International Journal of Information Technology and Management

Vol. IX, Issue No. XIII, August-2015, ISSN 2249-4510

AN ANALYSIS ON A FRAMEWORK OF MODELING AND SIMULATION FOR CYBER SECURITY: DEVELOPMENT AND APPLICATIONS

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

International Journal of Information Technology and Management
Vol. IX, Issue No. XIII, August-2015, ISSN 2249-4510

An Analysis on a Framework of Modeling and Simulation for Cyber Security: Development and Applications

Hemant Kumar Narayanbhai Patel[1] Dr. Jigar Patel[2]

[1]Research Scholar, Mewar University, Chhitorgrah. India

[2]Associate Professor, Kalol Institute of Management, GTU, Gujarat, India

Abstract – With the increasing occurrence of various cyber-attacks such as distributed denial of service (DDoS) and worm attacks, simulations are being used to develop security techniques and policies against such attacks. In a cyber-security environment, there are many entities that have different resources and behaviors; attack and defensive behaviors are exhibited upon interaction with other entities. In order to design simulation models for various cyber-security simulations, not only a generalized model that can represent various attacks and target entities but also a modeling method that considers different types of interactions between entities to make simulation models should be developed. In this paper, we describe a modeling methodology for the cyber-security simulation based on discrete event system specification (DEVS) formalism.

This paper describes a new hybrid modeling and simulation architecture developed for understanding and developing protections against and mitigations for cyber threats upon control systems. It first outlines the challenges to PCS security that can be addressed using these technologies. The paper then describes Virtual Control System Environments (VCSE) that use this approach and briefly discusses security research that Sandia has performed using VCSE. It closes with recommendations to the control systems security community for applying this valuable technology.

Computer networks are now relied 011 more than ever before for gathering information and performing essential business functions. I11 addition, cyber-crime is frequently used as a means of exploiting these networks to obtain useful and private information. Although intrusion detection tools are available to assist in detecting malicious activity within a network, these tools often lack the ability to clearly identify cyber-attacks. This limitation makes the development of effective tools an imperative task to assist in both detecting and taking action against cyber-attacks as they occur. In developing such tools, reliable test data must be provided that accurately represents the activities of networks and attackers without the large overhead of setting up physical networks and cyber-attacks. The intent of this paper is to use operation research and simulation techniques to provide both data and data-generation tools representative of real-world computer networks, cyber-attacks, and security intrusion detection systems. A simulation model is developed to represent the structure of networks, the unique details of network devices, and the aspects of intrusion detection systems used within networks. The simulation is also capable of generating representative cyber-attacks that accurately portray the capabilities of attackers and the intrusion detection alerts associated with the attacks. To ensure that the data provided is reliable, the simulation model is verified by evaluating the structure of the networks, cyber-attacks, and sensor alerts, and validated by evaluating the accuracy of the data generated with respect to what occurs in a real network.

----------X----------

INTRODUCTION

With the large scale expansion of network connectivity, there has been a rapid increase in the number of cyber-attacks on corporations and government offices resulting in disruptions to business operations, damaging the reputation as well as financial stability of these corporations. The recent cyber-attack incident at Target Corp illustrates how these security breaches can seriously affect profits and shareholder value. According to a report by Secunia[1], the number of reported security vulnerabilities in 2013 increased by 32% compared to 2012. However in spite of these increasing rate of attacks on corporate

and government systems, corporations have fallen behind on ramping up their defenses due to limited budgets as well as weak security practices. One of the main challenges currently faced in the field of security measurement is to develop a mechanism to aggregate the security of all the systems in a network in order assess the overall security of the network. For example INFOSEC [2] has identified security metrics as being one of the top 8 security research priorities. Similarly Cyber Security IT Advisory Committee has also identified this area to be among the top 10 security research priorities.

In addition, traditional security efforts in corporations have focused on protecting key assets against known threats which have been disclosed publicly. But today, advanced attackers are developing exploits for vulnerabilities that have not yet been disclosed called "zero-day" exploits. So it is necessary for security teams to focus on activities that are beyond expected or pre-defined. By building appropriate stochastic models and understanding the relationship between vulnerabilities and their lifecycle events, it is possible to predict the future when it comes to cybercrime such as identifying vulnerability trends, anticipating security gaps in the network, optimizing resource allocation decisions and ensuring the protection of key corporate assets in the most efficient manner.

In this paper, we propose a stochastic model for security evaluation based on Attack Graphs, taking into account the temporal factors associated with vulnerabilities that can change over time. By providing a single platform and using a trusted open vulnerability scoring framework such as CVSS[4-6], it is possible to visualize the current as well as future security state of the network leading to actionable knowledge. Several well established approaches for Attack graph analysis [7-15] have been proposed using probabilistic analysis as well as graph theory to measure the security of a network. Our model is novel as existing research in attack graph analysis do not consider the temporal factors associated with the vulnerabilities, such as the availability of exploits and patches. In this paper, a nonhomogeneous model is developed which incorporates a time dependent covariate, namely the vulnerability age. The proposed model can help identify critical systems that need to be hardened based on the likelihood of being intruded by an attacker as well as risk to the corporation of being compromised.

The nation is greatly and appropriately concerned with computer and network vulnerabilities and the threats they pose to our infrastructures. Presidential-level concern dates back to 1998 (PDD-63). Public accounts of malicious attacks on supervisory control and data acquisition (SCADA) and distributed control systems (DCS) are appearing with increasing frequency. This paper describes advances Sandia has made in the science of protecting these cyber-physical systems.

The computer aspects of cyber-physical systems are much like traditional Information Technology (IT) systems. Similarities include the use of Transmission Control Protocol (TCP) and Internet Protocol (IP) over Ethernet, the use of standard Personal Computers (PCs) running mainstream operating systems for engineering workstations and control interfaces, and the use of IT network devices such as switches and routers. They also share vulnerabilities such as network protocols that are too trusting, software stacks with buffer overflows, indirect connectivity to the Internet, unsecured product cycle issues, and authentication control. At the surface, the technical differences seem mild. Differences include computer and network configurations, applications software, data exchange characteristics including timing issues, and unique end point devices.

Though similar in many respects, cyber-physical systems are different from IT systems, and, from a security perspective, they are dramatically different. Cyber-attacks on physical systems can lead to serious consequences including product loss, damage, injury and death. Adversaries may need to make many unique technical steps to achieve these consequences. Operators might need to perform complex procedures to bring attacked physical systems to a safe state. As a result, defenders must be attuned to the unique patterns of these attacks so that they can defend against them and they must be attuned to the physicality of the systems so that they can respond appropriately. Addressing these differences drive the work behind this report.

CYBER-SECURITY ANALYTICS FRAMEWORK

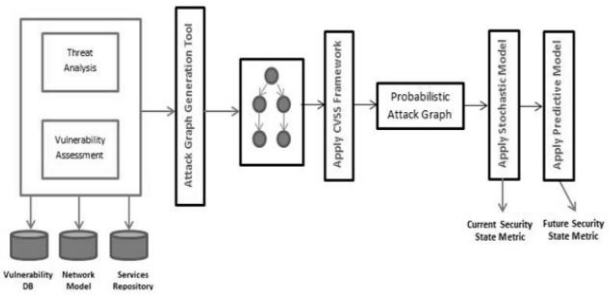

Figure 1. Cyber Security Analytics Framework

In this paper, we explore the concept of modeling the Attack graph as a stochastic process. In [40, 41], we established the cyber-security analytics framework (Figure 1) where we have captured all the processes involved in building our security metric framework. By providing a single platform and using an open vulnerability scoring framework such as CVSS it is possible visualize the current as well as future security state of the network and optimize the necessary steps to harden the enterprise network from external threats. In this paper we will extend the model by taking into account the temporal aspects associated with the individual vulnerabilities. By capturing their interrelationship using Attack Graphs,

we can predict how the total security of the network changes over time. The fundamental assumption we make in our model is that the time-parameter plays an important role in capturing the progression of the attack process. Markov model is one such modeling technique that has been widely used in a variety of areas such as system performance analysis and dependability analysis [11, 27, 42-43]. While formulating the stochastic model, we need to take into account the behavior of the attacker. In this paper, we assume that the attacker will choose the vulnerability that maximizes his or her probability of succeeding in compromising the security goal.

State Based Stochastic Modelling - State-space stochastic methods enable the probabilistic modeling of complex relationships and dependencies between known and latent variables. Several research fields have long used Modeling and Simulation to study the behavior of a system under different varying conditions. By applying the same methodology in the area of security enables an IT security administrator to assess the current security state of the entire network as well as predict how this state will change based on new threat levels, new vulnerabilities etc. Another capability is analyzing what-if scenarios to calculate metrics based on making certain changes to system. Most IT departments are faced with limited budgets and hence applying patches to all systems in a timely manner may not be feasible. Hence it is necessary to optimize the application of such security controls without compromising the network or disrupting business operations.

Architecture - Figure 2 shows a high level view of our proposed cyber security analytics architecture which comprises of 4 layers where each layer builds upon the previous one below.

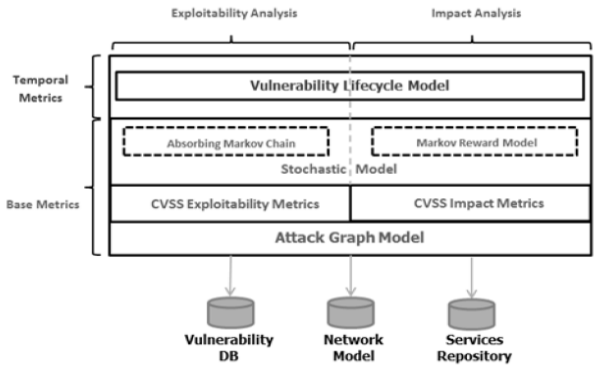

Figure 2. Cyber Security Analytics Architecture

Layer 1 (Attack Graph Model): The core component of our architecture is the Attack Graph Model which is generated using a network model builder by taking as input network topology, services running on each host and a set of attack rules based on the vulnerabilities associated with the different services.

Layer 2 (CVSS Framework): The underlying metric domain is provided by the trusted CVSS framework which quantifies the security attributes of individual vulnerabilities associated with the attack graph. We divide our security analysis by leveraging two CVSS metric domains. One captures the exploitability characteristics of the network and the other analyzes the impact a successful attack can have on a corporations key assets. We believe that both these types of analysis are necessary for a security practitioner to gain a better understanding of the overall security of the network.

Layer 3 (Stochastic Model): In this layer relevant stochastic processes are applied over the Attack Graph to describe the attacks by taking into account the relationships between the different vulnerabilities in a system. For example, in our approach, we utilize an Absorbing Markov chain for performing exploitability analysis and a Markov Reward Model for Impact analysis. In [40, 41] we discussed how we can model an attack-graph as a discrete time absorbing Markov chain where the absorbing state represents the security goal being compromised.

So far we have been focusing on the security properties that are intrinsic to a particular vulnerability and that doesn't change with time. These measures are calculated from the CVSS International Journal of Computer Networks & Communications (IJCNC) Vol.7, No.1, January 2015 7 Base metric group which aggregates several security properties to formulate the base score for a particular vulnerability.

Layer 4 (Vulnerability Lifecycle Model): In order to account for the dynamic/temporal security properties of the vulnerability, we apply a Vulnerability Lifecycle model on the stochastic process to identify trends and understand how the security state of the network will evolve with time. Security teams can thus analyze how availability of exploits and patches can affect the overall network security based on how the vulnerabilities are interconnected and leveraged to compromise the system.

CYBER-SECURITY MODELING AND SIMULATION

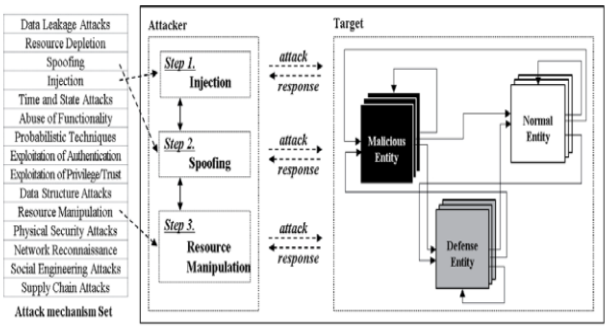

Figure 3. A cyber-security environment and components.

There are various mechanisms of cyber-attacks, each of which can be composed of two or more mechanisms. As shown in figure 3, an attacker interacts step by step with a target composed of various entities; the result of each step can be a critical factor that determines the final result. With regard to the target, entities have different responses to an attack depending on their inherent characteristics, such as vulnerability and capability to defend or attack. In addition, these characteristics can be changed as the attack progresses. Therefore, it is necessary to develop a simulation model that can observe interactions between an attacker and a target as well as represent various attack mechanisms and characteristics of targets.

A cyber-security simulation can be modeled using a modeling methodology for discrete event system, because the simulation progresses based on the interactions that have occurred during attack events. Using this methodology, we can trace changing state variables of an attacker and the target models during the simulation. In this study, we use the discrete event system specification (DEVS) formalism for the modeling, and suggest a method for developing a DEVS atomic model considering various characteristics of entities and their interactions.

DEVS MODELING OF CYBER-SECURITY SIMULATION-

Attributes of entities can be classified into physical and behavioral attributes. All entities can have physical attributes such as identification and resources, whereas behavioral attributes can be found in entities that can trigger events. In this paper, we define two types of entities, *subject* and *target*.

- *Subject* – an active entity that can manipulate other entities, *e.g.*, thread, process, system, and network.
- *Target* – a passive entity that can only be manipulated by a *subject*, *e.g.*, application, file, code, command, etc.

In the behavioral attributes of figure 4 (a), *intention* and *target* denote a characteristic and the target in the event, respectively. In addition, the *action*, an attribute of *behavior,* denotes event types; changing the value of *action* corresponds to a change of events.

We can develop an atomic model by considering the location of the *target* of a *subject* and whether the *target* is shared by other *subjects*. As shown in (b) of figure 4, if each *target* of *subject 1* and *subject 2* is located in itself, it can act as an atomic model and its events can be scheduled by that *subject.* Schematic (c) of figure 4 shows a situation where an entity can be both the *target* and the *subject*. In this situation, the *target* of *subject 2* is shared with *subject 1*. Finally, (d) shows a *target* entity located out of *subjects* that is shared by more than two *subjects*. As demonstrated using (c) and (d), an atomic model can be composed of multiple entities, and in order to schedule events considering the results of interactions between entities in the atomic model, state mapping between the model and entities is needed.

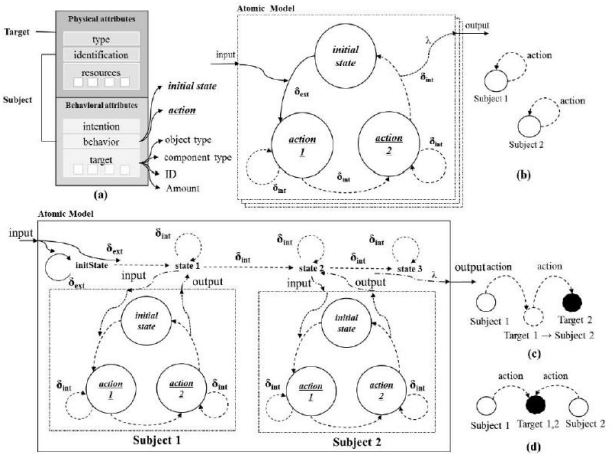

Figure 4. Modeling of a DEVS Atomic model considering the location of target and resource sharing.

LITERATURE REVIEW

There are three primary areas of research related to the problem being addressed, which include the modeling and classification of cyber-attacks, the simulating of computer networks, and the use of information fusion techniques in the cyber domain. Although there is some overlap between these topics, the combination of all three has only recently gained attention. Therefore, there is a great deal of opportunity in identifying some of the leading issues across these fields and providing a methodology that effectively addresses these issues.

Modeling and Classification of Cyber Attacks - An effective means to understanding cyber-attacks is through classifying the attacks and modeling the attack progression. This involves carefully observing the actions associated with a known attack to gain an understanding of the attacker behavior.

Fortunately, there has been significant progress made in modeling attacks.

Dougherty and Gonslaves (2007), for instance, developed an adaptive cyber-attack modeling system to assist in testing software protection. Previously, a team of subject matter experts (SMEs) were required to mimic the actions typically associated with hacker attacks in order to evaluate and validate their software protection methodology. This method, though, adds significantly to the cost and time required for
such a project, and the method is not really appropriate for the large numbers of scenarios which need to be thoroughly tested. The research performed by Dougherty and Gonslaves found that developing accurate models of cyber-attacks had the potential to substantially reduce the cost and time required.

Cheung. Fong, and Lindqvist (2006)developed a project called “Correlated Attack Modeling” (CAM) where attack scenarios are modeled by observing actual IDS alerts. These IDS alerts can generally be associated with a specific attack step (usually an exploit of some sort). Although this allows for actual attacks to be used in developing attack patterns, many IDS alerts could be false positives and thus affect the modeling process.

Holdender, Stotz. and Sudit (2008)developed a graph-based template that makes use of graph theory techniques to designate
what types of attack actions or exploits are necessary before other certain types can be performed.

Simulation of Computer Networks - When simulating the progression of attacks through a network and in generating
typical IDS alerts within a network, providing a simulated network structure to work with is a necessity. Even though these processes could be established on a physical network, the large overhead costs and long testing times make such an arrangement highly undesirable. Furthermore, covering the large variety of network semps and sizes with physical means is nearly impossible. Simulation modeling allows for numerous semps and significant structural changes to be made quickly.

Garg, Kwiat, and Upadliyaya (2011) developed a framework (known as SimCo) for measuring the capabilities of security mechanisms in detecting attacks. Inaccuracies among intrusion detection systems and other security systems can have a significant impact on organizations: thus, identifying where flaws lie within such systems is crucial.

DeLooze et al. (2004) have also developed a simulation methodology to model the combination of cyber-attacks and security systems. They developed a simulation model called “The Virtual Network Simulation” to assist in education and training courses for individuals pursuing careers in network security. The simulation model developed includes a vast amount of network devices (including IDSs) that can be setup
at the user's discretion, and the model interjects simulated attacks into these networks. However, since this system is semp as a training tool, the model requires consistent interaction with an individual to monitor, make adjustments to. and handle problems occurring within the simulated network. Therefore, this tool is also not well designed for data generation associated with the attacks and IDS alerts.

MODELING INTENTIONS AND MODEL OVERVIEW

The overall goal of developing this cyber-attack simulation model is to create an application that can generate valid intrusion detection system alerts in a virtual network representative of a real private network. With the cyber-attack simulator, a user can create or load a specific network topology, specify the vulnerabilities of the network,
create and run attack scenarios, and view sensor alert data produced. Several inputs and outputs are necessary to the functionality of the simulator. A diagram depicting the types of inputs and outputs is displayed in Figure 5.

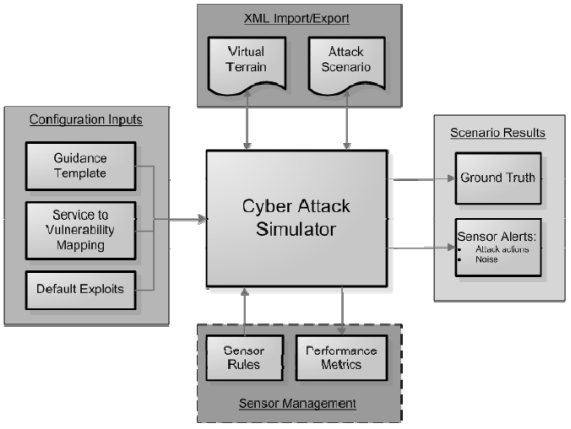

Figure 5: Cyber Attack Simulator Functionality.

As is shown in Figure 5. the simulator consists of three primary categories of inputs and outputs: configuration inputs. XML imports and exports, and scenario results. A sensor management add-on. developed by McConky (2007) is also shown.

The configuration inputs include data that is loaded from files as the simulator is opened. The guidance template file is a directed graph that indicates what sequence of stages can be used in an attack and what categories of exploits are included in each stage. This information is used when attacks are generated based on a set of parameters.

Another file includes the service to vulnerability mappings, which maps a machine service to a set of vulnerabilities through the use of seivice IDs and vulnerability IDs. This effectively indicates what exploits can be executed on a machine that is running a certain seivice. The default exploits file loads a database of known exploits (also referred to as available actions) that the simulator can choose and filter from. This database of actions is used by the simulator when creating the individual steps of an attack as well as when creating the noise (or false-positives) that occurs during an attack scenario.

CONCLUSION

In this paper, we presented a non-homogenous Markov model for quantitative assessment of security attributes. Since existing metrics have potential short-comings for accurately quantifying the security of a system with respect to the age of the vulnerabilities, our framework aids the security engineer to make a more realistic and objective security evaluation of the network. What sets our model apart from the rest is the use of the trusted CVSS framework and the incorporation of a well-established Vulnerability lifecycle framework, to comprehend and analyze both the evolving exploitability and impact trends of a given network. We used a realistic network to analyze the merits of our model to capture security properties and optimize the application of patches.

The functionality of the network model and the attack simulation are verified and validated through some different approaches. Several of the network modeling features, including the connector level structure, subnet implementation, machine sendee representation, and connector firewall permissions, are verified through the use of conditional statements and temporary debugging output. Other network features are visually (or graphically) verified through observation of the resulting network model. Such features include the connection links. IP addresses, saving process, and virtual terrain exportation. The attack simulation features are verified using a unique approach for each feature.

REFERENCES

- Agents in Internet". Proceedings 19th European Conference on Modelling and Simulation, 2005.
- B.P. Zeigler et el., Theory of Modeling and Simulation. 2nd edition, Academic Press, 2000.
- Cheung, S.. Fong. M.W., & Lindqvist, U. (2006). Modeling Multistep Cyber Attacks for Scenario Recognition. Proceedings of the Third DARPA Information Survivability Conference and Exposition, 1, 284-292.
- DeLooze, L.L.. Graig, C., McKean. P., & Mostow, J.R. (2004). Incorporating Simulation into the Computer Security Classroom. IEEE, 34.
- Dougherty. E.T., & Gonslaves, P.G. (2007). Adaptive Cyber Attack Modeling System. Proceedings of SPIE, 6201.
- Garg. A.. Kwiat, K.. & Upadhyaya, S. (2011). Attack Simulation Management for Measuring Detection Model Effectiveness. Department of Computer Science and Engineering at Stony Brook University
- Holender. M.. Stotz. A.. & Sudit. M. (2008). Situational awareness of coordinated cyber-attacks. Proceedings of The International Society for Optical Engineering, Orlando. April 2005.
- Innacio J. Martinez-Moyano et el., "Modeling behavioral considerations related to information security". Computers and Security, vol. 30, pp. 397-409, 2011.
- L. Wang, A. Singhal, and S. Jajodia, "Toward measuring network security using attack graphs," in Proceedings of the 2007 ACM workshop on Quality Protection, pp. 49-54, 2007.
- McConky. K. T. (2007). Design and Analysis of Information Fusion. Dynamic Sensor Management Rules for Cyber Security Systems Using Simulation. Unpublished Masters of Science Thesis for Rochester Institute of Technology. Rochester.
- R. Ortalo, Y. Deswarte, and M. Kaaniche, "Experimenting with quantitative evaluation tools for monitoring operational security," IEEE Transactions on Software Engineering, vol. 25, pp. 633–650, September 1999.
- Secunia Vulnerability Review 2014: Key figures and facts from a global IT-Security perspective, February 2014
- W.Li and R. Vaughn, "Cluster security research involving the modeling of network exploitations using exploitation graphs," in Sixth IEEE International Symposium on Cluster Computing and Grid Workshops, May 2006.