2016 International Conference on Computational Social Science
June 23-26, 2016 IC^{2}S^2

Cyber Security as an Evolving Host-Parasite System

Russell C. Thomas
Department of Computational and Data Sciences
George Mason University

Mathew Woodyard
Zions Bancorporation

Keywords: dynamic games, socio-technical systems, evolutionary systems, industry applications, agent-based modeling

ABSTRACT: When facing adaptive attackers, under what circumstances does evolution lead to effective cyber security defenses? This research examines cyber security as a host-parasite system. Host-parasite systems differ from competition systems in that resources and capabilities of the host might be repurposed by the parasite. Thus, innovations in host capabilities may lead to new possibilities and niches for parasites (an "unintended consequence"), in contrast to competition systems where only innovators reap the benefits. In this research, cyber security is modeled as a network of 2-level, 2-player repeated games among *N* defenders and *M* attackers with a large number of possible strategies for each player (a.k.a. "complicated") and with random payoffs. Computational experiments show that the relative rate of strategy evolution is key. When defender strategies evolve slower than a critical value, attackers are able to sustain themselves and persist. Therefore, successful cyber defense depends on the relative rate of strategy evolution.

According to many commentators, cyber security is different from other risky socio-technical systems because of intelligent adaptive adversaries. The implication is that intelligent/adversaries will outfox any defensive scheme and thus make it impossible to do quantitative risk analysis and may make it unlikely to achieve successful cyber defense. Specifically, it is claimed that intelligent adversaries lead to non-stationary loss event distributions that favor attackers. Cyber security has also been characterized as a 'complicated game' in the same sense that chess and go are called complicated – very large number of possible moves ("strategies") and a very large state space with uncertainty payoffs. The implication is that complicated games are beyond the ken of bounded rational players, and therefore players must resort to adaptive learning methods to choose strategies rather than the fully rational strategies assumed in Game Theory. Putting these two implications together, the research question is: When can adaptive learning processes lead to effective cyber security defenses, even in the face of intelligent/adaptive adversaries?

In most theoretical research, cyber security has been modeled as a *competitive system* between defenders and attackers. That is, defensive improvements and innovations reduce the likelihood and/or severity loss events due to attacks, and vice versa. In a competitive system, defensive improvements will never lead to increased probability of attacker success, and vice versa.

However, framing cyber security as a competitive system has fundamental flaws. First, defenders are primarily concerned with cooperative relationships with other defenders (a.k.a. "normal operations"). The sole purpose of security investments is to protect "normal operations" from undesirable outcomes and loss events. Second, attackers depend upon and subsist on the resources and capabilities of defenders. Simply put, attackers use and depend upon computers, software, networking, internetworking, storage, and so on, including the computing/communications resources of the targets of their attacks (a.k.a. defenders). Therefore, attackers do not aim to destroy or eliminate defenders as a class and as a pool of resources and capabilities. Instead, they aim, using their own resources and capabilities, to commandeer defender resources and capabilities to their own ends. This leads to a view of the system as *mutualistic* rather than competitive, and more specifically, as a *host-parasite system*. Host-parasite systems differ from competition systems in that resources and capabilities of the host might be repurposed by the parasite for the benefit of the parasite and to the detriment of the host. Thus, innovations in host capabilities may lead to new possibilities and niches for parasites (an "unintended consequence"), in contrast to competition systems where only innovators reap the benefits.

In this research, cyber security is modeled as a network of 2-level, 2-player repeated games among N defenders and M attackers with a large number of possible strategies for each player (a.k.a. "complicated") and with random payoffs. The upper-level game ("Investments Game") is choice of investments, where each alternative investment enables a set of possible "moves" (a.k.a. strategies, i.e. combinations of policies, process, and routines). The payoffs of the Investment Game depend on the realization of the lower-level game. The lower-level game ("Practices Game") is choice of moves. The two games have different "clock cycles", with the clock cycle for Practices Game being a hundred to a thousand times more frequent than the clock cycle of the Investment Game.

The game dynamics described below applies only to the Practices Game. The "friendly games" between defenders have Gaussian payoffs with benign (zero) correlation between payoffs. There "adversarial games" between attackers and defenders that are negatively correlated with lognormal payoffs and positive mean value for defenders. Thus, attackers have to do much better than random play in order to survive. All players choose strategies via experienced-based learning (see below). Without attackers ("parasites"), the N-player system of defenders leads to dynamics which beneficial all players, either via equilibria or through chaotic dynamics. Adding M attackers (i.e. an N+M player system) results in chaotic dynamics that sometimes favor defenders and sometimes favor attackers, either temporarily or sustained. Several parameters determine the learning rate (separately) for defenders and attackers, and critical value of these parameters determine whether, on average, the system will evolve strategies that are favorable to defenders or to attackers or to both (mutualistic).

The model has been implemented in *NetLogo*, drawing on the model of 2-player complicated games from Galla and Farmer (2013). Their complicated games feature 50 possible moves, which has been extended to 400 in the present model. Their games were limited to 2 players, which has been extended to N+M 2-player games in the present model. The Galla and Farmer model uses *experience-based learning*, and this is used in the present model. Players do not know each other's payoffs, only the current probability for each opponent move. At each clock

tick, players update their move probabilities with a convex combination of the previous value and an updated value. The updated value is a normalized function of the sum of the player's payoffs multiplied the probability of all opponent's moves. The dynamic effect of this mechanism is coupling between player preferences. Figure 1 shows results from two representative runs, each with 11 defenders (who play each other and also attackers), 3 defenders (who only play defenders), and the same payoff matrices for each (100 possible moves). The charts show results for two focal players, plus average payoffs for all players for the most recent 100 ticks. The run on the left results in successful cyber security defense, while on the right is unsuccessful (i.e. positive payoffs for attackers).

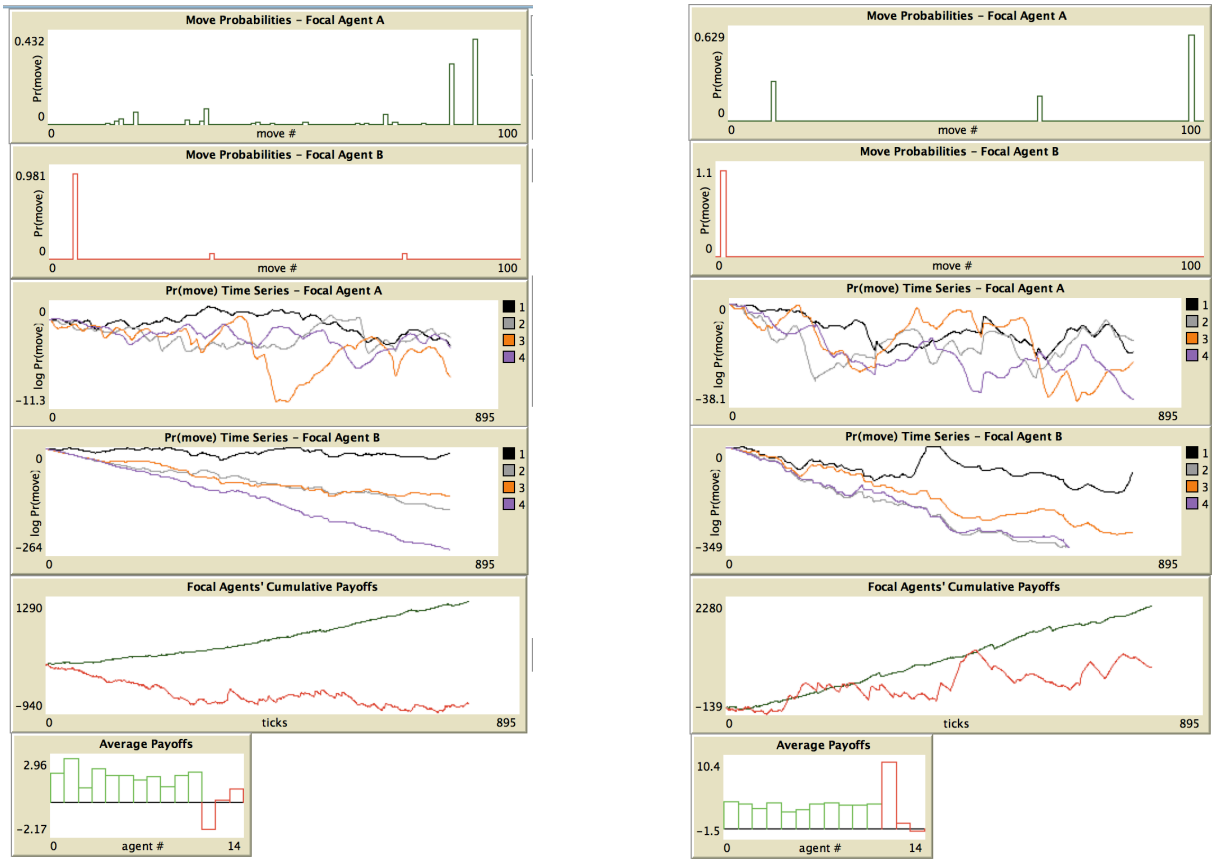

Figure 1. Two representative runs. Both exhibit chaos. The difference is defender learning rate.

Acknowledgment

This work has been partially supported by the US National Science Foundation under Grant No. CMMI-1400466.

References

Galla, T., & Farmer, J. D. (2013). Complex dynamics in learning complicated games. *Proceedings of the National Academy of Sciences*, **110**(4), 1232–1236.