Introduction to the HICSS-53 Minitrack on Cyber Deception for Defense

Kimberly Ferguson-Walter
Laboratory for Advanced Cybersecurity Research
Kimberly.ferguson-wa@navy.mil

Sunny Fugate
Naval Information Warfare Center, Pacific
fugate@spawar.navy.mil

Cliff Wang
Army Research Office
xiaogang.wang.civ@mail.mil

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 towards absolute security, but it is also essential to create techniques so a system can adaptively defend against an attacker who circumvents the current security. Deception for cyber defense approaches this goal—to rebalance the asymmetric nature of computer defense by increasing attacker workload while decreasing that of the defender.

Cyber deception is a collection of defensive techniques that considers the human component of cyber attacks. 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 cognition and behavior of both the cyber defender and cyber attacker is a critical component of cybersecurity.

In the cyber world, an attacker often only knows what is perceived through observation of the target network. The intruder may be thousands of miles away from the network to which he or she is attempting to gain entry. Networks 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 imbed deception since, in chaos, there is opportunity. Deception can alter the mindset, confidence, and decision-making process of an attacker, which can be more effective than traditional defenses. Furthermore, using deception for defensive purposes gives the defender at least partial control of what an attacker will know, and provides opportunities for strategic interaction with an attacker.

These research efforts require an interdisciplinary approach which is exemplified in the accepted papers which cross multiple disciplines. It is essential to understand attacker and defender cognition and behavior to effectively and strategically use cyber deception to induce cognitive biases and increase cognitive load, making our systems difficult to attack. This minitrack provides a venue for innovative research that rigorously examines advancements in cyber deception technologies, evaluations, case studies and models of cyber deception effects, as well as improved understanding of the cognition and behaviors of cyber operators. This year the minitrack features the following eleven papers and is closely linked to the HICSS-53 symposium entitled "Cyber Psychology Aids National Security":

- "Design of Dynamic and Personalized Deception: A Research Framework and New Insights" (by Cleotilde Gonzalez, Palvi Aggarwal, Christian Lebiere, Edward Cranford)
- "Delivering Honeypots as a Service" (by Jafar Haadi Jafarian, Amirreza Niakanlahiji)
- "Creating Convincing Industrial-Control-System Honeypots" (by Neil Rowe, Thuy Nguyen, Marian Kendrick, Zaky Rucker, Dahae Hyun, Justin Brown)
- "Invasion of the Botnet Snatchers: A Case Study in Applied Malware Cyberdeception" (by Jared Chandler, Kathleen Fisher, Erin Chapman, Eric Davis, Adam Wick)

URI: https://hdl.handle.net/10125/63964
978-0-9981331-3-3

- “Towards a Holistic Model of Deception: Subject Matter Expert Validation” (by Iaian Reid, Rob Black)
- “The Moonraker Study: An Experimental Evaluation of Host-Based Deception” (by Temmie Shade, Andrew Rogers, Kimberly Ferguson-Walter, Sara Beth Elsen, Daniel Fayette, Kristin Heckman)
- “Adaptive Cyber Deception: Cognitively Informed Signaling for Cyber Defense” (by Edward Cranford, Cleotilde Gonzalez, Palvi Aggarwal, Sarah Cooney, Milind Tambe, Christian Lebiere)
- “HoneyBug: Personalized Cyber Deception for Web Applications” (by Amirreza Niakanlahiji, Jafar Haadi Jafarian, Bei-Tseng Chu, Ehab Al-Shaer)
- “A Deception Planning Framework for Cyber Defense” (by Jafar Haadi Jafarian, Amirreza Niakanlahiji)
- “Concealing Cyber-Decoys using Two-Sided Feature Deception Games” (by Mohammad Sujan Miah, Marcus Gutierrez, Oscar Veliz, Omkar Thakoor, Christopher Kiekintveld)
- “Automating Cyberdeception Evaluation with Deep Learning” (by Gbadebo Ayoade, Frederico Araujo, Khaled Al-naami, Ahmad Mustafa, Yang Gao, Kevin Hamlen, Latifur Khan)