Agent-based Simulation for Assessing Network Security Risk due to Unauthorized Hardware

Neal Wagner, Richard Lippmann, Michael Winterrose, James Riordan, Tamara Yu and William W. Streilein
MIT Lincoln Laboratory
244 Wood Street
Lexington, MA 02420, USA
{neal.wagner, lippmann, michael.winterrose, james.riordan, tamara, wws}@ll.mit.edu

Keywords: Agent-based simulation, cyber security, risk assessment, network threat

Abstract

Computer networks are present throughout all sectors of our critical infrastructure and these networks are under a constant threat of cyber attack. One prevalent computer network threat takes advantage of unauthorized, and thus insecure, hardware on a network. This paper presents a prototype simulation system for network risk assessment that is intended for use by administrators to simulate and evaluate varying network environments and attacker/defender scenarios with respect to authorized and unauthorized hardware. The system is built on the agent-based modeling paradigm and captures emergent system dynamics that result from the interactions of multiple network agents including regular and administrator users, attackers, and defenders in a network environment. The agent-based system produces both metrics and visualizations that provide insights into network security risk and serve to guide the search for efficient policies and controls to protect a network from attacks related to unauthorized hardware. The simulation model is unique in the current literature both for its network threat model and its visualized agent-based approach. We demonstrate the model via a case study that evaluates risk for several candidate security policies on a representative computer network.

1. INTRODUCTION

In today's highly-connected world, computer networks are ubiquitous in systems that make up the critical infrastructure of any state or region. All sectors of critical infrastructure rely on secure computer networks to function properly. These critical networks are under a constant threat of cyber attack as evidenced by documented attacks against US companies across a wide range of critical-infrastructure-dependent industries including the transportation, financial services, energy, agriculture, telecommunications, and healthcare industries [1]. One common network attack targets unauthorized devices and hardware present on a network [2]. Such devices are more susceptible to attack because they are unmanaged or ill-managed and thus, more likely to contain vulnerabilities. Additionally, unauthorized devices may already be compromised when attached to the network and used as a foothold to compromise other network devices.

To protect networks, administrators must anticipate the various types of cyber attacks available, measure a network's susceptibility to these attacks, and put in place safeguards to stop them or mitigate their impact. However, strategies of network attack and defense are highly specific to the network environment in which they are executed and in general there are numerous scenarios that must be considered. The cost of testing these multiple scenarios for real-world systems is oftentimes prohibitive [3]. Thus, evaluation and selection of effective network policies and defense mechanisms is quite difficult and often left to the subjective judgment of network administrators.

Modeling and simulation seeks to remedy this problem by allowing for testing of multiple environment-specific scenarios at low cost. Agent-based systems use a computational model of autonomous agents that interact with each other and their environment. Such systems use a "bottom-up" modeling approach in which system control is decentralized and governed only by the behavior of the agents [4]. Agent-based modeling is the preferable technique for simulation of complex systems with a large number of active objects (e.g. users, actors, processes, organizational units, etc.) that are dependent on the order/timing of events for the following reasons: (1) it allows for capture and analysis of highly complex dynamics, (2) it can be implemented with little or no knowledge of the global inter-dependencies and/or aggregate effects of the system, and (3) it is easier to build upon as model changes generally require local not global adjustments [4].

This paper presents a prototype visualized agent-based simulation system for network security risk assessment with respect to authorized and unauthorized hardware. The goal of the system is simulate a network environment in which attackers, defenders, and regular and administrator users coexist and interact and allow for multiple scenario testing and evaluation of network security risk. Network administrators can use the system to evaluate candidate configurations of network controls and defense policies in a given network environment at low cost before selecting an appropriate configuration to be implemented on an actual network. Here, the

network security risk associated with a particular scenario is measured by capturing incidents of device compromise. The system is unique in the current literature both for its network threat model which is based on a prevalent critical network control defined by the SANS Institute, specifically Critical Control 1 - Inventory of Authorized and Unauthorized Devices [2], and its visualized agent-based simulation approach. The visual representation of the simulation model allows analysts to see the temporal dynamics of a network environment for a given scenario and illustrates how attack steps succeed or fail with different defensive measures. The visual component of the simulation may also serve to motivate network stakeholders to enforce new security policies by providing a visualization of the relative security risk of a network under varying security policies. The rest of this paper is organized as follows. Section 2. gives a brief review of related work on network security simulation, section 3. describes the simulation model and the decision support system built to utilize it, section 4. demonstrates the system via a case study, and section 5. concludes and discusses future work.

2. RELATED WORK

There exist numerous recent studies investigating various models appropriate for network intrusion detection and prevention. Some recent examples include [5–16]. While these studies employ simulation to explore the efficacy of proposed models for intrusion detection, the focus of these studies is on network situational awareness rather than network simulation.

Studies detailed in [17] and [18] provide agent based simulation studies that are focused on investigative network modeling rather than network situational awareness. An agent-based simulation to analyze a modeled network with respect to a specific network security protocol in order to automatically determine protocol compliance is given in [17]. The study given in [18] provides an agent-based model that integrates the OMNet++ network simulation software package with network libraries INET Framework and ReaSE to investigate cooperative botnet attacks and corresponding defenses.

Studies detailed in [19–21] provide non-agent simulation studies for investigative network modeling. A study that combines discrete event simulation with metaheuristic optimization to simulate network attacks and optimize network defenses is provided in [19]. The study given in [20] proffers a model built using OMNeT++ to simulate distributed denial-of-service attacks on wireless networks. An epidemic model to simulate malware propagation over network devices is provided in [21].

This paper, like the studies of [17, 18], utilizes an agent-based simulation approach for investigative network modeling to better understand network security risk. The main contributions of this work are as follows.

1. We model and simulate a critical network threat defined by SANS [2], specifically attacks exploiting unauthorized hardware.

2. We present a novel visual agent-based simulation decision support tool that can be used by administrators to analyze security risk with respect to this network threat.

3. SIMULATION SYSTEM

A visualized agent-based simulation model is developed to capture network users, administrators, attackers, and defenders and their interactions with each other and the network environment in which they co-exist. The simulation is intended to model the security risk caused by the presence of unauthorized devices on a network. The model is part of a prototype decision support system that aims to investigate varying attack/defense scenarios with respect to unauthorized devices for a given network environment and support network control and defense policy decisions. The decision support system contains three components: (1) the simulation model, (2) the animation used to visualize simulation dynamics, and (3) simulation outputs and metrics computed to capture security risk. The system is built using a combination of Processing 1.5 [22] and Java 1.6. The following sections describe system components.

3.1. Simulation Model

As discussed above, the simulation model is built on the agent-based paradigm in which system control is decentralized and dynamics are driven by the interactions of the various agents with each other and with their environment. The model contains three main submodels: (1) the network attack and defense model, (2) the network environment model, and (3) the network user model. The following sections provide the details of these submodels.

3.1.1. Attack and Defense Model

The attack model considered here is defined by SANS Critical Control 1 (CC1) [2]: it is an attacker who scans a network either internally or externally looking for vulnerabilities present on network devices and is assumed to opportunistically exploit a discovered vulnerability and thereby compromise the device containing the vulnerability. Unauthorized devices are defined as unmanaged or improperly managed devices that are attached to the network.

This threat is illustrated in figure 1. As shown in the figure, unauthorized devices include recently installed test servers, unconfigured switches, laptops that have been off the network for a long time and plugged in without being updated and patched, personal laptops that may be insecure, virtual machines (VMs), and insecure personal devices such as smart phones or music players plugged into desktop computers. A

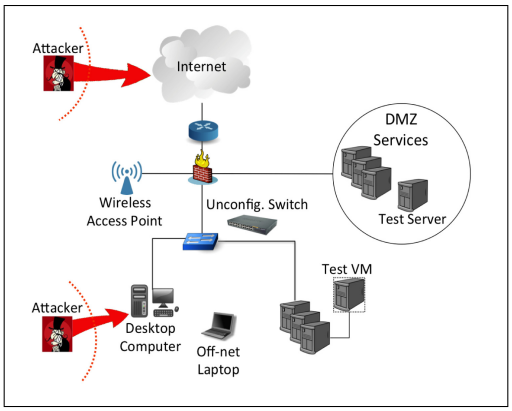

Figure 1. Attack model for unauthorized devices

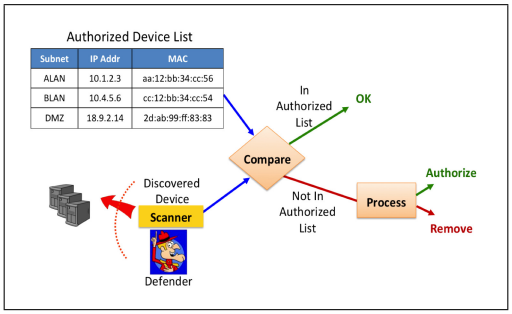

Figure 2. Defense model for unauthorized devices

common situation noted in [23] is for an unconfigured and insecure server to be attached to a network in the afternoon and left on the network overnight before being configured and patched in the morning. Such servers are often compromised overnight by attackers scanning networks looking for insecure servers.

Additionally, unauthorized devices may already be compromised when attached to the network. Whether a vulnerable network device is compromised when attached or compromised after being scanned and exploited by an attacker, it may be used as a foothold to compromise other network devices. Compromised devices seek out other network devices and attempt to exploit them. Attackers may also explicitly target high value devices such as servers and/or system administrator devices.

The defense model considered here is illustrated in figure 2. The defender maintains an inventory of authorized devices (depicted by the table in the upper left area of the figure) and the network is continuously scanned by the defender for new devices (depicted in the lower left area of the figure). New devices that are discovered are compared to the list of authorized devices. Detected authorized devices are allowed. Detected unauthorized devices trigger a remediation process that either authorizes or removes affected devices.

Additionally, the defender may enforce a prevention policy via security protocols, security training, or network access control to prevent unauthorized devices from being attached to the network in the first place.

3.1.2. Network Environment Model

The network model includes a fixed number of "slots" representing the network's available IP address space and each of these slots may be occupied by a network device. The model allows for specification of the number of IP slots available on the network. Network devices are categorized as having relatively high or low vulnerability to attacker exploit. Additionally, network devices are categorized as having relatively high or low asset value, where asset value is a representation of the device's relative value to the network. This is used to model the presence of high value devices such as servers or other devices critical to the organizational mission. The network environment simulates a single network day in which initially there are no devices with active user sessions, users probabilistically arrive and start sessions on devices for some time, and then leave (log out). Active devices communicate with other active devices in the network during the course of their user sessions.

Attackers scan network devices and probabilistically compromise devices based on their vulnerability levels. Compromised devices seek out other network devices to exploit. Defenders scan the network, probabilistically detect unauthorized devices, and, after some processing delay, remove or cleanse such devices. Additionally, unauthorized devices arrive at the network, attempt network connection, and are probabilistically either repelled or allowed to connect. This is used to model the network's organization-wide unauthorized device prevention policy. Unauthorized devices attempting connection may already be compromised when they arrive at the network. Unauthorized devices that are not already compromised have, by definition, high vulnerability levels.

3.1.3. Network User Model

There are two types of network users: regular and administrator users. The model allows for specification of the number of users of each type on the network. Users of both types probabilistically communicate with other active users on the network. Administrator users differ from regular users in that they can be specified to have a higher frequency of communication.

Attackers seek to compromise network devices with active user sessions. Compromised devices probabilistically compromise other devices by sending exploit communications to them with high frequency. Compromised administrator devices infect other non-compromised devices at a higher rate than compromised regular devices do. This is used to model the escalated privileges that administrator users have relative to regular users. Because administrator devices have escalated privileges, attackers may explicitly target such devices.

Table 1. Display of device conditions

Prop. Type	Cntl.	Prop. Val.	Cntl. Val.
Active User	Fill Color	Regular Admin	Blue Green
Asset Value	Shape	High Low	Diamond Circle
Vul. Level	Size	High Low	Large Small
Authorized?	Line Wt.	Yes No	Thin Thick
Compromised?	Line Color	Yes No	Red Black

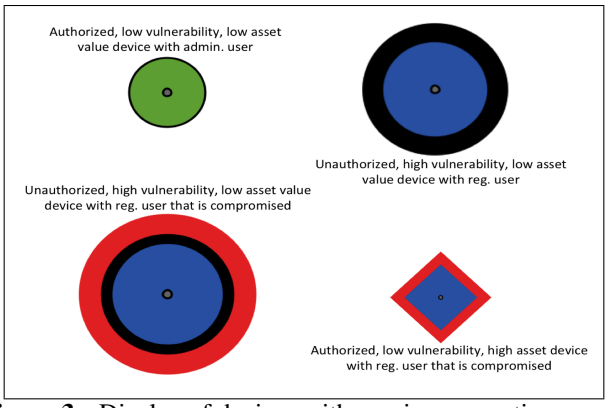

Figure 3. Display of devices with varying properties

3.2. Simulation Animation

The network is visually represented in space by a large white circle containing multiple small black dots representing available IP slots. Devices occupying the network are represented by shapes with varying visual properties. There are several properties that a device can have including the user session type (regular or administrator), the device's asset value (low or high), the device's vulnerability level (low or high), the device's authorization status (authorized or not), and the device's compromised status (compromised or not). These properties are visually represented by changing a device's display size, fill color, shape, line weight, and line color. Table 1 gives the mappings from device properties to visual representations. In the table, the types of device properties are given in the first column, the visual display controls in the second, specific property values in the third, and specific visual display control values in the fourth.

Figure 3 gives the visual displays for example devices with various properties. In the figure, the top left represents an authorized, uncompromised device with low asset value, low vulnerability level, and an administrator user; the top right represents a device that is unauthorized, uncompromised, low value, high vulnerability, and has a regular user; the bottom left represents the same device as depicted in the top right except that it is compromised; the bottom right represents a high asset value device that is compromised and has a regular user. The gray dot in the middle of each device display represents the IP slot that is occupied by that device on the network.

Figures 4—6 show screenshots of a visualized simulation during the course of a run. Figure 4 shows the network environment in an early stage of a particular simulation run. The white circle defines the network boundary and blue and green colored circles inside the boundary represent devices with active user sessions. Colored circles outside the network boundary (upper left of the figure) represent unauthorized devices that have been prevented from attaching to the network due to the network's security policy. The simulation system contains a zoom and pan feature that allows a user to pan to and zoom in on a particular area of the simulation animation. The inset in the lower right of figure 4 is produced by zooming and panning and shows a magnification of a small area of the simulation marked by an oval inside the network boundary. In the inset, the red square encompassing a network device represents an attacker scan and the yellow square encompassing another network device represents a defender scan. Also in the inset, light blue lines represent active communications between two network devices, single dots represent open IP slots that may be occupied by a new network device, and empty circles encompassing a dot represent network devices that have no active user session.

The inset in the lower left of figure 4 is another magnification of a small area of the same simulation run at a later stage in the run. Here, the large blue circle with a thick black border represents an unauthorized device that has penetrated the network boundary. The orange square encompassing the unauthorized device represents that the device has been detected by a defender scan, is currently being processed, and after some processing delay will be removed from the network.

Figure 5 shows the network environment at an early stage of another simulation run with different parameter settings than the run displayed in figure 4. Here it can be seen that six unauthorized devices have penetrated the network, three of which have been compromised by the attacker. The inset in the lower right of the figure is a magnification of the simulation area marked by the oval inside the network boundary and shows one of the compromised, unauthorized devices. Red lines represent infected communications between this compromised device and other uncompromised network devices that may cause infection to spread within the network. As can be seen in the inset, the compromised device has made an infected communication to an administrator device (colored green) in an attempt to compromise it.

Figure 6 shows the same simulation run depicted in figure 5 a few timesteps later. The inset provides a magnification of the same compromised, unauthorized device shown in the in-

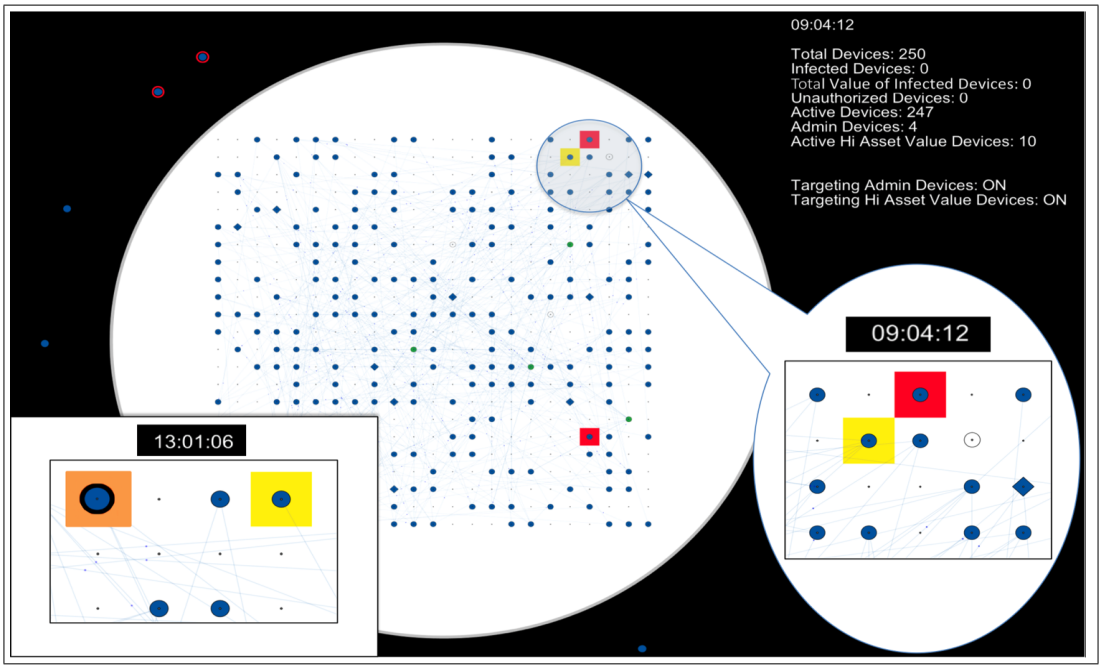

Figure 4. Simulation display at two stages of a particular run

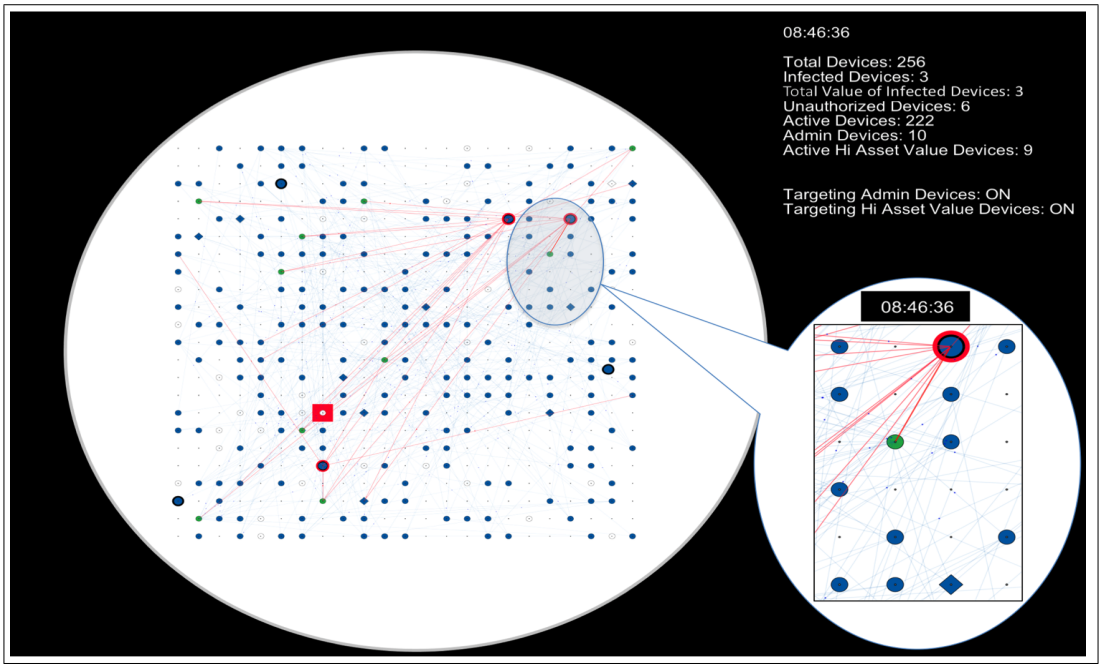

Figure 5. Simulation display at an early stage of another run with different parameter settings

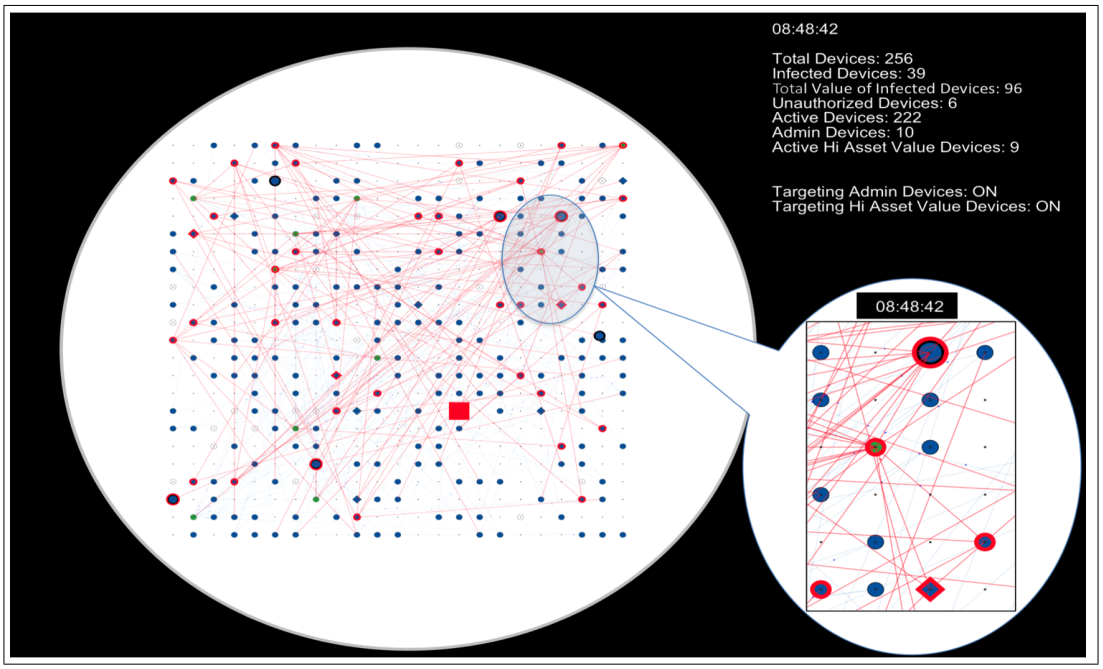

Figure 6. Simulation display corresponding to run from figure 5 a few timesteps later

set of figure 5. Here, it can be seen that the infected device has succeeded in compromising an administrator device (represented by a green administrator device encircled by a red border) and that the administrator device has quickly spread the infection to other devices on the network due to its escalated privileges.

3.3. Simulation Outputs and Metrics

Several simulation outputs are recorded throughout the course of a simulation run. The intent of these outputs is to capture relevant security-related system dynamics and assess network security risk. The following simulation outputs are recorded at each simulation timestep: the total number of devices, the number of active devices, the number of active administrator devices, the number of active high-asset value devices, the number of unauthorized devices, and the number of infected (compromised) devices. From observed simulation outputs, a metric capturing the total value of compromised devices is computed. This represents the relative value of compromised devices on the network corresponding to a given timestep and is given by

$$val_{comp} = \sum_{d \in devices_{comp}} val(d) \tag{1}$$

where d represents a compromised device and varies over all compromised devices currently on the network, $devices_{comp}$ represents the set of all compromised devices, $val(d)$ represents the asset value of compromised device d, and val_{comp} is the total value of compromised devices currently on the network.

The above metric computed at each simulation timestep is aggregated at the end of a simulation run to construct an additional metric: the expected percentage of total network value compromised at any instant in a simulation run. This metric represents the expected portion of the whole value of the network that is compromised at any given moment and is given by

$$E(val_{comp}) = \left[\frac{\sum_{t \in tsteps} \left(\frac{val_{comp}}{val_{total}} \right)}{|tsteps|} \right] \times 100 \tag{2}$$

with

$$val_{total} = \sum_{d \in \text{devices}} val(d). \tag{3}$$

In equation 2, t represents a simulation run timestep and varies over all timesteps in the simulation run, $tsteps$ represents the set of all simulation timesteps, val_{comp} is the weighted value of compromised devices given by equation 1, val_{total} is given by equation 3 and represents the total weighted value of network devices, and $E(val_{comp})$ is the expected percentage of total network value compromised at any instant in the simulation run. Equation 3 is similar to equation 1 with the exception that d represents an authorized network device rather than a compromised device and varies over all authorized network devices.

The following section demonstrates the use of the prototype simulation system via a case study in which security risk

Table 2. Simulation parameters defining network environment and attack threat (static over all experiments)

Parameter	Value
No. of devs.	250
No. of high asset devs.	10
High asset value	20
Defender process delay	5 mins.
Defender detect prob.	1.0
Border attempt freq.	2 per hr.
% unauth. devs. infected	20
Attack scan rate	1 per 2 hrs.
Auth. dev. infect prob.	0.001
Unauth. dev. infect prob.	0.10

is assessed for various security postures of a representative network system.

4. EXPERIMENTS

The intent of this section is to provide examples of how the prototype system can be used by a network security technician or manager to simulate network attacker/defender scenarios and evaluate the corresponding security risk. Table 2 lists simulation parameters and corresponding values that define the representative network environment and attack threat modeled. These parameters are kept constant throughout all experiments conducted. Parameter values are based on a representative network environment for a small to mid-sized organization as described in [24]. From the table parameter "No. of devs." specifies the number of authorized network devices, "No. of high asset devs." specifies the number of network devices that are considered to have high asset value, and "High asset value" specifies the relative value of a high asset device with respect to normal (non-high asset valued) devices. Parameters "Defender process delay" and "Defender detect prob." specify the length of time it takes a defender to process a detected unauthorized device, and the probability that an unauthorized device scanned by the defender will be detected, respectively. Parameters "Border attempt freq." and "% unauth. devs. infected" give the frequency that unauthorized devices will attempt to penetrate the network boundary by attaching to the network and the percentage of these that are already compromised, respectively. Finally, "Attack scan rate," "Auth. dev. infect prob.," and "Unauth. dev. infect prob. give the rate at which attacker scans arrive at network devices, the probability that an authorized device will be infected when scanned by the attacker, and the probability that an unauthorized device will be infected when scanned by the attacker, respectively.

For this study six different network security policies representing six different security postures are modeled for a representative network environment and attack threat. The six security policies are additive in nature, that is, each policy builds on the security posture of the previous policy by incorporating all of its controls and adding a new control or modifying an existing control with the intention of increasing its ability to protect/mitigate attack.

Table 3. Simulation parameters defining security policies (varied by experiment)

Exp. Name	Parameter	Value
Baseline	Def. scan rate	1 per day
	No. of admins.	10
	% unauth. devs. repel	0
Training	(↑) % unauth. devs. repel	80
Admin. policy	(↓) No. of admins.	5
Def. = Att.	(↑) Def. scan rate	1 per 2 hrs.
Def. > Att.	(↑) Def. scan rate	1 per hr.
NAC	(↑) % unauth. devs. repel	96

Table 3 summarizes the security policies investigated and the parameter/value pairs that define these policies. For the baseline experiment, the defender scans the network for unauthorized devices infrequently and no other controls are utilized. Here, the defender scan rate (parameter "Def. scan rate" in the table) is once per day, the number of network administrators is 10, and there is no policy for prevention of unauthorized devices attaching to the network (parameter "% unauth. devs. repel" representing the percentage of unauthorized devices repelled at the network boundary is set to 0). In the next experiment, training is introduced which serves to educate users to not attach unauthorized devices to the network. This is captured by increasing parameter "% unauth. devs. repel" to 80%. The third experiment adds restrictions on the number of administrators allowed on the network. As described in section 3.1.3., administrator devices have escalated privileges and, when compromised, spread infection more rapidly than compromised regular devices do. This policy aims to increase security by decreasing the likelihood that an administrator device is compromised which in turn may reduce the spread of infection throughout the network. This policy is captured by decreasing the number of network administrators from 10 to 5.

The fourth and fifth experiments are concerned with increasing the defender's scan rate. In the fourth experiment ("Def. = Att."), the defender scan rate is increased to equal that of the attacker while for the fifth ("Def. > Att.") the defender scan rate is increased further to exceed the attacker's rate. These two policies are captured by increasing the defender scan rate for network devices to once every two hours and once per hour, respectively. Finally, in the sixth experiment Network Access Control (NAC) is introduced which disallows unauthorized devices from being attached to the network. This is modeled by an increased percentage of unauthorized devices being repelled at the network boundary. It is

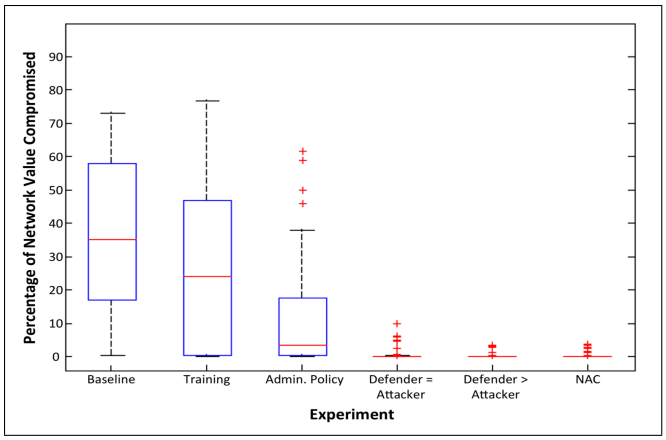

Figure 7. Experimental results

important to note that although NAC will stop all unauthorized devices from be attached in theory, in practice it is not always implemented perfectly and thus some unauthorized devices may still penetrate the network boundary. Thus, parameter "% unauth. devs. repel" is increased to 96% rather than 100% to represent imperfect NAC implementation.

A set of 50 simulation runs is executed for each of the six experiments and results are aggregated over the set and summarized in figure 7. In the figure, the expected percentage of network value compromised, given by equation 2, is visualized via a box plot corresponding to each experiment. The ends of the whiskers on the box plots represent the lowest datum within $1.5 \cdot IQR$ of the lower quartile and the highest datum within $1.5 \cdot IQR$ of the upper quartile where IQR denotes the interquartile range.[1]

From figure 7 it can be seen that each new security control added further reduces the median value (2^{nd} quartile) of the expected percentage of network value compromised relative to the baseline experiment. Additionally, the final experiment which combines all security controls investigated (NAC experiment in the figure) essentially reduces the expected percentage of network value compromised relative to the baseline from 35% to 0%.

Figures 4—6 correspond to simulation runs of two of the above experiments and underscore the benefits of the visualized simulation modeling approach. Figures 5 and 6 correspond to the baseline experiment where no unauthorized device prevention policy is utilized while figure 4 corresponds to the defender $>$ attacker experiment where all of the above security policies are utilized with the exception of NAC. As visualized in figures 5 and 6, a network without good security policy is quite vulnerable to attack as unauthorized devices can penetrate the network, be compromised by an attacker, and spread infection. As can be seen in figure 4, a network in which several network security controls are enforced results in significantly less network compromise as unauthorized devices that do penetrate the network boundary are quickly detected and removed by a defender scan.

As mentioned in section 1., the model's visual representation allows analysts to see the temporal dynamics of a network environment for a given scenario and serves to support understanding of the interactions between network security policy and attack. Specifically, the visual representation allows an analyst to see the stepwise progression of an attack and how it spreads through the network as well as the stepwise progression of the defender's response to the attack. This visually presented information complements the aggregated metrics that are given over the course of a simulation run. As illustrated by the visualizations given in figures 5 and 6, stepping through a simulation run allows an analyst to "see" the specific route an attack took to penetrate the network and then spread throughout the network. For the experiment depicted in the figures, the attack route in this instance was the following.

1. An unauthorized device that is already compromised attaches to the network (i.e. is not repelled by the network's unauthorized device prevention policy).

2. It attempts to spread compromise by sending infected communications to administrator devices on the network.

3. After some number of failed attempts (and no subsequent arrival of a defender scan), it succeeds in infecting an administrator device.

4. Once on the administrator device, it leverages the administrator's escalated privileges to quickly infect several other network devices.

The above experiments motivated three additional experiments that seek to test the effects of security policies that are non-additive, that is policies that employ a single security control in isolation rather than a combination of multiple security controls. The three experiments test the control associated with the defender $=$ attacker, defender $>$ attacker, and NAC experiments, respectively relative to the baseline experiment. The defender $=$ attacker experiment uses the same parameters as in the baseline experiment but increases the defender scan rate to 1 every 2 hours; the defender $>$ attacker experiment increases defender scan rate to 1 per hour, and the NAC experiment uses the baseline defender scan rate (1 per day) but increases the percentage of unauthorized devices repelled to 96%. Using a defender scan rate that is equal to the attacker scan rate results in a median expected percentage of network value compromised of 1.3%, using a defender scan rate that is greater than the attacker's rate results in a percentage of network value compromised of 0.1%, and using NAC

[1] For a detailed description of box plots and their implementations, please see [25].

only results in a percentage of network value compromised of 1.0%.

These results show that using any one of the three tested controls in isolation can significantly decrease network risk. Additionally, utilization of NAC or of a defender scan rate that is the same as the attacker's has approximately equivalent security benefits while employing a defender scan rate that exceeds the attacker's provides the best overall security benefit for a single control.

The above experiments demonstrate how a network administrator can use the proposed system to evaluate many different security controls and combinations of security controls for a modeled network and attack threat before zeroing in on actionable decisions to improve network security with respect to unauthorized hardware on the network.

5. CONCLUSIONS

This paper presents a prototype visualized agent-based simulation system designed to support network risk assessment with respect to authorized and unauthorized hardware. It is intended for use by network administrators to evaluate candidate configurations of network security controls and policies for a given network environment at low cost before selecting an appropriate configuration to be implemented. The system is unique both for its network threat model which is based on SANS Institute Critical Control 1 - Inventory of Authorized and Unauthorized Devices [2], and its visualized agent-based simulation approach which allows analysts to see the temporal dynamics of a network environment for a given scenario and serves to support understanding of the interactions between network security policy and attack.

The system is demonstrated via a case study in which a representative network environment and attack threat are modeled for varying configurations of security controls and policies. Results of the case study indicate that the addition of network controls and policies such as prevention of unauthorized devices attaching to the network, reducing the number of administrators, and increasing the defender scan rate can significantly improve the security posture of the modeled network with respect to unauthorized hardware. These results give an example of one of the benefits of the system, specifically the ability to quantitatively evaluate the efficacy of different network security controls for the protection they provide against vulnerabilities caused by unauthorized devices being attached to the network without having to incur the relatively large expense of testing such controls on a live network. Additionally the visual component of the system is utilized to observe a step-by-step progression of a particular attack in one of the experiments, which exemplifies another benefit of the system, specifically the ability to view temporal interactions between network attack and defense. Visualizations of this type may serve to motivate network stakeholders to enforce new security policies as they allow stakeholders to "see" how attacks can penetrate and spread through a network.

Planned future work for the system includes the addition of new threat models based on other critical network controls defined by SANS such as maintaining an inventory of authorized software and secure hardware/software configurations as well as modeling other common defensive measures such as network address translation and IP masquerading.

6. ACKNOWLEDGMENTS

This work is sponsored by the Department of Homeland Security under Air Force Contract FA8721-05-C-0002. Opinions, interpretations, conclusions and recommendations are those of the author and are not necessarily endorsed by the United States Government.

Biography

The authors are researchers in the Cyber Security and Information Sciences division of MIT Lincoln Laboratory. Their work is focused on developing cyber reasoning and response technologies, performing cyber risk assessment and decision support, and developing systems for cyber situational awareness and command and control.

REFERENCES

[1] Mandiant. Exposing one of china's cyber espionage units. Technical report, Mandiant, 2013.

[2] SANS Institute. SANS Critical Security Controls. http://www.sans.org/critical-security-controls/, 2013.

[3] Sanjay Jain and Charles R. McLean. Components of an incident management simulation and gaming framework. *Simulation*, 84(3), 2008.

[4] Andrei Borshchev and Alexei Filippov. From system dynamics and discrete event to practical agent based modeling. In *The 22nd Intl. Conference of the System Dynamics Society*, July 2004.

[5] F Ali and W Ismail. Network security threat assessment model based on fuzzy algorithm. In *IEEE International Conference on Computer Science and Automation Engineering (CSAE)*, June 2011.

[6] V Anjana and R Bhuvaneswaran. Agent based cross layer intrusion detection system for manet. In *4th International Conference on Advances in Network Security and Applications, CNSA*, July 2011.

[7] J Arokia and K Hunmuganathan. Multi-agent-based anomaly intrusion detection. *Information Security Journal*, 20(4-5):185–193, 2011.

[8] C Bonhomme, C Feltus, and D Khadraoui. A multi-agent based decision mechanism for incident reaction in telecommunication network. In *ACS/IEEE International Conference on Computer Systems and Applications, AICCSA 2010*, May 2010.

[9] L Caiming et al. A distributed surveillance model for network security inspired by immunology. In *Artificial Intelligence and Computational Intelligence. Third International Conference (AICI 2011)*, 2011.

[10] N Jaisankar and A Kannan. A hybrid intelligent agent based intrusion detection system. *Journal of Computational Information Systems*, 7(8):2608–2615, 2011.

[11] N Jaisankar, R Saravanan, and K Durai Swamy. An agent based security framework for protecting routing layer operations in manet. In *1st International Conference on Networks and Communications, NetCoM 2009*, December 2009.

[12] A Ohoussou et al. Autonomous agent based intrusion detection in virtual computing environment. In *IEEE Intl. Conference on Wireless Communications, Networking and Information Security, WCNIS 2010*, June 2010.

[13] J Schafer and M Drozd. Detecting network attacks using behavioural models. In *6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS'2011*, September 2011.

[14] M Sa and A Rath. A simple agent based model for detecting abnormal event patterns in distributed wireless sensor networks. In *International Conference on Communication, Computing and Security, ICCCS 2011*, February 2011.

[15] J Sen. An agent-based intrusion detection system for local area networks. *International Journal of Communication Networks and Information Security*, 2(2):128–140, 2010.

[16] S Stafrace and N Antonopoulos. Military tactics in agent-based sinkhole attack detection for wireless ad hoc networks. *Computer Communications*, 33(5):619–638, 2010.

[17] M Akbarzadeh and M Azgomi. Modeling and analysis of agent-based specifications of security protocols. In *2009 Intl. Conference on Innovations in Information Technology (IIT)*, December 2009.

[18] I Kotenko, A Konovalov, and A Shorov. Agent-based simulation of cooperative defence against botnets. *Concurrency and Computation: Practice and Experience*, 24(6):573–588, 2012.

[19] E Kiesling et al. Simulation-based optimization of information security controls: An adversary-centric approach. In *2013 Winter Simulation Conference*, 2013.

[20] M Malekzadeh et al. Validating reliability of OMNeT++ in wireless networks dos attacks: Simulation vs. testbed. *International Journal of Network Security*, 13(1):13–21, 2011.

[21] O Toutonji, S Yoo, and M Park. Stability analysis of VEISV propagation modeling for network worm attack. *Applied Mathematical Modelling*, 36(6):2751–2761, 2012.

[22] Ben Fry and Casey Reas. Processing 1.5.1. https://www.processing.org/download/?processing, 2011.

[23] R.P. Lippman, J.F. Riordan, T.H. Yu, and K.K. Watson. Continous security metrics for prevalent network threats: Introduction and first four metrics. Technical report, MIT Lincoln Laboratory, 2012.

[24] Jim Hietala. Network Security- A Guide for Small and Mid-sized Businesses. Technical report, SANS Institute, 2005.

[25] M Frigge, D Hoaglin, and B Iglewicz. Some implementations of the boxplot. *The American Statistician*, 43(1):50–54, 1989.