A Holistic Game Inspired Defense Architecture

Sajjan Shiva, Harkeerat Singh Bedi, Chris Simmons, Marc Fisher II, Ramya Dharam
Department of Computer Science
University of Memphis
Memphis, TN, USA

Abstract— **Ad-hoc security mechanisms are effective in solving the particular problems they are designed for, however, they generally fail to respond appropriately under dynamically changing real world scenarios. We discuss a novel holistic security approach which aims at providing security using a quantitative decision making framework inspired by game theory. We consider the interaction between the attacks and the defense mechanisms as a game played between the attacker and the defender. We discuss one implementation of our holistic approach, namely, *game inspired defense architecture* in which a game decision model decides the best defense strategies for the other components in the system.**

Keywords - Cyber Security; Game Theory; Holistic Security.

I. INTRODUCTION

The research and practicing community have been paying attention to the Internet and data security problems for more than two decades. However, these problems are far from being completely solved. The main limitation of the current security practice is that the approach to security is largely heuristic, is increasingly cumbersome, and is struggling to keep pace with rapidly evolving threats. The core security breaches occur in terms of confidentiality, integrity, and availability.

To overcome these problems, four types of security endeavors have been employed in the past. (a) Implementation of *Secure Communication Infrastructure* where, cryptographic algorithms are used to build secure networking protocols such as Internet Protocol Security (IPSEC) or Transport Layer Security (TLS). However if one endpoint is compromised, the crypto becomes helpless. (b) *Utilizing Monitoring and Response Systems* such as firewalls, intrusion detection systems (IDS) and antivirus programs. Further, with the advent of the virtualization technology, researchers are advocating to host applications on a virtual machine X, so that all activities in X could be observed by a monitor application residing outside X. Nevertheless, a perfectly safe monitor is yet to be designed. (c) In the *Built-In Approaches for System Development*, security features are designed up front and form part of the system development. However the *Bolt-On* approaches compensate for the errors made earlier in the development cycle and emergent errors introduced after the system is deployed. Bolt-on approach is the only solution for deployed (legacy) systems. (d) *Code Instrumentation Tools and Self Checking Modules* provide for enforcement of data and control flow integrity of a software component to provide security. Such techniques compute a flow graph using static or dynamic analysis, and instrument the program to check if the execution at runtime conforms to the flow graph. However, these techniques are not generally effective against polymorphic exploits.

Despite the past considerable effort to protect and secure software and data, it can be observed that the goal of securing the same is far from being accomplished.

Data security is a data engineering problem, which we aim to address in our proposed solution. We propose a holistic security approach Shiva et al. [11] which provides a framework that encompasses a whole system in a layered and organized manner. Most strategies to implementing security mainly focus on one specific area at a time. To help advance the cyber and data security community, our approach collectively uses monitoring tools, knowledge management systems, and game inspired decision models for achieving an optimal level of security.

The following Section II discusses our proposed holistic security scheme. Section III discusses an implementation of our holistic approach. Section IV briefly provides the related work with respect to approaches which focus on offering comprehensive security solutions. Section V provides the concluding remarks and future work with respect to our holistic approach.

II. A HOLISTIC SECURITY SCHEME

We envision a 4-layer holistic security scheme as illustrated in Figure 1. At the innermost layer are the core hardware and software components. We envision each of these components having a provision of being wrapped with a self-checking module (with inspiration from the traditional BIST architecture). At the second layer reside the Secure Applications which are designed with Built-In or Bolt-On security approaches utilizing self-checking concepts and components. At the third layer lies the traditional Security Infrastructure that is built using firewalls, anti-virus software, etc. At the fourth layer, we envision a Game Inspired Decision Module (GIDM) which is responsible for choosing the best security strategy for all the inner layers.

We visualize this fourth layer as one placed directly above the three previously defined layers, emphasized by the pie formation in Figure 1. This placement stresses the fact that GIDM can obtain input from any of the layers and can recommend probable defense actions for the same. The solid arrows in Figure 1 represent the progression of information pertinent to attack detection to the outer layer. The dotted line represents the flow of corresponding corrective action strategy as decided by the outer layer for the inner layers.

We observe that in the past, majority of the security efforts have only been in the second and the third layers. Traditional intrusion detection systems can be considered as residing in the third layer, which can be made more effective by the use of game inspired decision techniques, which resides in the outermost layer. Note that our layered view is an operational one and does not have any direct relationship with the traditional ring-oriented privilege separation principle or the OSI network stack.

We now define the layers contributing to our holistic security approach and characterize their purpose and interaction with the other layers to form a cohesive secure solution.

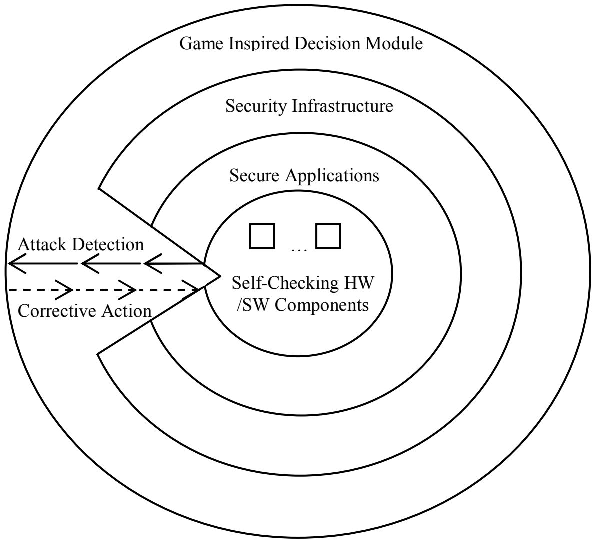

Figure 1. The Holistic Security Approach

A. *Self-Checking HW/SW Components*

The innermost layer consists of self-checking hardware and software components. Monitoring allows observing the behavior of the software to determine whether it complies with its intended behavior. We intend to use the BIST methodology Kranitis et al. [6] for monitoring hardware components. For monitoring software components we intend to use run time monitoring tools Delgado et al. [7] to specify the software properties that need to be monitored. When these monitors recognize a deviation of the software behavior we intend to use protocols for communicating the said information with the Game Inspired Decision Module (GIDM), which is explained later. GIDM will use a knowledge management system and a honey pot to effectively communicate the flow of information. This information is used to take preventative action against software executing malicious activity.

B. *Secure Applications*

The second layer in our holistic security model contains security applications, which offer a built-in or bolt-on approach. The built-in approach uses pre-release security components in a software application which ensure agreement with secure software specifications. The bolt-on approach use post-release patches and software updates to achieve the optimal level of security. In addition to built-in and bolt-on approaches we intend to perform monitoring in this layer by enabling the developers to develop monitors for the existing secure applications. The monitors can notify violations of specified properties to GIDM via protocols and perform recovery actions recommended by GIDM to avoid further deviation of the software.

C. *Security Infrastructure*

The third layer is the security infrastructure within GIDA, which primarily focuses on the use of tools such as intrusion detection system (IDS) and firewalls capturing raw input. The third layer also provides protocols for communicating with the outermost layer which is the Game Inspired Decision Module.

D. *Game Inspired Defense Model (GIDM)*

This outermost layer functions as the brain behind our holistic approach whose main purpose is to evaluate these attack vectors using game theoretic analysis and decide the best action strategy for the inner layers to counter committed or probable attacks. GIDM and a knowledge management system (KMS) accept input from the inner three layers, which contain the information related to malicious activity. The KMS classifies the nature of an attack using attack vectors and associated defense measures, which are propagated as input to GIDM. This decision module can also interact with honeypots which are used to gain knowledge of attack activity in a mendacious manner without the attacker being aware. This information is filtered into GIDM for selecting the optimal decision for defense. Information regarding the handling of defense recovery based on the attack is propagated back to the inner layers.

III. GAME INSPIRED DEFENSE ARCHITECTURE

Game Inspired Defense Architecture (GIDA) is an implementation of the above described holistic security approach. It focuses on the concept of offering defense strategies against probable and committed attacks by modeling such situations as multi-player game scenarios.

Figure 2 shows our Game Inspired Defense Architecture. We illustrate its flow of execution using a network based attack scenario. An attacker on the Internet aims at exploiting a vulnerability in one of components c_x on the Target Application which includes self-monitoring modules m_x. The modules monitor the individual components and contain the provision to send their findings to either the KMS or the Game Inspired Decision Module. These modules also include the ability to stop the execution of such components if deemed necessary. The Game Inspired Decision Module acts as the brain of this architecture and computes defense strategies based on feedback from the monitoring modules, KMS, the Honeypot and the Intrusion Detection System (IDS). Execution of such strategies aims to protect and defend the Target Application against adversaries.

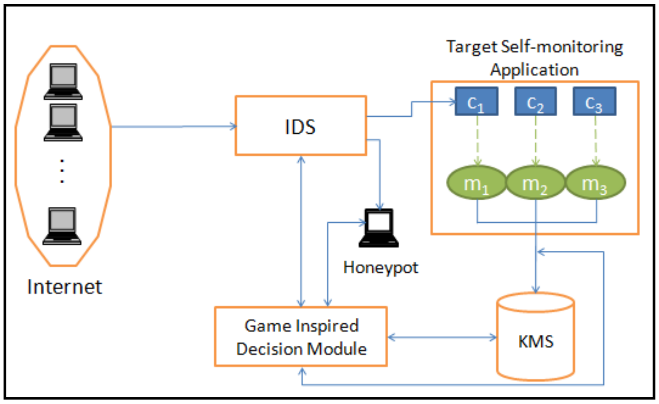
Target Self-monitoring Application
c_1
c_2
c_3
m_1
m_2
m_3
IDS
Honeypot
Internet
Game Inspired Decision Module
KMS

Figure 2. Game Inspired Defense Architecture

We now discuss the several components used by GIDA and explain their functionality and purpose for accomplishing the aim of providing robust security for target systems.

We begin with a brief introduction of the basic game theoretic concepts and explanation of our recent work on implementation of game theoretic models in the domain of cyber security.

A. Imperfect Information Stochastic Game

We recently proposed two game theory models to address some of the challenging cyber security issues. We model the strategic interactions between the attacker and defender as a competitive game played among them. The concept of a solution for such games as per game theory is captured by the Nash equilibrium which prescribes a strategy S_p for each player p, such that any player p deviating from S_p would receive a lower payoff, if the others adhere to their prescribed strategies.

The first model uses static and dynamic games and is specific to the class of DDoS attacks and their potential countermeasures Wu et al. [14] while the second model is based on an imperfect information stochastic game which fits to the generic cyber security scenario. Below we briefly review our stochastic game model whose details are available in Shiva et al. [10].

Prior stochastic game models for network security [4] assume that the players have perfect information about the current state of the game, which implies that the defender is always able to detect an attack and the attacker is always aware of the employed defense mechanism. In real systems, a player uses a sensor (e.g., the defender's sensor can be a part of the Intrusion Detection System (IDS)) to observe the current status of the system to decide the strategy. It is widely believed that no real sensor can perfectly read the environment, i.e., usually there is a non-zero error probability. So, in most cases, the above assumption about perfect information does not hold in real life. We relaxed this assumption and designed a stochastic game model which is able to capture more realistic scenarios. It considers that a player knows the system's true state at a particular moment with some error probability, i.e., at any given point in time the true state and a player's perception can be potentially different. With this additional constraint of imperfect information, we computed the best strategy for a player considering other players' choice of possible strategies. We have validated our theoretical results via simulation experiments in MATLAB.

Results obtained by our prior work [10, 14] in this domain of game theory become the foundation for our holistic security approach. We aim to extend our game theoretic models to also take input from the monitoring performed over execution of arbitrary software in a target system for securing the same. We also intend to use a knowledge management system as part of our decision making process to further enhance the quality of our suggested defense solutions. The following subsection illustrates how we intend to use software monitoring in our architecture.

B. Software Monitoring

Monitors can either be embedded along with the application code or can be separated and placed away from the application code. Monitors developed using monitoring tools will provide users flexibility to specify software properties to be monitored using logical formalisms. Monitors generated from formal specifications are then used to verify the execution of the program behavior.

Monitors thus present in the innermost two layers will be responsible for notifying GIDM about the behavioral changes of the software that could indicate an attack. Once GIDM performs a decision analysis on the probability of attack, it informs the monitor of the appropriate action to take to minimize the damage to the application software. This information is also transferred to the KMS for appropriate attack classification. This approach to self-checking software enables verification of control flow towards an applicable output for defense measures.

C. Knowledge Management System

Simmons et al. [12] proposed a cyber-attack taxonomy called AVOIDIT that classifies attack vectors to assist defenders with disseminating defense strategies. Five major classifiers are used to characterize the nature of an attack, which are classification by attack vector, classification by attack target, classification by operational impact, classification by informational impact, and classification by defense. It is presented in a tree-like structure to neatly classify attack vectors and common vulnerabilities used to launch cyber-attacks.

The proposed cyber-attack taxonomy is used as a repository schema for a knowledge management system (KMS). The KMS is a component within the game inspired decision model that captures monitoring related data from the inner layers in an attempt to classify an attack and output to GIDM for decision analysis.

The KMS is used for regenerating the consummate path to an attack for propagating appropriate defenses. Notification is sent to GIDM, which investigates the applicability of determining the action space of the defender and attacker. Integrating attack information into the GIDM allows game agents to locate data easier for the most relevant defense method. This approach towards attack classification and defense dissemination provides seamless transfer of knowledge for our holistic security approach.

IV. Related Work

Achieving greater security involves the integration of assorted tools necessary for a comprehensive solution Amer and Hamilton [1]. A holistic security approach is a complex problem necessary to understanding the appropriate transfer of information. Ye and Farley [15] illustrate a *attack-norm* approach which is aimed at efficient attack identification. Execution of their model uses multiple tools for performing functions like data screening, feature extraction, characteristic modeling, sensing and decision making for separating attack signals from normal data before attack identification which leads to improved performance.

Bhatia et al. [2] proposed multi-layer cyber-attack detection through honeynet. They emphasize on the need to replace single layer detection technology with multi-layer detection. Ulieru [13] proposed a model evaluating holistic security ecosystems in accordance with reacting to information technology related to emergency responses. The research investigates a holistic approach to cross-organizational workflow coordination and decision making. This provides great insight into the development of a holistic security approach to cyber security.

The recent acquisition made by Intel [3] of security firm MacAfee implies the importance of holistic security where monitoring of both hardware and software together can better respond to threats.

Liu et al. [8] presented a methodology to model the interactions between a DDoS attacker and some defense mechanism such as 'pushback'. Roy et al. [9] surveyed existing game theoretic solutions designed to enhance network security. They emphasized that game theory has the advantage of treating explicitly intelligent decision makers having divergent interests.

Amer and Hamilton [1] proposed an inclusive up-to-date intrusion detection system (IDS) taxonomy, which provide insight into the characteristics of an IDS to tailor one which best suits the security needs of organizations and developers. Mirkovic and Reihner [5] offered a comprehensive taxonomy of DDoS attack and defense mechanisms in aim to classify attacks and defense strategies.

V. Conclusion and Future Work

In this paper we presented a holistic security approach which provides a multi-layer framework to achieve an optimal level of security. GIDA focuses on use of security monitoring tools to observe deviations in the function of software and hardware, a KMS for classifying attacks, and a game decision module for deciding the best defense strategy based on captured information.

Our experimentation [10, 14] included modeling and simulation of game theory-based solutions against DoS and DDoS attacks. In future work, we aim to extend the functionality of such previously proposed game models by incorporating them in architectures like GIDA for addressing a broader array of cyber and data engineering problems. We also aim to use attack test-beds like DETERLAB to further investigate the efficiency of our proposed holistic security approach.

References

[1] Amer, S., Hamilton, J., "Intrusion Detection Systems (IDS) Taxonomy – A Short Review", Defense Cyber Security, 13 (2), June 2010.

[2] Bhatia, J., Sehgal, R., Bhushan, B., Kaur, H., "Multi Layer Cyber Attack Detection through Honeynet", New Technologies, Mobility and Security, NMTS '08, November 2008.

[3] Darling, P. (2010). Intel to Acquire McAfee. Oct 27, 2010. http://newsroom.intel.com/community/intel_newsroom/blog/2010/08/19/intel-to-acquire-mcafee.

[4] Lye, K., and Wing, J., 2005. "Game strategies in network securit", Intnl J. of Information Security 4 (02): 71--86.

[5] Mirkovic, J., and Reiher, P., "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", In ACM CCR (April 2004).

[6] Kranitis, N., Paschalis, A., Gizopoulos, D., Xenoulis, G., "Software Based Self-Testing of Embedded Processors", IEEE Transactions on Computers, Vol 54, No.4, April 2005.

[7] Delgado, N., Gates, Q., Roach, S., "A Taxonomy and Catalog of Runtime Software-Fault Monitoring Tools", IEEE Transactions on Software Engineering, Vol. 30, No. 12, December 2004.

[8] Liu, P., Zang, W., and Yu, M., "Incentive-based modeling and inference of attacker intent, objectives, and strategies", *ACM Transactions on Information and System Security (TISSEC).* 2005.

[9] Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., Wu,Q., "A Survey of Game Theory as Applied to Network Security", *HICSS 43* Hawaii International Conference on System Sciences, 2009.

[10] Shiva, S., Roy, S., Bedi, H., Dasgupta, D., and Wu, Q. 2010. "An Imperfect Information Stochastic Game Model for Cyber Security", The 5th Intnl Conference on i-Warfare and Security.

[11] Shiva, S., Roy, S., Dasgupta, D., "Game theory for cyber security", Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, 2010.

[12] Simmons, C., Shiva , S., Dasgupta , D., and Wu, Q., "AVOIDIT: A cyber attack taxonomy,", Technical Report: CS-09-003, University of Memphis, August 2009.

[13] Ulieru, M., "A Complex Systems Approach to the Design and Evaluation of Holistic Security Ecosystems", International Conference on Complex Systems, 2007

[14] Wu, Q., Shiva, S., Roy, S., Ellis, C., and Datla, V. 2010. "On Modeling and Simulation of Game Theory-based Defense Mechanisms against DoS and DDoS Attacks", SpringSim.

[15] Ye, N., & Farley, T. (2005). "A scientific approach to cyberattack detection", *Computer , 38*, 55--61.