Cybersecurity via Signaling Games

Toward a deception-free cyber future

Problem: How can we establish trust, manage risk, and mitigate deceptive cyber attacks when decision-making is constrained by limited awareness of vulnerabilities, threats and systems properties.

Proposed Solution: A fundamental model of human actions and the formal machine properties they affect.

Our approach: A **game-theoretical** model to simultaneously study systems states/properties and human incentives:

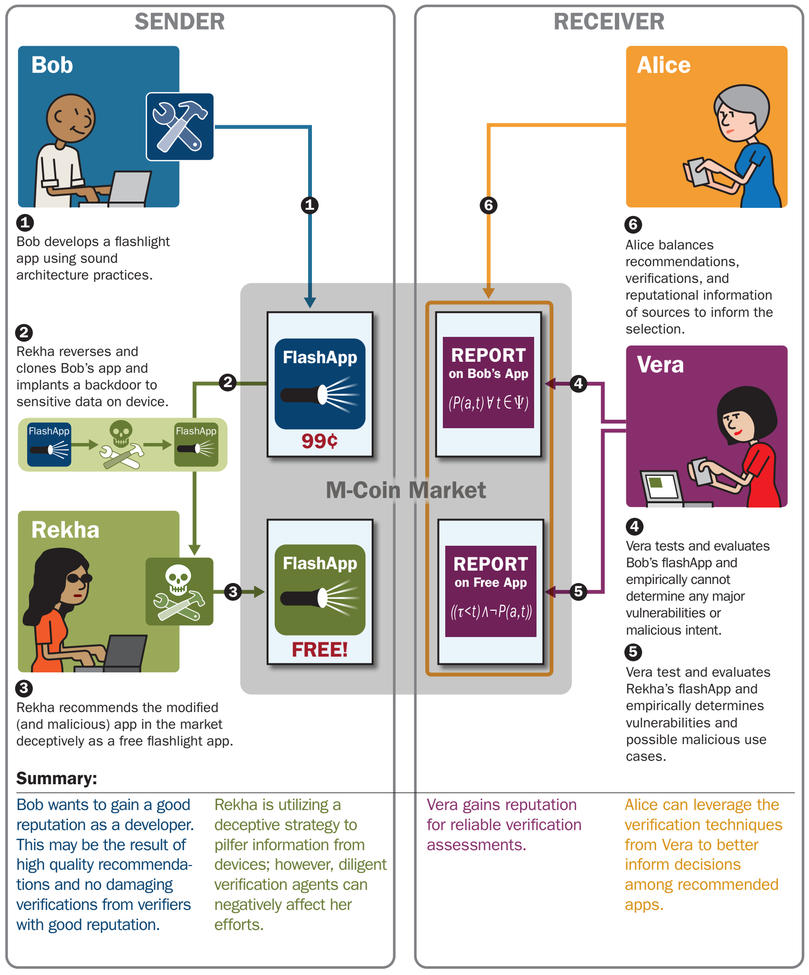
- Gives mathematical (and virtual) means to create and explore a wide range of mechanisms that re-design the microcosm of interactions
- Agent based model/simulation and analytic calculation applied toward understanding behavior modes in social technological systems

Applications: Using the game model we have:

- Studied multiple cybersecurity problems
- Qualitatively characterized modes of social-technological systems with adversarial strategies
- Identified novel mechanisms for mode selection including self-adaptive systems and risk-sensitive controllers

Key insight: Cybersecurity depends on

- The formal states, properties, and actions supported by the cyber-physical structures
- Utilities of agents operating with limited information of machine properties, device states, configurations. Agent utilities (or types) are not common knowledge leading to asymmetries.
- **These Utilities can be formalized with information-asymmetric signaling games to model adversarial and deceptive strategies.**



In cyber systems, several information asymmetric games can arise. This image illustrates malware injection and malicious recommendation.

The Scenario:

To illustrate the nature of information asymmetries and non-cooperative strategies in social-technological systems, consider the 'flashlight' app that tracks a device's GPS positions. The app is advertised as benign but the GPS tracker component is hidden by the software distributor – at least during the 'operational attack period' where trusting users remain unaware of that capability. The flashlight app collects GPS data from the device and compromises the users' privacy without their knowledge. This scenario describes a loss of private information but generalizes to an adversarial attempt to increases informational asymmetries, and this disposes the trusting user to various risks and grave exploitation possibilities.

Explored applications:

- **Fundamental dynamics of agent based systems.** Computer simulations of evolutionary games and mutable strategies explore the qualitative system modes parameterized by costs/benefits of signaling games. Talk is cheap, and costly signaling helps. Scaling a 'market of proof checkers' with an m-coin mechanism provides a way to impute costly signaling and a strong recovery pathway for systems under high levels of deception.
- **Epistatic signaling and minority games.** Considers games over multiple vulnerabilities (exploits) and examines how a social system may response to curtail evolving deceptions. Preferential early mover advantages have similar effects to maintaining strong global effectiveness measures but will be easier to implement.
- **App markets and malware:** We consider a means to create and evolve defensive strategies to malware built from semi-supervised learning of formal properties associated with malware traces. We outline a means to deploy these defenses with a Recommendation/Verifier System.
- **Insider threat and risk sensitive compliance controller.** We consider the problem of intentional and unintentional malicious insiders and the relation between their actions/signals and the risk they cause. We discover a means to estimate risk and actuate compliance incentives in a closed control loop.

Publications:

- **Awarded Best Paper: "Compliance Control: Managed Vulnerability Surface in Social-Technological Systems via Signaling Games,"** 2015 ACM CCS International Workshop on Managing Insider Security Threats
- **"Cyber Security via Minority Games with Epistatic Signaling,"** 2014 International Conference on Bio-inspired Information and Communications Technologies
- **"Agent-Based Trace Learning in a Recommendation-Verification System for Cybersecurity,"** 2014 IEEE International Conference on Malicious and Unwanted Software
- **"Cyber Security via Signaling Games: Toward a Science of Cyber Security."** 2014 International Conference on Distributed Computing and Internet Technology.

Future Work:

- Formalize notion of deception and risk in games (utilities/properties).
- Application to identity deceptions and Sybil attacks.
- Scaling the agent based recommendation/verification system.
- Policy optimization built on data science and inference.

Contact: W. Casey, J.A. Morales, R. Weaver, E. Wright at CMU SEI , B. Mishra (Courant Inst. NYU)