provider greater into the MATE attacks problem.

Table 5: MATE related behavior with their different dimensions

Mate-related Behavior	MATE Risk-taking Behavior (MRB)	MATE Damaging Behavior (MDB)
Definition	Behavior that may place digital assets at risk	Behavior that will cause direct damage to digital assets
Example	Password posting; copying confidential data to mobile devices	Sensitive data leakage and theft, financial theft, disclosure, modification, sabotage etc.
Intentionality	Intentional	Intentional
Motive	Malicious	Malicious
Expertise	Low to high	High
Role	MATE	MATE
Task-relatedness	Yes	Yes
Consequence	Risk	Direct damage
Other-characteristics	Perform what one is likely not to do	Perform what one is prohibited from doing

4.5 Security Assurance Behavior (SAB) and MATE

Every type of behavior has significant impact on human and therefore, can be directly applicable to MATE. SAB can be defined as an active behavior by an end-user who has a strong motive to protect IS assets. This type of behavior denotes those intentional behaviors that individuals actively perform in order to protect IS assets in a work setting. SAB is pretty similar to the “beneficial” behavior well-defined by (Stanton, Stam, 2005) and is truly the most desired behavior from IS security management perspective. SAB is also to some extent related to organizational citizenship behavior (OCB) (Organ, 1988) initiated in the field of management. SAB main characteristic is that it implies effortful action and does require comparatively high level of expertise to protect IS assets. SAB is also entirely different from compliant behavior (Vroom and Von Solms, 2004) since SAB is more active and require effortful actions.

Promoting this kind of behavior helps to reduce the number of MATE attacks and provide greater insight in the protection of high-value digital assets. In the current InfoSec literature, very few studies are available on SABs. Future studies should focus more on exploring the OCB and SABs literature and its applications to MATE and subsequently the impact of OCB and SAB on MATE attacks.

Besides, criminological theories to examine MATE damaging behavior and theories from risk may help clarify MATE risk-taking behavior. Future research Studies may concentrate on how to “prevent” and how to “promote” a kind of behavior related to MATE. For doing so, we actually need to know the inhibitors and the enablers of the corresponding behavior. A desirable behavior relies both on the application of the driving forces and the suppression of inhibiting forces. Studies grounded on deterrence theory usually focus on the prevention forces. Enabling factors like neutralization (Siponen and Vance, 2010) and relevant advantage of job performance (Guo, Yuan, 2011) have been investigated but future studies should explore more enabling factors of the corresponding behaviors. Future work should be more focused on evaluating the intrinsic (denotes to perform an activity since it is inherently exciting) motivations toward desirable behavior related to MATE.

4.6 Intentionality and MATE

Compromising the security of a system is impossible without intentional or unintentional actions. The security breach incident caused by intentional actions is also known as deviant behavior while unintentional violations are, often categorized, as misbehavior(Guo, Yuan, 2011, Stanton, Stam, 2005, Willison and Warkentin, 2013).

Most of the existing studies lack the differences between the surveys’ samples caused by intentional violations from those who unintentionally violate the prerequisite policies and procedures. The cause of intentional violations is likely differing from the cause of unintentional violations, although the consequences can be just as harmful. However, mixing these two types of behavior can eloquently limit the efficiency and applicability of a number of recommended remedies in this particular area. Despite the fact that MATE attacks is done intentionally and is highly inspired to damage, disrupt and compromise the application and system security. InfoSec training aiming at creating awareness (Bulgurcu et al. , 2010, D'Arcy, Hovav, 2009, Herath and Rao, 2009a, Straub and Welke, 1998, Straub Jr and Nance, 1990), deterrence (D'Arcy and Herath, 2011) and neutralization (Siponen and

Vance, 2010) may not be applicable and effective for averting the deviant behavior of MATE. Thus, clearly, there is a need to efficiently address the range of behaviors from merely volitional actions (but not malicious) to malicious actions (Willison and Warkentin, 2013).

From this perspective, future research should specify and use more focused studies on MATE and one possible way of screening MATE is using the two major indicators of deviant behavior, i.e. moral beliefs and self-control (Hu et al. , 2012, Kvale and Brinkmann, 2009). The findings of such research studies could provide greater insight into the problem of MATE attacks and may meaningfully advance our understanding of MATE inspirations and psychological developments.

4.7 Fear and MATE

Fear appeals studies together with the potential of fear as a stimulus with various other surrounding issues have just scratched the surface in the field of InfoSec research. However, in the context of InfoSec research, is the degree of fear caused being diagnosed with cancer is similar to the level of fear confronted while compromising the application and system security? Though, the feeling experienced in both the situations may be entirely dissimilar having diverse characteristics, such as its distinctive appearance and intensity found in different persons, its rate of dissipation, its relationship to cope with appraisal, its potential to interact with other factors, and how it is converted into behavior. Fear is a multi-faceted concept that can mark itself to several degrees. Though, this disparate nature of fear underlines the difficulty of doing research in this particular area, but at the same time it gives an opportunity and hope for a meaningful contribution to the common body of knowledge.

Fear is the fundamental driver of (Rogers, 1983) Protection Motivation Theory (PMT) and has recently been studied in the field of behavioral InfoSec domain (Herath and Rao, 2009b, Ifinedo, 2012, Johnston and Warkentin, 2010, Liang and Xue, 2010, Posey et al. , 2011). An exciting research (Vance et al. , 2013, Vance A, 2012) conducted to explore a real-time dynamic fear appeal through in-progress activities and its application in augmenting password security.

How apparently the setting of an artificial laboratory can precisely signify the fear experienced by an individual in a moment of launching an attack against a target? Utilizing different methodologies and diverse approaches in a fear appeals research increase our understanding the impact of fear has on MATE. Another prospect of research would be to examine fear dynamics over time when users react to different events, or when the user is subject to more intense warnings while threat levels are increasing. Fear in relation to MATE will provide greater insight into the problem of MATE attacks.

4.8 Measuring Actual Behavior and MATE

There have been many extant security research articles (shown in Table 6) that measured behavioral intention (positive or negative), but the question remains if behavioral intentions always lead to actual behavior, especially in the security context. Going beyond the "low-hanging fruit" (Straub, 2009) to measure actual secure behavior is the “holy grail” of Information Security (InfoSec) research. For example, how can we study real “black hat” behaviors? Who are our subjects? How can we interview or survey inside abusers, external hackers, MATE and other cyber-criminals? How can we collect relevant quality data to know their intentions and the antecedents of those intentions? These equally important challenges have no parallel in technology acceptance research. Measuring actual behavior is a consistent challenge; however, the following extant research methodologies could provide greater insight and explore this newly growing research area.

Actual behavior can be measured, if accessible to the researcher, through electronic means such as server logs and cameras or by indirect observation such as managerial monitoring of behavior. Qualitative methodologies can offer an efficient way to better comprehend the actual inspirations and behaviors and have just started to scratch the surface in Behavioral InfoSec research. Furthermore, longitudinal studies, and controlled laboratory and field experiment research studies are still rare and need to be addressed to enrich the behavioral InfoSec research area (Crossler, Johnston, 2013). Controlled laboratory and field experiments is one of the promising approaches that is capable to unveil a discrete dissimilarity between individual’s expressed behaviors and their real behaviors (Acquisti and Grossklags, 2004). To the best of our knowledge, none of the reviewed studies has measured the actual intensions and behavior of MATE. The analysis of the table 6 shows that little work has been carried out in measuring the actual behavior in question; however, none of these methodologies applied to MATE. Measuring the actual behavior of MATE can give considerable help and support in designing new techniques and strategies in the field of SP research.

Table 6 shows the existing methodologies used to measure the actual behavior in different fields. The table gives great guidance on how to measure the actual behavior of an individual? However, the table clearly shows that few studies are carried out in the field of information security and MATE has largely been neglected.

Table 6: Extant methodologies used in measuring the actual behavior

1	**Extant methodologies used in measuring the actual behavior**	**Qualitative Methodology**	Positivist Scientific Approach (Eisenhardt and Graebner, 2007, Yin, 2009)	Interpretive Case Studies (Myers and Newman, 2007)	Grounded Theory (Glaser et al. , 1968)	
2		**Longitudinal Methodology**	External factors affecting the actual behavior related to security (Warkentin M, 2006)	longitudinal study on system usage as opposed to intentions (Kim and Malhotra, 2005)		
3		**Controlled Laboratory and Field Experiments Methodology**	Event related potential (ERP) field experiment (Dimoka et al. , 2012)	Functional magnetic resonance imaging (fMRI) Technology (Dimoka, 2010, 2012)	Study on cognitive assessments of security threats and responses (Davis et al. , Warkentin M, 2012)	Field experiment on brain processing of different malware warnings (Anderson B, 2012)
4		**Methodological Use of Information Manipulation Theory (IMT)**	Quality, quantity, clarity and relevance manipulation (McCornack, 1992, McCornack et al. , 1992)	Manipulating messages for Receiver deception (Levine et al. , 2003)		
5		**Spoofing Real Websites Methodology**	Study based on secure behavior discontinuation and continuation (Warkentin M, 2006)			
6		**Video Taped Scenarios and Deception Research Methodology**	Real cases of deception (Jensen et al. , 2010, Jensen et al. , 2011)	Video tapped deceptive approach to detect unreliable insider behavior (Ho SM, 2012)	Understanding InfoSec behaviors such as responding to phishing attacks (Ormond D, 2012, Wright and Marett, 2010)	

5 Conclusion and Future Remarks

A question worth considering is why security system fails when all prescribed measures and controls are in place and active. The paper presents an answer to the question and achieves the objective of the paper by presenting three elements in properly securing digital assets and highlighting the need for directly addressing the MATE (human aspects of security) to form part of the holistic security strategy alongside the necessary techniques and technologies. Moreover, the characteristics and analysis of MATE versus insider threats reveals that people still try to rely on perimeter defenses when the reality is that there are no boundaries. Furthermore, security is becoming a moving target and a story of multiple lines of defense (or "defense in depth") and as the threats evolve so too must the defenses. Besides, people defend the enterprise fundamentally as if it is static, when, in reality, it's dynamic. Individuals continue to imagine that their devices are under their control and secure which is not true. Although the devices and infrastructure we use to consume information have largely changed, the way we protect that information and the users who depend on it has not.

Transforming the concept into a more manageable taxonomy with recognizable dimensions has also a logical appeal in mitigating the consequences of MATE attacks. Despite the implied focus upon technology, the problem of MATE attacks is still there and is difficult to resolve. Obviously, technological advancements and innovations make the armory more and more impressive but mere technology cannot bring a complete solution. Without considering the human factor it might be just an illusion to address MATE attacks. Undoubtedly, human factors play a vital role in the majority of accidents is a troubling feature of contemporary "security know-how". We introduce the human element and come up with novel directions that directly take into account the human aspects. We believe that considering the human challenge; and exploring these future research challenges could have high impact and provide greater insight in properly addressing MATE attacks. This in turn enhances the defense capabilities of high-value digital assets with improved extant techniques and leads to innovate and develop state of the art next-generation security tools and technologies (to properly secure distributed software systems and remarkable volumes of digital content and services relied on many modern systems).

Acknowledgments

This work is fully funded by the Malaysian Ministry of Education under the High Impact Research Grant of University of Malaya. UM.C/625/1/HIR/MOE/FCSIT/03.

References

The What & Why of De-perimeterization. https://collaboration.opengroup.org/jericho/deperim.htm

Acquisti A, Grossklags J. Privacy Attitudes and Privacy Behavior. Economics of Information Security. 2004:165-78.

Adeyemi IR, Razak SA, Zainal A, Azhan NAN. A Digital Forensic Investigation Model for Insider Misuse. Advances in Computational Science, Engineering and Information Technology: Springer; 2013. p. 293-305.

Albrechtsen E, Hovden J. The information security digital divide between information security managers and users. Computers & Security. 2009;28:476-90.

Anderson B HJ, Vance A, Kirwan B, Eargle D, Hinkle LJ,et al. Neural correlates of gender differences in distinguishing malware warnings and legitimate websites: a NeuroIS study. 2012.

Axelrod CW, CISM C. Accounting for value and uncertainty in security metrics. Information Systems Control Journal. 2008;6:25-9.

Bratus S. What hackers learn that the rest of us don't: Notes on hacker curriculum. Security & Privacy, IEEE. 2007;5:72-5.

Broadhurst R, Chang LY. Cybercrime in Asia: Trends and Challenges. Handbook of Asian Criminology: Springer; 2013. p. 49-63.

Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly. 2010;34:523-48.

Bureau FIP. Unintentional Insider Threats: A Foundational Study. 2013.

Ceccato M, Di Penta M, Falcarin P, Ricca F, Torchiano M, Tonella P. A family of experiments to assess the effectiveness and efficiency of source code obfuscation techniques. Empirical Software Engineering. 2013:1-35.

Collberg C. Defending Against Remote Man-At-The-End Attacks. http://www.cs.arizona.edu/projects/focal/security/project1.html

Collberg C. The Case for Dynamic Digital Asset Protection Techniques. Department of Computer Science, University of Arizona. 2011.

Collberg C, Davidson J, Giacobazzi R, Gu YX, Herzberg A, Wang F-Y. Toward digital asset protection. Intelligent Systems, IEEE. 2011;26:8-13.

Corritore CL, Wiedenbeck S. What do novices learn during program comprehension? International Journal of Human ‐ Computer Interaction. 1991;3:199-222.

Craik KJW. The nature of explanation: CUP Archive; 1967.

Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R. Future directions for behavioral information security research. computers & security. 2013;32:90-101.

D'Arcy J, Herath T. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. European Journal of Information Systems. 2011;20:643-58.

D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research. 2009;20:79-98.

Davis F, Riedl R, vom Brocke J, Léger P-M, Randolph A. Gmunden, Austria| June 3-6, 2012| www. NeuroIS. org. Systems Research.22:687-702.

Dimoka A. What does the brain tell us about trust and distrust? Evidence from a functional neuroimaging study. Mis Quarterly. 2010;34:373-96.

Dimoka A. How to conduct a functional magnetic resonance (fMRI) study in social science research. MIS Quarterly. 2012;36:811-40.

Dimoka A, Banker RD, Benbasat I, Davis FD, Dennis AR, Gefen D, et al. On the Use of Neuropyhsiological Tools in IS Research: Developing a Research Agenda for NeuroIS. MIS Quarterly. 2012;36:679-702.

Dreyfus HL, Dreyfus SE. Peripheral Vision Expertise in Real World Contexts. Organization studies. 2005;26:779-92.

Eisenhardt KM, Graebner ME. Theory building from cases: opportunities and challenges. Academy of management journal. 2007;50:25-32.

Falcarin P, Collberg C, Atallah M, Jakubowski M. Guest Editors' Introduction: Software Protection. Software, IEEE. 2011;28:24-7.

Farahmand F, Spafford EH. Insider behavior: an analysis of decision under risk. The 1st International Workshop on Managing Insider Security Threats (MIST 2009)2009. p. 22.

Farahmand F, Spafford EH. Understanding insiders: An analysis of risk-taking behavior. Information Systems Frontiers. 2013;15:5-15.

Fenz S, Neubauer T, Accorsi R, Koslowski T. FORISK: Formalizing information security risk and compliance management. Dependable Systems and Networks Workshop (DSN-W), 2013 43rd Annual IEEE/IFIP Conference on: IEEE; 2013. p. 1-4.

Flynn L, Huth C, Trzeciak R, Buttles P. Best Practices Against Insider Threats in All Nations. 2013.

Frangopoulos ED, Eloff MM, Venter LM. Psychosocial risks: Can their effects on the security of information systems really be ignored? Information Management & Computer Security. 2013;21:53-65.

Furnell S, Clarke N. Power to the people? The evolving recognition of human aspects of security. Computers & Security. 2012;31:983-8.

Glaser BG, Strauss AL, Strutzel E. The discovery of grounded theory; strategies for qualitative research. Nursing Research. 1968;17:364.

Gomes A, Mendes AJ. Learning to program-difficulties and solutions. International Conference on Engineering Education–ICEE2007.

Goyal S. Public vs Private vs Hybrid vs Community-Cloud Computing: A Critical Review. 2014.

Greitzer FL, Strozer J, Cohen S, Bergey J, Cowley J, Moore A, et al. Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation Strategies. System Sciences (HICSS), 2014 47th Hawaii International Conference on: IEEE; 2014. p. 2025-34.

Gu YX, Wyseur B, Preneel B. Software-Based Protection Is Moving to the Mainstream. IEEE software. 2011;28.

Guo KH, Yuan Y, Archer NP, Connelly CE. Understanding nonmalicious security violations in the workplace: A composite behavior model. Journal of Management Information Systems. 2011;28:203-36.

Herath T, Rao HR. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems. 2009a;47:154-65.

Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems. 2009b;18:106-25.

Ho SM MN, Warkentin M. Lie to me: gender deception and detection in computer-mediated communications. 2012.

Hu Q, Dinev T, Hart P, Cooke D. Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*. Decision Sciences. 2012;43:615-60.

Ifinedo P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security. 2012;31:83-95.

Im GP, Baskerville RL. A longitudinal study of information system threat categories: the enduring problem of human error. ACM SIGMIS Database. 2005;36:68-79.

Jakubowski M, Falcarin P, Collberg C, Atallah M. Software Protection. IEEE Software. 2011;28:0024-27.

Jang-Jaccard J, Nepal S. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences. 2014.

Jeng AB, Lee CL. A Study on Online Game Cheating and the Effective Defense. Recent Trends in Applied Artificial Intelligence: Springer; 2013. p. 518-27.

Jensen ML, Lowry PB, Burgoon JK, Nunamaker JF. Technology dominance in complex decision making: The case of aided credibility assessment. Journal of Management Information Systems. 2010;27:175-202.

Jensen ML, Lowry PB, Jenkins JL. Effects of Automated and Participative Decision Support in Computer-Aided Credibility Assessment. Journal of Management Information Systems. 2011;28:201-34.

Johnston AC, Warkentin M. Fear appeals and information security behaviors: an empirical study. MIS quarterly. 2010;34:549-66.

Jordan T, Taylor P. A sociology of hackers. The Sociological Review. 1998;46:757-80.

Kim SS, Malhotra NK. A longitudinal model of continued IS use: An integrative view of four mechanisms underlying postadoption phenomena. Management science. 2005;51:741-55.

Kvale S, Brinkmann S. Interviews: Learning the craft of qualitative research interviewing: Sage Publications, Incorporated; 2009.

Lakhani K, Wolf R. Why hackers do what they do: Understanding motivation and effort in free/open source software projects. 2003.

Levine TR, Asada KJK, Massi Lindsey LL. The relative impact of violation type and lie severity on judgments of message deceitfulness. Communication Research Reports. 2003;20:208-18.

Liang H, Xue Y. Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems. 2010;11:394-413.

Loch KD, Carr HH, Warkentin ME. Threats to information systems: today's reality, yesterday's understanding. MIS Quarterly. 1992:173-86.

Lowry PB, Cao J, Everard A. Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. Journal of Management Information Systems. 2011;27:163-200.

Magklaras G, Furnell S. A preliminary model of end user sophistication for insider threat prediction in IT systems. Computers & Security. 2005;24:371-80.

Maloof MA, Stephens GD. elicit: A system for detecting insiders who violate need-to-know. Recent Advances in Intrusion Detection: Springer; 2007. p. 146-66.

Martinez M, de Andres D, Ruiz J-C, Friginal J. Analysis of results in dependability benchmarking: Can we do better? Measurements and Networking Proceedings (M&N), 2013 IEEE International Workshop on: IEEE; 2013. p. 127-31.

Mayer RE. The psychology of how novices learn computer programming. ACM Computing Surveys (CSUR). 1981;13:121-41.

McCornack SA. Information manipulation theory. Communications Monographs. 1992;59:1-16.

McCornack SA, Levine TR, Solowczuk KA, Torres HI, Campbell DM. When the alteration of information is viewed as deception: An empirical test of information manipulation theory. Communications Monographs. 1992;59:17-29.

Myers MD, Newman M. The qualitative interview in IS research: Examining the craft. Information and organization. 2007;17:2-26.

Organ DW. Organizational citizenship behavior: The good soldier syndrome: Lexington Books/DC Heath and Com; 1988.

Ormond D WM. Message quality and quantity manipulations and their effects on perceived risk. 2012.

Pieters W, van Cleeff A. The precautionary principle in a world of digital dependencies. Computer. 2009;42:50-6.

Posey C, Roberts T, Lowry PB, Courtney J, Bennett B. Motivating the Insider to Protect Organizational Information Assets: Evidence from Protection Motivation Theory and Rival Explanations. The Dewald Roode Workshop in Information Systems Security2011. p. 22-3.

Qin Z, Li Q, Chuah M-C. Defending against unidentifiable attacks in electric power grids. Parallel and Distributed Systems, IEEE Transactions on. 2013;24:1961-71.

Rogers RW. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. Social psychophysiology. 1983:153-76.

Shan Z, Cao H, Lv J, Yan C, Liu A. Enhancing and identifying cloning attacks in online social networks. Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication: ACM; 2013. p. 59.

Siponen M, Vance A. Neutralization: new insights into the problem of employee information systems security policy violations. MIS quarterly. 2010;34:487.

Soloway E, Ehrlich K. Empirical studies of programming knowledge. Software Engineering, IEEE Transactions on. 1984:595-609.

Srite M, Karahanna E. The role of espoused national cultural values in technology acceptance. MIS quarterly. 2006a;30:679-704.

Srite M, Karahanna E. The role of espoused national cultural values in technology acceptance. MIS quarterly. 2006b:679-704.

Stanton JM, Stam KR, Mastrangelo P, Jolton J. Analysis of end user security behaviors. Computers & Security. 2005;24:124-33.

Straub DW. “Black Hat, White Hat Studies in Information Security,”. 2009.

Straub DW, Welke RJ. Coping with systems risk: security planning models for management decision making. Mis Quarterly. 1998:441-69.

Straub Jr DW, Nance WD. Discovering and disciplining computer abuse in organizations: a field study. Mis Quarterly. 1990:45-60.

Svensson G. Auditing the Human Factor as a Part of Setting up an Information Security Management System: KTH; 2013.

Tang M, Qiu Z, Li W, Sun W, Hu X, Zhang H. Power analysis based reverse engineering on the secret round function of block ciphers. Concurrency and Computation: Practice and Experience. 2013.

Valacich JS, Jenkins JL, Nunamaker Jr JF, Hariri S, Howie J. Identifying Insider Threats through Monitoring Mouse Movements in Concealed Information Tests. HICSS-46 Symposium on Credibility Assessment and Information Quality in Government and Business2013.

Vance A, Eargle D, Ouimet K, Straub D. Enhancing Password Security through Interactive Fear Appeals: A Web-based Field Experiment. System Sciences (HICSS), 2013 46th Hawaii International Conference on: IEEE; 2013. p. 2988-97.

Vance A OK, Eargle D. Enhancing password security through interactive fear appeals. 2012.

Vroom C, Von Solms R. Towards information security behavioural compliance. Computers & Security. 2004;23:191-8.

Wall DS. Enemies within: Redefining the insider threat in organizational security policy. Security Journal. 2013;26:107-24.

Warkentin M SJ, Johnston AC. Security software discontinuance. 2006.

Warkentin M WE, Johnston AC, Straub DW. Identifying the neural correlates of protection motivation for secure IT behaviors. 2012.

Warkentin M, Willison R. Behavioral and policy issues in information systems security: the insider threat. European Journal of Information Systems. 2009;18:101.

Weir W. Fifty Military Leaders who Changed the World: Career Press; 2007.

Whitman ME. Enemy at the gate: threats to information security. Communications of the ACM. 2003;46:91-5.

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

Wright RT, Marett K. The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. Journal of Management Information Systems. 2010;27:273-303.

Yin RK. Case study research: Design and methods: Sage; 2009.

Zhang D, Lowry PB. Issues, limitations, and opportunities in cross-cultural research on collaborative software in information systems. Journal of Global Information Management (JGIM). 2008;16:61-84.

Zhang D, Lowry PB, Zhou L, Fu X. The impact of individualism—collectivism, social presence, and group diversity on group decision making under majority influence. Journal of Management Information Systems. 2007;23:53-80.