DARTMOUTH

Institute for Security Technology and Society
at Dartmouth

Cyber Deception Research

Cyber deception methods such as honeypots are crucial in today's environment of network security. Malicious attackers are often highly persistent and may have a wide variety of objectives in their attacks. In many instances, the attacker can obtain information and carry out certain attacks before the defender even notices. Therefore, the ability to deceive and impose additional costs on an attacker is extremely useful for administrators defending a network. Dartmouth has contributed several research projects to cyber deception methods and implementations.

Probabilistic Logic of Cyber Deception

When planning an attack on a network, malicious attackers often obtain a variety of information about the network in order to best accomplish their objective. To impose uncertainty and further costs on an attacker, this project proposes returning a consistent mix of true and false results from a network scan based on a probabilistic logic theory, which can exponentially increase the difficulty in crafting an attack.

The Stackelberg Honey-based Adversarial Reasoning Engine performs very well, even when the adversary deviates from the initial assumptions made about his or her behavior.

This project develops a formal Probabilistic Logic of Deception which captures an adversary's knowledge of a system. It defines attacker behavior as searching for nodes with the highest utility to compromise, and the objective of the defender as keeping the attacker away from the most valuable nodes in the network. Other metrics for quantifying damage for a probabilistic state are also defined.

From this concept, two algorithms were developed: a slow Naive-PLD and a heuristic Fast-PLD. Both algorithms were evaluated using a 600 node network based on expected damage and execution time. For nearly all rounds of testing, while Naive-PLD's execution times were impractical for real contexts, Fast-PLD reduced the expected damage of the attacker's steps while reasonable execution times. From these results, it is clear Fast-PLD can be deployed in a real world context to reduce the damage an attacker may have.

SHARE

Noisy-Rich (NR) attackers are attackers who keep exploiting vulnerabilities until they compromise a network, posing the largest risk compared to stealthy or random attackers as they do not count on a single attack succeeding but continue to attack a target network again and again until they succeed.

SHARE (Stackelberg Honey-Based Adversarial Reasoning Engine) is an adversarial foundation based on Stackelberg games that models how NR-attackers attack an enterprise network and how a defender can induce deception by placing honey nodes and apparent vulnerabilities to minimize the impact of the attack. SHARE defines the attacker as having two actions of scanning or exploiting a vulnerability, while the defender can add a System Vulnerability Dependency Graph (SVDG) and/or enterprise or remove a SVDG and/or enterprise. The addition actions are used to add honey nodes and vulnerabilities, while the remove action removes vulnerabilities from an SVDG (through patching or deactivating software).

After attacker and defender strategies are outlined, the defender needs to choose whether to stop the attack upon detection or after a delay. The former was found to cause more damage in the long run as the attacker learns the defender's strategy, while the latter offers better long term defense against intelligent adversaries as they could not precisely learn where the honey vulnerabilities are.

SHARE was tested using vulnerability data from NIST and 5 different types of networks (Small, Medium, Large, Synthetic Medium, Synthetic Large). Results showed that, though computing the defender's strategy is expensive, the defender's strategy, along with stopping after a delay, works well in practice.

Pareto-Optimal Adversarial Defense of Enterprise Systems

Enterprise security managers today are often faced with the challenge of scheduling patching of a large array of software, which often takes up much time and effort. While most security managers patch vulnerabilities that pose the highest threat, this allows attackers to then try and penetrate the system using vulnerabilities not rated as having a high impact. This project seeks to find out what strategy an attacker might take to maximize damage, and what optimal strategy a defender can take to minimize expected damage. The optimal strategy of the defender is thus defined as a Pareto optimization problem.

The defender's strategy is represented as deciding which software to run and what patches to apply to them. Any given defender strategy has an impact on productivity and cost, which are factored into the optimization problem.

The attacker's strategy is defined as a set of vulnerabilities that they will use to penetrate the network. The attacker, as they do not have access to the enterprise's Vulnerability Dependency Graph (VDG), which is a more general version of attack graphs, must uncover vulnerabilities to use in their strategy.

After finding the best attacker strategy using an Integer Linear Program, the Pareto analysis is conducted for the defender. The best defender strategy is formulated as a bi-objective optimization problem of minimizing the impact of the attacker and maximizing total productivity. After computing the Pareto frontier, a compromise can be chosen between impact and productivity, which leads to an Optimal Defender Strategy for a Pareto point on the frontier.

After testing on 4 VDGs, the Pareto optimization algorithms proved to offer solutions that effectively balanced an attacker's impact and productivity in a reasonable execution time.

Hybrid Adversarial Defense

While much research has been done in honeypot placement in a network, most of that research has two drawbacks: they assume that honeypots are the only form of defense and they do not model the attacker's behavior. This project seeks to develop a hybrid adversarial defense of an enterprise network that optimally places both traditional defenses and honeypots while considering an attacker model.

Like SHARE, this project uses a Stackelberg game to model the interaction between the attacker and defender. The attacker's beliefs about the network are represented by a novel Attacker Belief Evolution Tree (ABET), while the defender's reasoning about an attacker's behavior is defined by a Defender ABET (DABET). From this, two algorithms were created to find an optimal defense strategy. H_Exact finds the correct optimal solution but is inefficient, and H_Greedy finds a suboptimal solution efficiently.

After evaluation of the algorithms using 5 different types of networks, H_Greedy was found to produce very high quality solutions (93% to 98% optimal) in the vast majority of cases while maintaining fast processing times. These results indicate that this hybrid adversarial defense system provides an efficient and practical method of finding an optimal defense strategy for an enterprise network.

Additional Information

References

1. Sushil Jajodia, Noseong Park, Fabio Pierazzi, Andrea Pugliese, Edoardo Serra, Gerardo I. Simari, and V. S. Subrahmanian. "A Probabilistic Logic of Cyber Deception." *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2532-2544, Nov. 2017.
2. Sushil Jajodia, Noseong Park, Edoardo Serra, and V. S. Subrahmanian. "SHARE: A Stackelberg Honey-Based Adversarial Reasoning Engine." *ACM Transactions on Internet Technology (TOIT)*, vol. 18, no. 30, May 2017.
3. Edoardo Serra, Sushil Jajodia, Andrea Pugliese, Antonino Rullo, and V. S. Subrahmanian. "Pareto-Optimal Adversarial Defense of Enterprise Systems." *ACM Transactions on Information and System Security (TISSEC),* vol. 17, no. 11, March 2015.
4. Tanmoy Chakraborty, Sushil Jajodia, Noseong Park, Andrea Pugliese, Edoardo Serra and V. S. Subrahmanian. "Hybrid adversarial defense: Merging honeypots and traditional security methods." *Journal of Computer Security* 26 (2018): 615-645.

Video

https://www.cs.dartmouth.edu/~dsail/projects/decepti on /videos/

Presentation

https://www.cs.dartmouth.edu/~dsail/projects/ deception/slides/

PARTICIPANTS

Lead: V.S. Subrahmanian

Tanmoy Chakraborty, Sushil Jajodia, Noseong Park, Fabio Pierazzi, Andrea Pugliese, Antonino Rullo, Edoardo Serra, Gerardo I. Simari.

DARTMOUTH
Security and Artificial Intelligence Laboratory