Inside the Insider Threat

Jason W. Clark, PhD (Mini-Track Chair)

This year we have an exciting minitrack entitled *"Inside the Insider Threat"* planned for you. The minitrack will discuss the topic of insider threats. Insider threats are a present and growing concern to organizations worldwide. Trusted employees have the capability for inflicting devastating consequences by both intentional/malicious and unintentional/accidental means to their employer's critical assets to include people, data, facilities, and technologies, primarily because of their detailed knowledge and authorized access to these systems. Given the complexity of the insider threat problem any approach to mitigating this problem therefore must have both a behavioral and a technical component. As previously stated, insider incidents may be accidental or arise from conflicting policies that confuse the putative attacker. These unintentional insider attacks are as dangerous as deliberate insider attacks but must be handled differently due to the lack of maliciousness. Understanding how to cope with unintentional insider attacks effectively is also a complex, difficult problem.

Analyzing and detecting insider threats involve both technical and non-technical approaches across many different disciplines, including human-oriented ones.

This minitrack selected three papers emphasizing this cross-cutting work.

The first paper is:

Psychological Profiling of Hacking Potential

This paper investigates the psychological traits of individuals' attraction to engaging in hacking behaviors (both ethical and illegal/unethical) upon entering the workforce. We examine the role of the Dark Triad, Opposition to Authority and Thrill-Seeking traits as regards the propensity of an individual to be interested in White Hat, Black Hat, and Grey Hat hacking. A new set of scales were developed to assist in the delineation of the three hat categories. We also developed a scale to measure each subject's perception of the probability of being apprehended for violating privacy laws. Engaging in criminal activity involves a choice where there are consequences and opportunities, and individuals perceive them differently, but they can be deterred if there is a likelihood of punishment, and the punishment is severe. The results suggest that individuals that are White Hat, Grey Hat and Black Hat hackers score high on the Machiavellian and Psychopathy scales. We also found evidence that Grey Hatters oppose authority, Black Hatters score high on the thrill-seeking dimension and White Hatters, the good guys, tend to be Narcissists. Thrill-seeking was moderately important for White Hat hacking and Black hat hacking. Opposition to Authority was important for Grey Hat hacking. Narcissism was not statistically significant in any of the models. The probability of being apprehended had a negative effect on Grey Hat and Black Hat hacking.

The second paper is:

Experimental Investigation of Demographic Factors Related to Phishing Susceptibility

This paper reports on a simulated phishing experiment targeting 6,938 faculty and staff at George Mason University. The study examined various possible predictors of phishing susceptibility. The focus of the present paper is on demographic factors (including age, gender and position/employment). Since previous studies of age and gender have yielded

URI: https://hdl.handle.net/10125/64013
978-0-9981331-3-3

discrepant results, one purpose of the study was to disambiguate these findings. A second purpose was to compare different types of email phishing exploits. A third objective was to compare the effect of different types of feedback given to those who clicked on one or more of three simulated phishing exploits that were deployed over a three-week period. Our analysis of demographic factors, effects of phishing email content, and effects of repeated exposure to phishing exploits revealed significant age effects, marginally significant gender differences, and significant differences in email type. A multi-level model estimated effects of multiple variables simultaneously.

The third paper is:

Data Value Analysis for Predicting Insider Threat Risk using a Bayesian Inference Network

Data has high value when it makes a large difference in the estimation of insider threat risk. However, there is limited research on approaches to measure the value of data applied to a Bayesian inference network used to predict insider threats. This paper proposes a methodology, the Node Importance Test (NIT), to represent the impact of a given node on the determination of an individual's riskiness. Experiments illustrate how nodes influenced by various data sources have different ranges of impact on insider threat risk prediction. On average, nodes influenced by user activity monitoring (UAM)-file, and -device data impact risk scores the most. Nodes influenced by employment, medical, and legal data impact risk scores the least. In conclusion, the results show that UAM-file data as a whole are more "valuable" than UAM-login/logout data. These conclusions could reasonably be used as grounds to prioritize acquisition of one type of data over another.