Cyber Security: Understanding the Role of Deception as a Strategy in Cyber Attack Detection

Motivation: Cyber attacks, i.e., the disruption of normal functioning of computers and loss of private information through malicious network events, are becoming widespread. Current game-theoretic approaches, which study the interaction between attackers and defenders, have lesser studied the role of deception as a strategy to counter cyber attacks. Deception refers to falsely implicating attackers in honeypots in order to defend and capture network threats more accurately and timely (Figure 1).
Objective: This research program aims to account for cognitive limitations on memory and recall for attackers and defenders and explore experiential decisions made by attackers and defenders in cyber-security games that involve deception.
Methodology: An important aspect of the project involves development of cyber-security games that enable us to manipulate deception as a strategy to counter cyber attacks. In such games, actions of attacker and defender will be associated with payoffs and the goal of each player is to maximize her payoff. Next, the project will focus on the development of computational cognitive models of attackers and defenders. The model predictions will be tested by collecting human data in cyber-security games and comparing the model predictions to human decisions.
Implications: Such an investigation will help improve current technical solutions and provide better decision support to defenders in countering cyber attacks via deception.

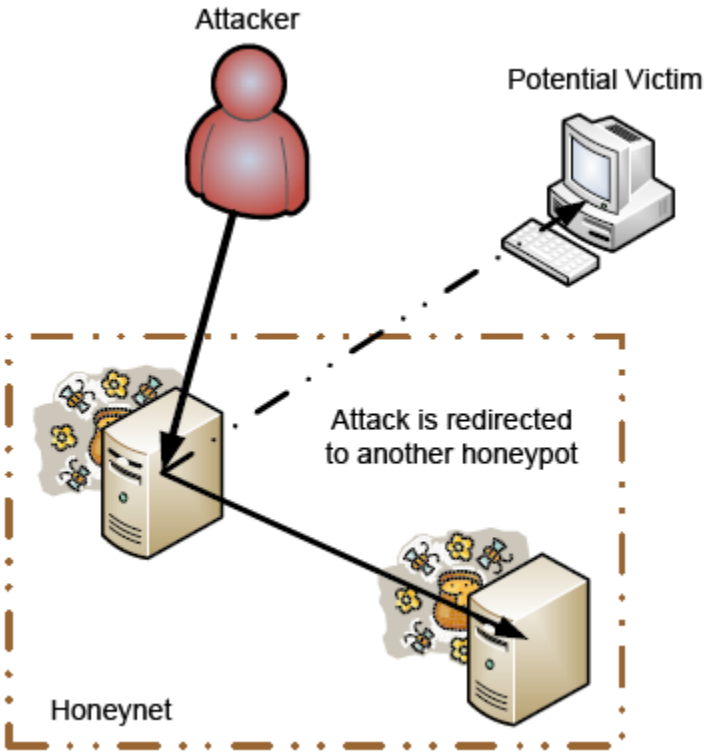

Figure 1. Using Deception to lure an attacker into a honeypot and evade a potential victim