Carnegie Mellon University

Is Cyber Deception Worth It?

MARCH 9, 2021

Austin Whisnant

Deception

- Providing false or misleading information to influence a rational enemy's strategic calculus

- Deception has played an important role in warfare for 1,000s of years
    - Useful for gaining an upper hand from a position of disadvantage

- In the cyber domain, deception is a critical component of offensive tactics, but how useful is it for defense?

- Some defensive deception tools are used in practice, but it's not clear to what extent and whether they are worth it

Background

- Plenty of research on whether defensive deception tools ”work” – i.e. whether they deceive attackers
- Research on how to use and prioritize deception techniques as part of a larger strategy is lacking
- Defenders already have a lot on their plates, and limited time and budget to implement defensive strategy

TODO Example

- High-level how attacks work…
- Comparison between defended and deceptive network…

The Theory

- Deception tactics are not worth the investment in time, money, and expertise, especially when compared to other defensive techniques.
- Counter-attack from the defensive position is usually not an option; therefore the cost of deception to the attacker is minimal
  - → the attacker’s strategic calculus will not change
  - Most attackers will continue the attack until they succeed

Research Questions

Is the benefit of using cyber deception greater than the cost?

Is the overall benefit of cyber deception greater than the overall benefit of other cyber defense techniques?

Are the answers to the above consistent across all types of defender/attacker combinations?

(Preliminary) Metrics

Defense

Initial cost of tool(s)

Time spent implementing + maintaining defensive tools

Time to detection of adversary

Intelligence collected/used on adversary tactics, techniques, and procedures (TTPs)

Offense

Attack success rate

Total time to succeed

Attack abandonment rate

Study Design

Game-theoretical Analysis

- Cost-benefit analysis
- Model building and implementation

Simulation

- Test case simulation
- Monte-carlo simulation
- Machine learning application for “solution”

Mixed Methods Validation

- Survey of defensive experts
- Human subjects experiments

Plan

Data Collection

Online survey targeting defensive practitioners, distributed via LinkedIn and Twitter

Experiment conducted using existing online training platform. Careful design and execution based on lessons learned from (minimal) existing literature and expertise

Data Analysis

Requires IRB

Mainly quantitative – looking for cost estimates, deployment sizes, durations, etc.

Human cognition and behavior is out of scope

Preliminary Related Work

- Palvi Aggarwal, Cleotilde Gonzalez, and Varun Dutt. “HackIt: A Real-Time Simulation Tool for Studying Real-World Cyberattacks in the Laboratory”. In: Handbook of Computer Networks and Cyber Security: Principles and Paradigms. Ed. by Brij B. Gupta et al. Cham: Springer International Publishing, 2020, pp. 949–959
- Cristiano De Faveri and A. Moreira. “A SPL Framework for Adaptive Deception-based Defense”. In: HICSS. 2018
- Kimberly Ferguson-Walter et al. “Game Theory for Adaptive Defensive Cyber Deception”. In: Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security. HotSoS ’19. Association for Computing Machinery, 2019.
- Kimberly Ferguson-Walter et al. “The Tularosa Study: An Experimental Design and Implementation to Quantify the Effectiveness of Cyber Deception”. In: 52nd Hawaii International Conference on System Sciences, 2019
- Robert S. Gutzwiller, Kimberly J. Ferguson-Walter, and Sunny J. Fugate. “Are Cyber Attackers Thinking Fast and Slow? Exploratory Analysis Reveals Evidence of Decision-Making Biases in Red Teamers”. In: Human Factors and Ergonomics Society 2019
- Aaron Schlenker et al. “Deceiving Cyber Adversaries: A Game Theoretic Approach”. In: Proceedings of the 17th International Conference on Autonomous Agents and Multi Agent Systems. AAMAS ’18. Stockholm, Sweden: International Foundation for Autonomous Agents and Multiagent Systems, 2018