On the Road to Holistic Decision Making in Adaptive Security

Mahsa Emami-Taba, Mehdi Amoui, and Ladan Tahvildari

> *"When you have to make a choice and don't make it, that is in itself a choice."*
>
> William James (1842–1910)
> Philosopher and psychologist

Security is a critical concern in today's software systems. Besides the interconnectivity and dynamic nature of network systems, the increasing complexity in modern software systems amplifies the complexity of IT security. This fact leaves attackers one step ahead in exploiting vulnerabilities and introducing new cyberattacks. The demand for new methodologies in addressing cybersecurity is emphasized by both private and national corporations. A practical solution to dynamically manage the high complexity of IT security is adaptive security, which facilitates analysis of the system's behaviour and hence the prevention of malicious attacks in complex systems. Systems that feature adaptive security detect and mitigate security threats at runtime with little or no administrator involvement. In these systems, decisions at runtime are balanced according to quality and performance goals. This article describes the necessity of holistic decision making in such systems and paves the road to future research.

Introduction

Cybersecurity threats, such as Internet worms (tinyurl.com/lg2wghw), can spread too quickly for humans to respond and pose a genuine risk to users and systems. In March 2013, a computer scam fooled some Canadian Internet users by picking up their location and making it appear as though the Royal Canadian Mounted Police had frozen their screens; pop-ups demanded that users must pay a $100 fine to have their computer unlocked (CBC, 2013; tinyurl.com/lhuwq82). In the same month, a computer virus paralyzed computer networks of broadcasters and banks in a network attack in South Korea (BBC, 2013; tinyurl.com/cgustwk). The economic and national security consequences of these types of attacks are severe. The official website of the United States Department of Homeland Security (DHS; tinyurl.com/kttv9qo) indicates that the Secret Services Cyber Intelligence Section has directly contributed to the arrest of transnational cybercriminals who were responsible for the theft of hundreds of millions of credit card numbers and the loss of approximately $600 million to financial and retail institutions. The same resource indicates that, in 2011, the DHS prevented $1.5 billion in potential losses through cybercrime investigations. The distributed architecture of networks results not only in faster propagation of cyberattacks, but it also affects a greater number of vulnerable cyberdevices. For example, in 2003, the Slammer worm infected more than 90% of vulnerable hosts in 10 minutes (Moore et al., 2003; tinyurl.com/koweuj5). Traditional security models are not able to keep up with the security attacks that propagate at machine speed.

McConnell (2011; tinyurl.com/65udd87) explored the technical options to enhance cybersecurity through three major building blocks: automation, interoperability, and authentication. These building blocks provide the means to limit the spread of attacks and thus minimize consequences. McConnell introduced the concept of automated courses of action (ACOA), which encapsulates many of the complex decisions and activities in-

On the Road to Holistic Decision Making in Adaptive Security

Mahsa Emami-Taba, Mehdi Amoui, and Ladan Tahvildari

volved in defending cybersystems. The concept of ACOAs is a novel step toward enabling the collective action required to protect against evolving cyberthreats. Novel decision-making approaches will enhance these courses of actions in response to cybersituations.

Automation accelerates the analysis of monitored data and perhaps increases the number of symptoms that can be detected in order to prevent a threat. Moreover, automation helps to speed up the decision-making process at the time of attack. An immediate, suboptimal response can sometimes be more effective than a later, optimal response. These timely actions prevent the spread of attack and therefore minimize the consequences of the attack. In recent years, interest in building software systems that are adaptive to their security goals has increased. Self-adaptive software (SAS) systems address automation in response to changes in the requirement and environment. SAS *monitors* itself and its context, *detects* significant changes, *decides* how to react, and *executes* such decisions (Salehie and Tahvildari, 2009; tinyurl.com/lffu25g). *Adaptive security* refers to solutions that aim to adapt their defence mechanisms at runtime. This class of SAS is called self-protecting software (SPS). SPS systems have the ability to detect security attacks and trigger countermeasures. These systems not only defend against the malicious attack but also are capable of anticipating problems and taking steps to avoid them or moderate their effects (Salehie and Tahvildari, 2009; tinyurl.com/lffu25g). In this article, we focus on the role of *automation* in cybersecurity. First, we raise awareness of the importance of addressing adaptive security from a holistic view of the system. Second, we show how game theory can contribute to decision making in adaptive security.

The rest of this article is organized as follows. The next section provides an overview of the active work on self-protecting systems. Then, we highlight the importance of creating a holistic decision-making strategy in cybersecurity, after which we discuss the use of game theory in the network and application architecture layers of the system. Finally, we conclude by describing the steps required to achieve a holistic decision-making strategy.

SPS Tools and Techniques

Projects in both academia and industry have addressed adaptivity in software systems. Table 1 lists recent research and development achievements in self-protecting software systems.

A revealing insight from this overview of tools and techniques is the absence of adaptation decision-making that captures all the possible knowledge from the software system and incorporates that knowledge in making effective adaptive decisions. In both academia and industry, SPS is still in its early years.

Holistic Decision Making in Adaptive Security

The fundamental relationship between security and decision making is highlighted by Alpcan and Başar (2010; tinyurl.com/mfvae39). Making systematic decisions, such as allocating resources while balancing risks, can benefit the system with efficient protection against both known and unknown attacks. The dynamic nature of network security requires dynamic analysis and decision making based on the monitored data. Dynamic measurements of the system metrics and states manifest dynamic changes both in the system itself and in the environment.

Figure 1 illustrates the process of acquiring data from different layers of the software's architecture through sensors. The adaptable software may contain one or more layers than are shown in this figure. Here, the rest of the layers that are not included in the software *itself* are considered as the *environment*. A *holistic decision-making strategy* considers knowledge from different layers of the system in its decision-making process. The monitored data is gathered from the sensors of the system itself and its environment. Depending on the system, some layers may not provide access for the sensors or effectors in that layer. The data gathered by sensors is transmitted through event buses to the adaptation manager, which contains the four main adaptation processes: monitor, analyze, plan, and execute. The planning process encapsulates the decision-making engine. The knowledge of the system itself and its environment is shared among the adaptation processes. Correspondingly, adaptation action is applied through effectors in various layers of the software system. The decision-making technique must embody the gathered knowledge from various sources and find the effective alternate action in the most appropriate layer of the software system. The set of adaptive security actions can be applied in more than one layer of the software system. The effectors that are responsible for performing adaptation actions reside in the layers of the system itself and its environment based on the access permission to different architecture layers.

On the Road to Holistic Decision Making in Adaptive Security

Mahsa Emami-Taba, Mehdi Amoui, and Ladan Tahvildari

Table 1. Notable examples of research from academia and industry relating to self-protecting systems and adaptive security

Academic Research		
Author (Year)	**Project/Approach**	**Description**
Hashii et al. (2000) tinyurl.com/lkbsdbw	An extensible security infrastructure that supports fine-grained security policies	Accommodates adaptive security by dynamically modifying the policies based on the mobile code environment.
Feiertag et al. (2000) tinyurl.com/kdqqdu8)	Intrusion detection inter-component adaptive negotiation (IDIAN)	Allows intrusion-detection systems to dynamically cooperate and evolve based on the changes in the environment. The negotiation among intrusion-detection systems is facilitated by a negotiation protocol.
Scott and Davidson (2001a) tinyurl.com/n3fofdb (2001b) tinyurl.com/m3vb5ez	Strata project	Uses software dynamic translation (SDT) technology to alter code at the instruction-level. Strata can be exploited to provide adaptive security by defining dynamic and adaptive security policies.
Knight et al. (2002) tinyurl.com/kyyye9q	Willow architecture	Provides adaptive security by reconfiguration.
English et al. (2006) tinyurl.com/lwyqmbn	Trust management	Provides adaptive security by reconfiguration.
Claudel et al. (2006) tinyurl.com/kcu5veo	Application of JADE	Benefits from component-based software engineering to protect distributed systems.
Al-Nashif et al. (2008) tinyurl.com/lrfk6uh)	Multi level intrusion detection system (ML-IDS)	Detects network attacks by inspecting and analyzing the traffic using several levels of granularity.
Blount et al. (2011) tinyurl.com/k4c43r2	Adaptive rule-based malware detection	Leverages learning classifier systems to improve the accuracy of intrusion detection in detecting unknown attacks.
Pasquale et al. (2012) tinyurl.com/kgovcan	SecuriTAS	Enables software designers to model security goals and requirements of a system at the design time. The model is used at runtime to analyze and plan processes of adaptation.
Industry Research		
Author (Year)	**Project/Approach**	**Description**
Burns et al. (2001) tinyurl.com/lqjp8w5	Automatic management of security policies in dynamic networks	Validates policies by models of network elements and services.
Ryutov et al. (2005) tinyurl.com/l3r6r7d	Adaptive trust negotiation and access control (ATNAC)	Uses a framework that provides adaptive access control.
Costa et al. (2005) tinyurl.com/me5ch4u	Vigilante	Provides automatic worm containment. The advantage of Vigilante is that it is not limited to network-level information about the worms.
He and Lacoste (2008) tinyurl.com/m8xxhqv)	Component-based software paradigm	Provides adaptive security in ubiquitous systems.

On the Road to Holistic Decision Making in Adaptive Security

Mahsa Emami-Taba, Mehdi Amoui, and Ladan Tahvildari

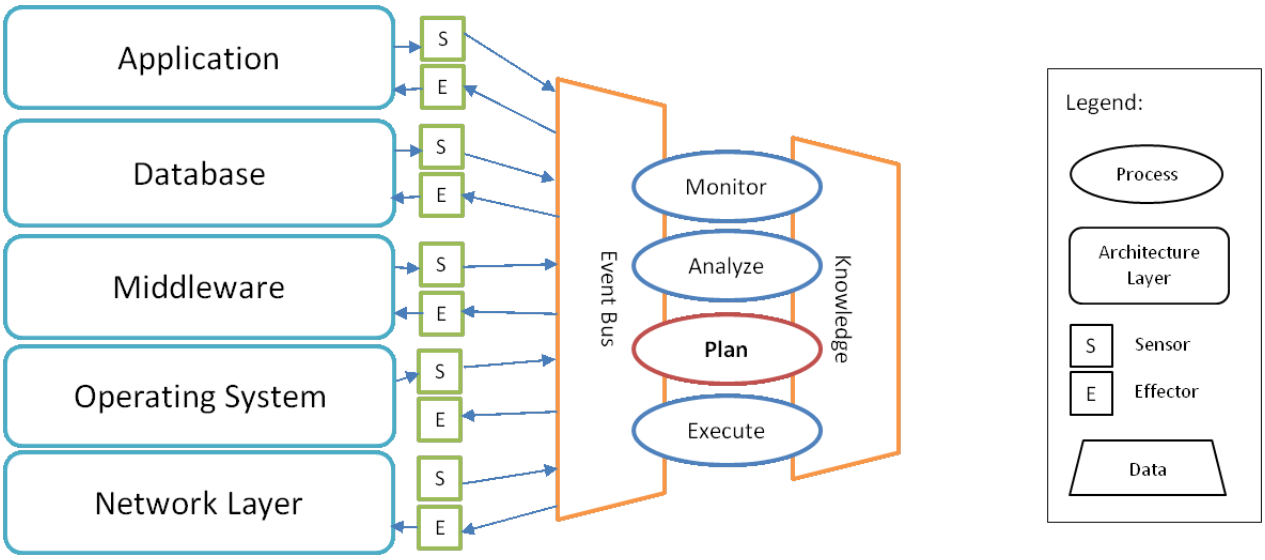

Figure 1. Decision making based on holistic shared knowledge of system layers

The need for holistic management in disciplines such as management science is explored through enterprise integration (Dalal et al., 2004; tinyurl.com/kkwvapu). Besides, vulnerability and risk management can benefit from a holistic methodology by assessing the non-linear relations of contextual parameters and the complexity and dynamics of social systems (Cardona, 2003; tinyurl.com/l3m6zdl). Recently, the idea of delivering a holistic approach to addressing cybersecurity has received greater attention. Bencomo, Belaggoun, and Issarny (2013; tinyurl.com/kr6sc56) provide a holistic view to tackle self-adaptation under uncertainty. They use the mathematical model of dynamic decision networks (DDNs) to support decision making under uncertainty for self-adaptation. An architecture-based approach in SPS systems was recently proposed by Yuan and colleagues (2013; tinyurl.com/n6ydvn7); their approach benefits from the holistic view of the systems that is provided by the software architecture.

A holistic view of the application and its environment can be completed through feedback loops. Feedback loops help to combine the result of adaptation with theoretical formulation of the problem. Developing a decision solely based on the mathematical model does not reflect the actual consequences of the decisions made. Incorporating a feedback loop in the decision-making engine helps to repeatedly observe the result of the actions made and consider its effectiveness in future alternative actions.

In summary, to achieve a holistic decision making strategy: i) security goals must be defined at each architecture layer of the system; ii) appropriate decision-making models and techniques should be applied to reduce conflicts and increase the decision quality; and iii) adaptation should not be limited to detecting and preventing attacks – adaptation must also stop the spread of the attack after it happens.

From game theory to adaptive security

A variety of mathematical theories can be used to model and analyze cybersecurity. Resource-allocation problems in network security can be formulated as *optimization problems* (Alpcan and Başar, 2010; tinyurl.com/mfvae39). In dynamic systems, *control theory* is beneficial in formulating the dynamic behaviour of the systems. In contrast, *game theory* provides rich mathematical tools and techniques to express security problems. Security games allow players (the defender and the attacker) to develop a systematic strategy based on formalized methods. In security games, players do not have access to each other's payoffs; therefore, they observe the opponent's behaviour and estimate the result of their action. Security games can be modelled as *non-cooperative games* in which players make decisions independently.

Due to limited resources in software systems, a practical approach is to utilize the resources and protect them against malicious attacks. Critical assets such as person-

On the Road to Holistic Decision Making in Adaptive Security

Mahsa Emami-Taba, Mehdi Amoui, and Ladan Tahvildari

al or sensitive information also require protection. Game theory provides a formal approach to maximize the effectiveness of resources against cyberthreats (Tambe, 2011; tinyurl.com/m6nwedq). From simple deterministic games to more complex stochastic games, security games can be used to model security in intrusion-detection systems and social, wireless, and vehicular networks (Alpcan and Başar, 2010; tinyurl.com/mfvae39).

The analytical foundation of game theory can be applied to security problems at various architecture layers of the system. For example, intrusion detection is a defence mechanism at the network layer. Intrusion-detection systems can take adaptive actions such as intensifying monitoring efforts when malicious behaviour is detected. In the remainder of this section, we look at the applicability of game theory in two architecture levels: the network layer and the application layer.

Security games at the network level

Network security is a strategic game between the malicious attacker and the administrator (Alpcan and Başar, 2010; tinyurl.com/mfvae39). In a simple intrusion-detection game, the attacker chooses between the alternative actions of attacking or non-attacking. Due to limited resources by the systems and the fact that monitoring and analyzing the monitored data adds overhead to the system, the system has the option to continue the default monitoring or to intensify monitoring. This simple formulation can be extended in complex cases such as stochastic games or games with limited information, which are discussed in greater detail by Alpcan and Başar (2010; tinyurl.com/mfvae39). After distinguishing the alternative actions by each player, the next step is to associate the payoff for each action. Based on the decision strategy, players select the alternative that yields a better payoff. Similar modelling can be applied to intrusion-prevention systems and efforts to prevent denial-of-service attacks. In the latter case, the alternative actions of the attacker could be changing the rate of data generation in the network. Meanwhile, the system's alternative actions are: i) checking the rate of congestion and ii) modifying the refresh interval. After identifying the main components of the game theory (i.e., players, the set of alternative actions, and the payoffs), the more appropriate type of game can be selected based on the availability of data. For example, if complete knowledge of the adversary payoffs is available, *repeated complete-information games* can be exploited in modelling.

Security games at the application level

Existing cybersecurity approaches based on game theory are mostly focused on providing security at the network level. The mathematical foundation of game theory can also be applicable to security at a variety of architecture levels such as the database or operating system. Here, we discuss the applicability of game theory in providing security at the application level. Depending on the architecture layer, the source of the data to be monitored is different. To detect a cyberattack at the network level, the data to be monitored can be packet data, network traffic, etc. At the application level, a cyberattack can be detected from various data sources. For example, the system can monitor the number of transactions by a specific user or the access rights of a user over a specific window of time. Even though the nature of the monitored data may vary, the problem can still be modelled as a non-cooperative game. The alternative set of actions includes more high-level actions that should align with the system's specified policies. As an example, the dynamic change to the access rights of a user should satisfy the pre and post conditions specified in the IT policy.

Previous approaches, such as those used by Alpcan and Başar (2010; tinyurl.com/mfvae39), only apply game theory at one layer of the system. To provide a holistic approach in making decisions at runtime using game theory, defining the set of alternative actions that can be taken by both players should not be limited to actions in only one layer of the systems. The same requirement applies to the data gathered by sensors in various architecture layers.

Conclusion

This article presents a brief overview on adaptive security and existing tools and techniques for SPS, and it introduces a visionary approach in holistic decision making to achieve adaptivity in cybersecurity. It provides insights into the use of game theory as a decision-making strategy that can be applied in different architecture levels. A proper decision-making strategy not only helps to model security goals and actions at runtime, but it also enables systematic decision making after the attack happens and it consequently limits the spread of attack in distributed systems.

On the Road to Holistic Decision Making in Adaptive Security

Mahsa Emami-Taba, Mehdi Amoui, and Ladan Tahvildari

Acknowledgements

The authors would like to express their appreciation for the generous financial support received from the Communications Security Establishment Canada (CSEC) on this project. Special thanks to Sharon Liff, D'Arcy J. Walsh and Daniel H. Craigen for their tremendous technical support. We also thank the reviewers for their valuable feedback.

About the Authors

Mahsa Emami-Taba received her BEng degree in Computer Engineering from Shahid Beheshty University, Iran, in 2005. She received her MMath degree in Computer Science from the University of Waterloo, Canada, in 2009. After completing her studies, she worked as a software designer and developer. She is currently working toward a PhD degree in the Department of Electrical and Computer Engineering at the University of Waterloo. Her research interests include self-adaptive software systems, adaptive security, and nature-inspired adaptive software.

Mehdi Amoui is a Postdoctoral Fellow at the University of Waterloo, Canada. He currently works as a researcher/consultant on a joint research project with the Software Verification and Validation team at Blackberry Inc., Canada. In 2002, he received his PhD from the University of Waterloo on the topic of an evolving software system for self-adaptation, and in 2006, he received an MASc degree in Artificial Intelligence and Robotics from the University of Tehran. His main research interests include self-adaptive software systems, search-based software engineering, software evolution, and software quality.

Ladan Tahvildari is an Associate Professor in the Department of Electrical and Computer Engineering at the University of Waterloo, Canada, and she is the founder of the Software Technologies Applied Research (STAR) Laboratory. Together with her research team, she investigates methods, models, architectures, and techniques to develop higher-quality software systems in a cost-effective manner. Her research accomplishments have been recognized by various awards, including the prestigious Ontario Early Researcher Award, which recognized her work in self-adaptive software. She is a Senior Member of the IEEE, a member of the ACM, and a Professional Engineer (PEng).

Citation: Emami-Tabla, M., M. Amoui., and L. Tahvildari. 2013. On the Road to Holistic Decision Making in Adaptive Security. *Technology Innovation Management Review*. August 2013: 59–64.

Keywords: cybersecurity, cyberattacks, adaptive security, holistic decision making, self-adaptive software, self-protecting software, automation, game theory, architecture