PROJECT SUMMARY

Overview:

Dynamic analysis of potential malware within virtual environments are being employed by antimalware to complement static analysis or signature based detection, which often cannot keep up with developments of new malware and code obfuscation techniques. In response, malware developers study deployed antimalware and find new ways to detect emulated environments to hide their malicious activity and evade detection. Creating emulated environments that are indistinguishable from the real machine being defended would be too expensive.

We will use sandbox to refer to virtual environments, a.k.a. instrumentation or emulation. The tools of game theory are well suited to analyze the strategic interaction between malware developers (M) and antimalware developers (AM) in our setting of sandboxing where AM's strategies involve the use of virtual environments to dynamically analyze the malware. Unfortunately, despite the large literature and wide application of game theoretic analysis of problems in physical and security, sandboxing has not been analyzed. Currently, the development of antimalware is a largely manual exercise.

To unleash the power of game theory in the AM vs. M war via sandboxing, we aim at establishing the computational game-theoretic foundation of the sandbox game. More precisely, the key research question we ask is the following.

Key research question. How can we model sandboxing as a game and characterize and compute optimal strategies for the antimalawarel?

We will address this question in various realistic game theoretic models. The goal is to understand the mathematical structure of the optimal strategy for AM, often called an equilibrium, and to compute such strategies to minimize the chance of infection. We propose to explore extensions of the basic model along three dimensions. Dimension 1: Information and dynamics of the game. Dimension 2: Antimalware's strategy space. Dimension 3: Malware's strategy space.

Intellectual Merit:

The main merit of this research is to establish the trade-offs between emulation, resource allocation, and distinguishability. It will provide useful results to current ongoing research efforts on environmental authentication. Recent work in game theory have successfully found applications in real world problems of physical and cyber-security. However, there is surprisingly little work on game theoretic analysis of malware antimalware interactions, despite its pervasiveness. This proposal bridges of the gap between the cybersecurity and game theory research communities in fighting malware. The proposed research will benefit from the expertise of cybersecurity experts on the behavior of malware developers, research on new attack vectors, vulnerabilities and limitations of hardware and software platforms. On the other hand, dealing with the challenges of real world problems in fighting malware will lead to the development of new theory in algorithmic game theory. The proposed research will also benefit from economics research dealing with bounded rationality of malware developers, and the incentive structure of malware and antimalware developers.

Broader Impacts:

The major broader impact is that the proposed computational methods for computing optimal strategies of sandboxing will improve the efficiency and effectiveness of antimalware. This will have significant impact in a wide range of situations, including elections, businesses, national security, etc. This research will produce metrics to evaluate different commercial malware products by quantifying the amount of resources they allocate to sandboxing and protections they can provide.

Keywords: antimalware, sandbox, game theory, equilibrium.