HICSS-54 Cyber Deception and Cyber Psychology for Defense CFP

Hawaiian International Conference on System Sciences (HICSS)

January 5-8, 2021 in Kauai, Hawaii

Submission Deadline: June 15, 2020

Cyber Deception and Cyber Psychology for Defense Minitrack

Track: Digital Government

Description

Creating a system that is always protected and secure in all situations against all attackers is a far-reaching and likely impossible goal. It is important for researchers to continue to move systems closer to guarantees of security, but it is also essential to create techniques to adaptively defend against an attacker who circumvents the current security or has insider knowledge of system properties or security practices. Deception for cyber defense works towards that goal—to rebalance the asymmetric nature of computer defense by increasing attacker workload and risk while decreasing that of the defender.

Cyber deception is one defensive technique that considers the human component of a cyber attack. Deception holds promise as a successful tactic for making an attacker's job harder because it does more than just block access: it can also cause the attacker to waste both time and effort. Moreover, deception can be used by a defender to impart an incorrect belief in the attacker, the effects of which can go beyond any static defense. Understanding the human cognition and behavior of both the cyber defender and cyber attacker is a critical component of cybersecurity. Cyber psychology research advances the science of human behavior and decision making in cyberspace to understand, anticipate, and influence attacker behavior. It also seeks to ensure scientific rigor and quantify the effectiveness of our defensive methods.

In the cyber world, an attacker only knows what is perceived through observation of the target network. The intruder is often thousands of miles

away from the network to which he or she is attempting to gain entry. Unfortunately, modern networks and systems often unintentionally provide more information to an attacker than defenders would like. However, the network owner also has the opportunity to reveal information he or she desires the attacker to know—including deceptive information. Because network information is often complex and incomplete, it provides a natural environment in which to embed deception since, in chaos, there is opportunity. Deception can alter the mindset, confidence, and decision-making process of an attacker, which can have more significant effects than traditional defenses. Furthermore, using deception for defensive purposes gives the defender at least partial control of what an attacker knows, which can provide opportunities for strategic interaction with an attacker.

Authorized users of systems and networks, or masqueraders of these users, may act as attackers. These insiders can leak sensitive information deliberately or accidentally. Detecting and thwarting these attacks is more difficult than dealing with external attackers because the users are often authorized to access the information they leak, or the systems and networks the data is on. As a defensive technique, deception in this context must take into account the psychology of the attacker and the organizational, political, and societal environments in which the attack occurs.

These research efforts require an interdisciplinary approach and the mini-track is soliciting papers across multiple disciplines. It is essential to understand attacker and defender cognition and behavior to effectively and strategically induce cognitive biases and increase cognitive load, making our systems more difficult to attack.

Topics of interest include (but are not limited to):

- Science of Deception (e.g., evaluation techniques, deception frameworks applied to cyber);
- Practice of Cyber Deception (e.g., case studies, deception technology, deception detection);
- Understanding/influencing the cyber adversary (e.g., adversary emulation, measures of effectiveness);
- Psychological and social-cultural adversarial mental models that can be used to estimate and predict adversarial mental states and decision processes;

- Cognitive Modeling of cyber tasks;
- Adversary observation/learning schemes through both active multi-level “honey bait” systems and passive watching, in conjunction with active learning and reasoning to deal with partial information and uncertainties;
- Oppositional Human Factors to induce cognitive biases and increase cognitive load for cyber attackers;
- Metrics for quantifying deception effectiveness in driving adversary mental state and in determining optimized deception information composition and projection;
- Experimental Design, approaches, and results;
- Theoretical formulation for a one-shot or multiple rounds of attacker/defender interaction models;
- Identification of social/cultural factors in mental state estimation and decision manipulation process;
- Cyber maneuver and adaptive defenses;
- Cyber defense teaming;
- Protecting our autonomous systems from being deceived;
- Policy hurdles, solutions, and case studies in adoption of cyber deception technologies;
- Predicting, understanding and protecting against insider threats;
- Analyzing the effects of insider attacks;
- Human factors and the insider threat problem;
- Examining the causes of an insider threat from a behavioral science perspective;
- Measuring the effectiveness of mitigation technologies and methodologies.

Digital (Electronic) Government Track

Electronic Government, or more recently Smart Government, is a multidisciplinary research domain, which studies the use of information and technology in the context of public policy making (smart governance, open government, and digital divides), smart government operations (transformation, management, organization, infrastructure, interoperability, emergency management, safety, and security), citizen engagement and interaction (e-participation, transparency, collaboration, and digital democracy), and government services (including using social media).

Numerous disciplines contribute to this intersection of research such as computer science, information systems, information science, political science, organizational sciences (public administration and business administration), sociology, and psychology among others.

The HICSS e-Government track has been a hotbed for groundbreaking studies and new ideas in this particular research domain. Many studies first presented here were developed further and then turned into publications at top journals. Thirteen minitracks cover the full spectrum of research avenues of electronic government including minitracks dedicated to emerging topics, open government, and social media, or most recently, government and disaster resiliency and supply chain security.

The HICSS e-Government Track has assumed an excellent reputation among e-Government scholars. In a recent study it has been ranked the academically most rigorous and most valuable research conference on e-Government in the world. The E-Government Track has the lowest acceptance rate of all HICSS tracks and the highest average per-session attendance. Having a paper accepted at the e-Gov Track at HICSS means something. Furthermore, HICSS is in the top 2 percent of all IEEE conferences with regards to proceedings hits and paper downloads.

For details and author instructions see: https://hicss.hawaii.edu/authors/

About HICSS

The Hawaii International Conference on System Sciences (HICSS) has been known worldwide as the longest-standing working scientific conferences in Information Technology Management. Since 1968, HICSS has provided a highly interactive working environment for top scholars from academia and the industry from over 60 countries to exchange ideas in various areas of information, computer, and system sciences. HICSS ranks second in citation ranking among 18 Information Systems (IS) conferences [1], third in value to the MIS field among 13 Management Information Systems (MIS) conferences [2], and second in conference rating among 11 IS conferences [3].