Defense By Deception

Mark Grechanik

University of Illinois,Chicago

Susan McGregor

Columbia University

Deception

The process by which agents choose actions to manipulate beliefs of the other agents so as to take advantage of their erroneous inferences.

We study attackers and victims as agents whose interacting choices produce outcomes with respect to their preferences.

Deception in Cybersecurity

- Attackers use deception as a tool to penetrate defenses, e.g., to gain passwords from victims using phishing emails.
- Each agent in the cybersecurity game acts based on its belief state, which consists of a logically closed set of sentences.
- Turning deception into a weapon against attackers has been something of a Holy Grail in the field of cybersecurity.

Goals of DbD


DbD
Change the beliefs of the attacking agents to divert resources
No production instrumentation and monitoring

Core Ideas of DbD

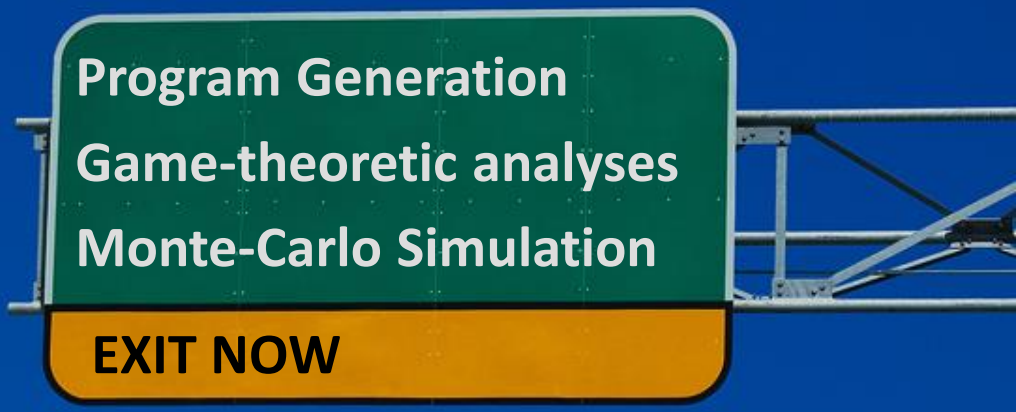
Create an automated approach to distort the belief of the malicious agents about the system they attack;

Define the sequence of steps that will lead to detection of the malicious agent before this agent can cause any harm;

Force the agent to perform actions based on the distorted beliefs – adjust the level of deception based on the actions of the attacking agent.

Automating DbD

It is a decades old problem that has not been solved. Existing approaches cannot address this problem. **It is a huge problem with no solution**.



Key Points

- Bespoke DbD (Defense by Deception) efforts usually:
  - Hide actual functionality/approach of the system
  - Create false beliefs for attackers
  - Trick attackers into quickly revealing themselves and/or abandoning the attack
- How can we automate the design of DbD tools that work on generic systems
  - Systems that automate distortion of the perceived reality of the system with respect to attackers
  - Possibly reduced performance

Solution Steps

- Model system, resources and possible types of attacks
- Synthesize DbD strategies to the resources and assign defense costs
- Generate game theoretic moel and simulate the DbD to simulate what type of defense is most successful
- *Short-term target:* Mobile apps
- *Long-term target:* Automate design of tools for securing commercial software/applications

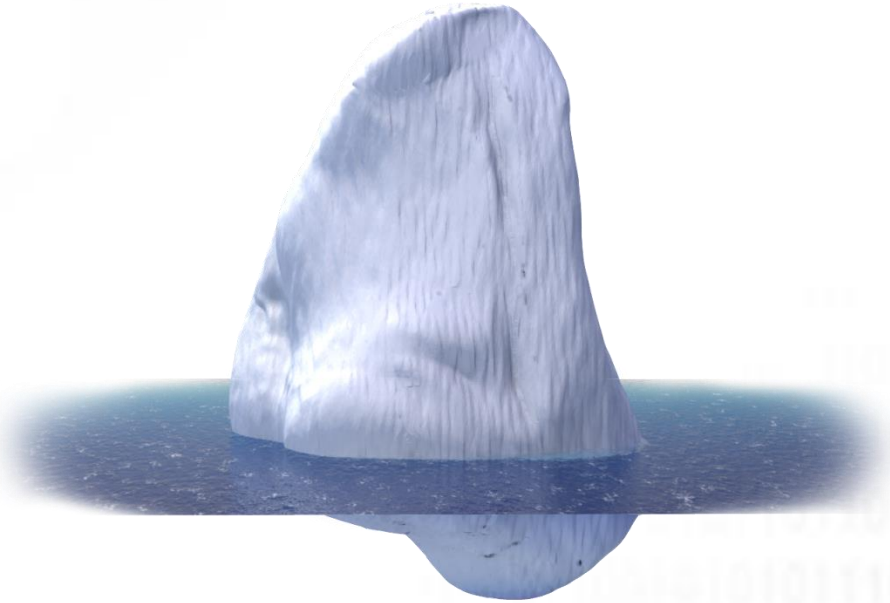
Other Perspectives

- Privacy applications of deception
- "Social camouflage" via pseudonyms in online gaming platforms
- Obfuscation - cockney rhyming slang
- Deception for defense - avatars in VR/AR
- Is part of the problem that there is just asymmetry in the way that different parties value these resources? As in, a lot of the technology is doing something that people just don't care enough to secure?

Game Theory

- Is game theory used in the real world (as we know that honeypots are)?
- As in, can it be used to design systems?
- Used extensively in the financial system to estimate performance of various funds
- Are they used to determine whether certain strategies are effective in actual software development? We don't know.
- Do we have the data about attacks needed to do this? Not really.
- Simulations are still expensive to design and run.

It Is Just the Tip of The Iceberg



It is a research agenda to address problems at the intersection of predictive analysis, defense by deception, and game-theoretic analysis to enable stakeholders to protect their systems from various attacks that cost industries billions of dollars annually.

Looking Ahead

- Create a theory of DbD for securing software applications.
- Design automated approaches for modeling the detection and protection against attacks using DbD.
- Empirical evaluation
- Technology transfer

Conclusions

This proposed research program is novel, as to the best of our knowledge, there exists little prior approach that addresses the problem of using DbD for securing systems in an automated way.

The short-term impact of DbD will be in the mobile apps community, where developers will use our approach to secure existing applications. The long-term impact will be on tools in securing commercial software and systems.

Mark Grechanik
Email: drmark@uic.edu