A Supervisory Control Approach to Dynamic Cyber-Security

Mohammad Rasouli, Erik Miehling, and Demosthenis Teneketzis

Department of Electrical Engineering and Computer Science
University of Michigan, Ann Arbor, MI, USA

Abstract. An analytical approach for a dynamic cyber-security problem that captures progressive attacks to a computer network is presented. We formulate the dynamic security problem from the defender’s point of view as a supervisory control problem with imperfect information, modeling the computer network’s operation by a discrete event system. We consider a min-max performance criterion and use dynamic programming to determine, within a restricted set of policies, an optimal policy for the defender. We study and interpret the behavior of this optimal policy as we vary certain parameters of the supervisory control problem.

Keywords: Cyber-Security, Computer Networks, Discrete Event Systems, Finite State Automata, Dynamic Programming.

1 Introduction

Cyber-security has attracted much attention recently due to its increasing importance in the safety of many modern technological systems. These systems are ubiquitous in our modern day life, ranging from computer networks, the internet, mobile networks, the power grid, and even implantable medical devices. This ubiquity highlights the essential need for a large research effort in order to strengthen the resiliency of these systems against attacks, intentional and unintentional misuse, and inadvertent failures.

The study of cyber-security problems in the existing literature can be divided into two main categories: static and dynamic.

Static problems concern settings where the agents, commonly considered to be an attacker and a defender, receive no new information during the time horizon in which decisions are made. Problems of this type in the security literature can largely be classified under the category of resource allocation, where both the defender and attacker make a single decision as to where to allocate their respective resources. The main bodies of work involve infrastructure protection [3, 7, 9] and mitigation of malware and virus spread in a network [5, 6, 8, 16]. Some of the above works consider settings where the agents are strategic [3, 9]. The presence of strategic agents results in a game between the attacker and defender. The strategic approaches in the above works are commonly referred to as allocation games. The survey by Roy et al. [18], as well as [20], provide useful outlines of some static game models in security.
Dynamic security problems are those that evolve over time, with the defender taking actions while observing some new information from the environment. The formulation of a security problem as a dynamic problem, instead of a static one, offers numerous advantages. The first advantage is clear; since real-world security problems have an inherently dynamic aspect, dynamic models can more easily capture realistic security settings, compared to static models. Also, most attacks in cyber-security settings are progressive, meaning more recent attacks build upon previous attacks (such as denial-of-service attacks, brute-force attacks, and the replication of viruses, malware, and worms, to name a few). This progressive nature is more easily modeled in a dynamic setting than in a static setting.

The literature within the dynamic setting can be further subdivided into two areas: models based on control theory and models based on game theory. The control theory based security models in the literature differ in the ways in which the dynamics are modeled. The work by Khouzani et al. studies the problem of a malware attack in a mobile wireless network; the dynamics of the malware spread are modeled using differential equations. A large part of the literature on control theory based models focuses on problems where the dynamics are modeled by finite state automata. The works of implement specific control policies (protocols) for security purposes. The work of Schneider uses a finite state automaton to describe a setting where signals are sent to a computer. Given a set of initial possible states, the signals cause the state of the computer to evolve over time. An entity termed the observer monitors the evolution of the system and enforces security in real-time. Extensions of Schneider’s model are centered around including additional actions for the observer. Ligatti et al. extend Schneider’s model by introducing a variety of abstract machines which can edit the actions of a program, at run-time, when deviation from a specified control policy is observed. More recent work develops a formal framework for analyzing the enforcement of more general policies. Another category of dynamic defense concerns scenarios where the defender selects an adaptive attack surface in order to change the possible attack and defense policies. A notion termed moving target defense (a term for dynamic system reconfiguration) is one class of such dynamic defense policies. The work of Rowe et al. develops control theoretic mechanisms to determine maneuvers that modify the attack surface in order to mitigate attacks. The work involves first developing algorithms for estimation of the security state of the system, then formalizing a method for determining the cost of a given maneuver. The model uses a logical automaton to describe the evolution of the state of the system; however, it does not propose an analytical approach for determining an optimal defense policy.

---

1 This new information could consist of the attacker’s actions, events in nature, or the state of a some underlying system.

2 For example, changing the network topology.