An Integrated Modeling Framework for Application Layer Security

Dr. Uma Kannan, Alabama State University, AL, USA, ukannan@alasu.edu
Dr. Rajendran Swamidurai, Alabama State University, AL, USA, rswamidurai@alasu.edu

Abstract

Cybersecurity is a complex problem. To study the complexity underneath the system and forecast possible future cyber events, we used system dynamics (SD)modeling and simulation.Network operations are normally modeled and simulated using the discrete-event simulation (DES) techniques. Since the primary focus of the DES modeling is packet traffic, the cyberattacks and resulting defenses are viewed from the layer 3 (network layer) of the open system interconnection (OSI) model. This does not discover more harmful attacks that might occur at higher(layer 4 and above) OSI layers. There are 32 million small businesses across the United States and 81 percent of them do not have cybersecurity personnel. Today's extraordinary (COVID-19) situation, application layer (layer 7) security is the key concern for everyone, because every business revenue is heavily dependent on online/always-on presence. Research shows that almost 70 percent of successful cyber attacks are happening at the application layer. This paper presents a new integrated SD modeling framework for the application layer security to help small businesses from cyberattacks.

DOINumber:10.14704/nq.2022.20.8.NQ44936 **NeuroQuantology 2022; 20(8): 9147-9158**

1. Introduction

The Internet is the global system of interconnected networks in the public domain [1]. Cyberspace, which does not exist in any physical form, is a complex environment resulting from the interaction of people, software, and services on the Internet through connected devices and networks [2]. The Internet along with Cyberspace is known as the Cybernetwork. Today, Cybernetworks are an integral part of our homeland like any other physical parts such as cities [3]. With the COVID-19 pandemic, it has become a vital necessity for everyone to do their day-to-day activities and keep in touch with others [4]. International Telecommunication Union 2021 report [4] shows that about 90 percent of people from developed countries and approximately 63 percent of the world's population were using the Internet in 2021, which was a 9 percent increase (during the pandemic) from 2019.

According to the U.S. Small Business Administration Office of Advocacy 2020 report, small businesses comprise 99.9 percent of all firms in the U.S, which is 31.7 million in total [5]. Out of these 25.7 million (81 percent) companies have no employees [5], meaning operated only by the owners and there are no cybersecurity personnel. Today, web applications have become the predominant way of delivering services over the Internet and preferred by billions of people to perform

critical tasks such as banking, healthcare, etc. [6-11]. Due to their popularity, web applications also became the primary targets [9], about 63 percent of total Internet attacks [7], for a wide range of malicious actors. In this extraordinary (COVID-19) situation every business revenue is heavily dependent on online; that is, to run their business successfully these business websites or applications must be "always-on" round the clock [12]. These businesses cannot be successful until the customers have confidence that these web applications are secure [13]. Imperva research [14] shows that, for the past several years, the yearly data breach growth is about 30 percent and almost 50 percent data breaches originated at application layer. Almost 70 percent of successful cyberattacks occur on web applications [14]. In 2020, the number of new application interface (API) vulnerabilities grew by 4 percent [15] and an organization's average loss due to distributed denial-of-service (DDoS), which is one of the foremost cyberattack types in the application layer, is $2.5 million [16]. Therefore, application layer attacks should be a key concern for all businesses that heavily depends on online presence [16].

The application layer is most vulnerable to cyberattacks as compared to other layers [17] and security at this layer is totally different from other layers due to several reasons. First, since the application layer is close to/operated by a large number of end-users, the attack surface at the application layer is too big [17]. Second, it is very difficult to differentiate the cyberattacks from legal Internet connections at the layer 7 (application layer), because all the connections whether they are attack or legitimate user connections, they all need to go through the layer 3/4 (network/transport layers) interface validation process. Third, the majority of the users at the application layer are unskilled end-users, whereas lower layers users are more skilled and more security conscious users such as Information Technology (IT) managers, network engineers, and network administrators [17]. Fourth, the services provided by the applications are located outside the 7 OSI layers which is not under the control of network administrators [13], and finally, many application vulnerabilities are introduced in the design phase of the software development lifecycle, IT managers or network administrators have little control over preventing these vulnerabilities [13]. Therefore, we need to depart from the traditional cyberattacks/defenses techniques and use a totally different approach to address the application layer security.

2. The Role of Modeling and Simulation in Cybersecurity

To solve a complex problem like Cybersecurity, first we need to capture the complexity underneath it [18]. Modeling and simulation is the best available tool to study a system's complexity and forecasting the probable impacts of cyberattacks on that system [18]. Modeling is used to study the behavior and the effectiveness of the design of the system under study [19-21]. Modeling is not only allowing us to capture the essential parts and their relationships of a real-world system, but also the behavior of the system under study [22-24] in order to view the Cybersecurity situation [18]. With respect to Cybersecurity, the modeling process allows us to capture key information about the system under study such as network infrastructure, security settings, business services, and list possible security vulnerabilities and threats [25]. Once the Cybersecurity model is created, we can use simulation to imitate the attacker's activities to assess the system's risk exposure [25], get insight of the whole system [26], and validate the model [18]. An organization can identify the gaps or weaknesses in the system (that is, the system's risk exposure) by first setting the model with known security controls and vulnerabilities and then simulating possible cyberattacks on the model [18, 25]. Simulation

allows the Cybersecurity personnel or network administrators to better understand their system both on abstract and concrete levels and allows them to investigate the real-word system by means of various "what-if" questions [18,27,28]. Simulation is also a powerful tool for providing education and training on the system [18,27,28].

3. Application Layer Security Modeling

The application layer acts as an interface between an application's user and the underlying communication network [18]. The application layer is the computer network's communication endpoint (that is, source and destination of the communication) and its main functions are initiate the data transfer, define user authentication process, and coding (converting the human communications into digital format) and decoding (converting the digital information received into human readable format) [18].

In general, the modeling and simulation community uses the discrete-event simulation (DES) techniques to model the computer networks. That is, to study the network, they will simulate the packet movement throughout the network and observe the network parameters such as throughput and latency. [18] In DES, cyberattacks are simulated by sending a huge number of packets through the network and observing the result [18]. There are two major drawbacks in this DES approach: 1) since DES uses huge number of packets for cyberattack simulation, the computer can able to simulate only few seconds of network operations, and 2) the discrete event simulation's primary focus is on packet traffic, it views the cyberattacks and the resulting cyber defenses from layer 3 (network layer) and cannot model/simulate the cyberattacks that might happen in higher layers (that is, layer 4 and above) especially on the application layer [18]. Therefore, we need a different technique than DES to model/simulate the application layer cyberattacks/defenses.

System dynamics (SD) [29] is a modeling technique in which a system is defined as a collection of interacting elements [30] and used to study how a system changes over time [29]. Originally, in the early 60's the SD was developed by Forrester at Massachusetts Institute of Technology (MIT) to solve long standing, chronic, dynamic industrial management problems [31,32]. Currently SD is used to solve a variety of business policy and strategy problems [33-35]. From our previous research [18], we have identified that the SD is the suitable tool for modeling and simulating various cybersecurity problems especially the application layer security problems. Since SD uses differential/integral equations for modeling, it allows us to simulate a cybersecurity situation (that is network operations) for any length of duration starting from a few seconds to several years.

In SD, a system is defined as a collection of elements that interact continuously over time to form a unified whole [36]. SD Focuses on understanding of how the components of a system interact, how and why the dynamics of concern are generated, and how policies and decisions affect system performance [18]. Like any other simulation model, a SD model has its structure (the static part of the model) and behavior (the dynamic part of the model). The relationships between the physical processes, information flows and managerial policies defines the model's structure [37]. The dynamic behavior of the system is generated by operating the structure over a period [37]. A causal-loop diagram is used to depict the SD system by showing the parts, the links and feedback loops between the system parts as well as between the system and its operating environment [36]. Causal-loop diagrams help the decision-makers to get insight of the complex system such as a cybersecurity model

[18,36]. To model a variety of cyberattack scenarios and observe the system performances under various conditions in SD, we need to do the following steps: 1) convert these causal-loop diagrams into stack-flow diagrams, 2) translate the stack-flow diagrams into system of differential equations, and 3) solve this system of differential equations via simulation [18]. Once the SD cybersecurity model is created, decision-makers can use graphical SD simulation software such as Powersim, iThink and STELLA, or Vensim to extend their system understanding by manipulating the system parts, linkage or feedback, system parameters, or management policies and procedures on the model [18].

4. The Integrated Model for the Application Layer Security

Our integrated model for the application layer security is shown in figure 1.

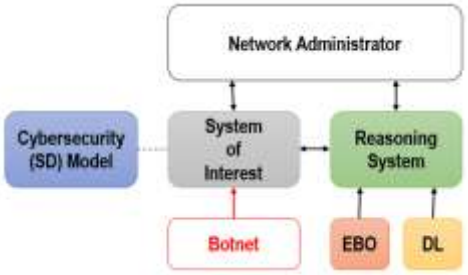

Figure1: The Integrated Application Layer Security Model

4.1. System of Interest

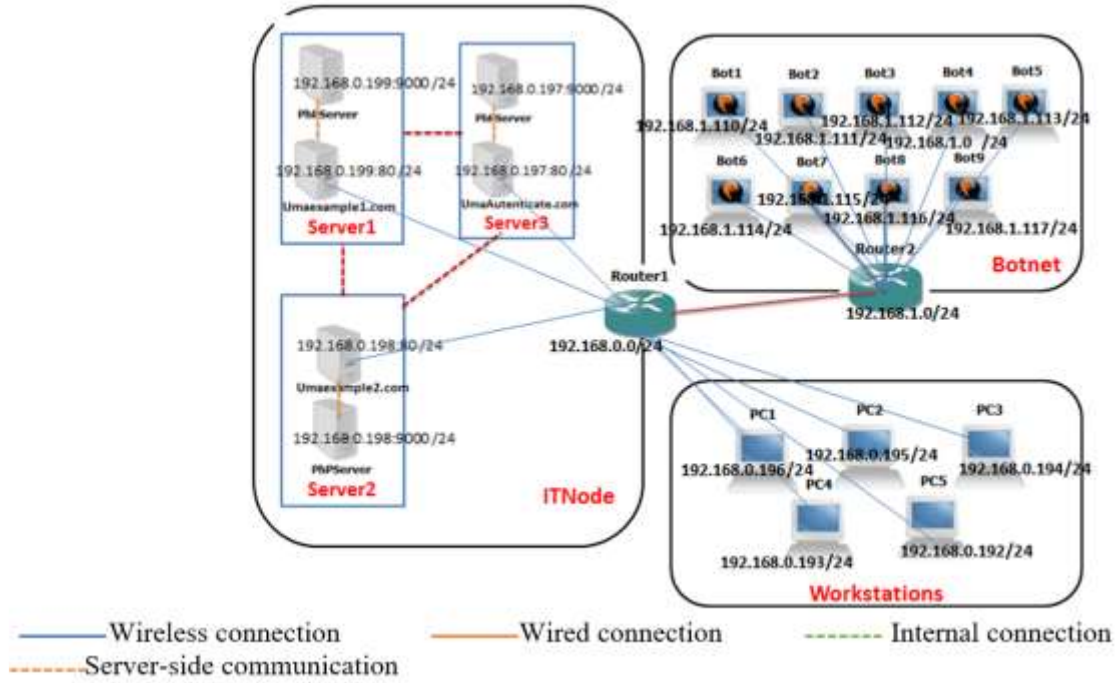

Figure 2: The System of Interest [18]

For this study we created a University IT system with real hardware that consists of three major sections: 1) *an IT node:* consists of three modules learning management system (e.g., Canvas), an email system (e.g., Tiger Mail), and an integrated administrative software system (e.g., Banner) and each of these modules were hosted on different web servers; 2) *a Botnet:* a separate LAN consists of Kali Linux machines used to conduct cyberattacks on the IT node, hosted outside the University LAN; 3) *Workstations:* group of client machines (personal computers and laptops with Windows, Linux, and Mac Operating systems) hosted on the University LAN itself and used by faculty, staff, and students for normal day-to-day operations. The IT system and the LANs configurations are shown in figure 2.

To study our University IT system, first we created an abstract SD model with the essential features of the system. Second, we simulated it over a time with different scenarios to collect the system's behavior over a time. Finally, we used the simulation outputs to refine our abstract model. We repeated this several times until our SD model became an exact replica of the real-world system. The role of the simulation in the design were: 1) identify the gap in the design, that is, identify the key characteristics that may be omitted in the abstract model and include them in the next iteration, 2) try alternative design choices to see which design provides better performance in terms of avoiding bottlenecks and cost-benefits. The role of the simulation in system modeling [38] is shown in figure 3.

4.2. Cybersecurity SD Model

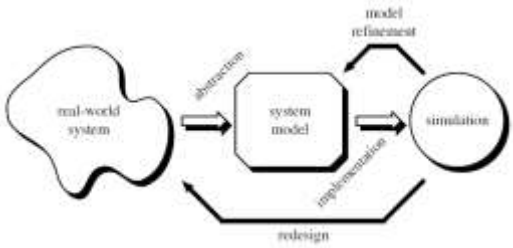

Figure 3: System modeling process [38]

To study how our system behaves under a distributed denial of service (DDoS) attack, we created a sub-model with a domain web server which hosts the hypothetical University's homepage – umaexample1.com in our case and a botnet, which located outside the university LAN, to conduct the DDoS attack. The logic model, real-world physical hardware model, and the SD simulation stack-flow diagram model are shown in figures 4, 2, and 5 respectively.

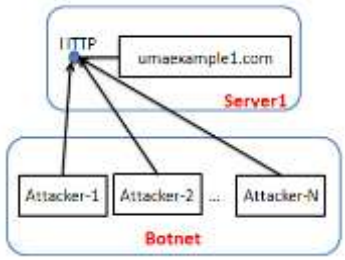

Figure 4: Logical Model for a DDoS Attack

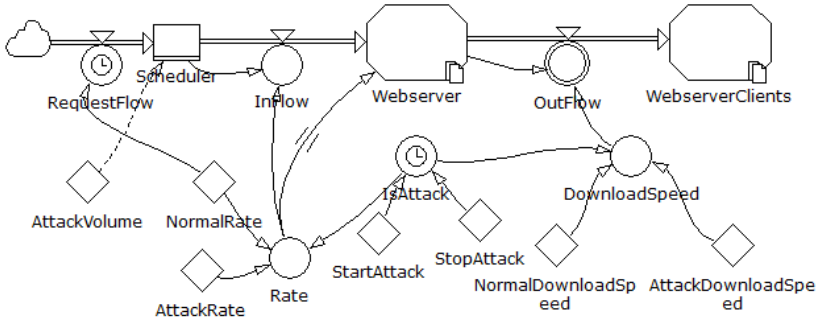

Figure 5: Stack and Flow SD model for a DDoS attack

4.3. Effects-Based Operations

The U.S. Airforce developed a modeling technique called Effects-based operations (EBO) to carry out air strikes [18]. Under EBO, before conducting an air strike the U.S. Air Force will identify the desired effects using wargaming and simulation and then will plan attacks to achieve those desired effects [18,39]. EBO modeling will help an organization to realize the results of first order or direct effects (how an attacked application behaves) and possible indirect or higher order ripple effects (how related applications of the attached application behaves) of a cyberattack from the system level [18].

To study how our system behaves under cyberattack, we simulated an attack on one application of the IT system, say Ebill, and observed the behaviors of the Ebill as well as the other related applications of the system, such as Banner and learning management system, and the home page. This helped us in planning the recovery strategy from such a cyberattack in near future.

4.4. Reasoning System

A reasoning system is a software that drives conclusions or possible answers using logical deduction and induction from the knowledge/information provided to it [40]. There are two types of reasoning systems: an interactive reasoning system and a batch reasoning system; the former needs user feedback and guidance whereas the later provides the conclusions without user feedback and guidance [40-42].

Recent studies have shown that observational data-driven deep learning (DL) models have the potential to make high-quality predictions of events. Among available models, the Long Short-Term Memory (LSTM) neural networks [43], which are variants of recurrent neural networks (RNNs), tend to perform better than general neural network models and physical models. LSTM network models can be an optimal tool for modeling systems since they are capable of tracking long-term dependencies. The two important components

of LSTM networks are states and gates. The states are the representation of memory units that reside inside every LSTM node. The gates regulate the amount of information flowing through every LSTM node. Every LSTM node contains two different types of states: hidden state (stores working memory), which carries the information of the previous node. This memory can be overwritten by the information in the second state called the cell state (stores long-term memory in the current node), which runs through the entire chain and carries long-term dependencies to all the nodes in the network. In addition to the two memory states, an LSTM node also contains three types of gates: input gate, output gate, and forget gate [44]. These gates are used to update the cell state, produce a new hidden state, and help the neural network to overcome the potential unbounded growth of cell states respectively [44].

We have created a deep-learning-based reasoning system using LSTM networks. During the operation, 1) the reasoning system will collect log information about the user, network devices, and network connections, 2) identify the new devices/connections (by tracking the old devices), 3) store long-term dependencies of cyber events, and 4) identify new events (to pass on to the reasoning system to alert about cyber-attacks). Similarly, the system will identify new users and keep a track of their activities to alert when an abnormal user behavior is observed.

5. Results

To study our integrated system performance under cyberattacks, that is how our system responds to a cyberattack on an application, say the Banner system which is hosted on the umaexample1.com, we conducted a DDoS attack (see figure 4 above) and observed the system behavior, which are shown in figure 6 and 7.

Normal Scenario:
Node: www.umaexample1.com
Server configuration: maximum 256 parallel connections (on a given time)
Service Request: 4 connections/sec
Start time: 1st second
End time: 240th second

The attack scenario:
Attack node: www.umaexample1.com
Server configuration: maximum 256 parallel connections (on a given time)
Attack type: DDoS slow read attack (5000 connections, 200 connections/sec)
Attack start time: 60th second
Attack end time: 120th second

As described in the scenarios, we created a SD simulation model (shown in figure 5) to model the cyberattack on the web server. As shown in figure 6, we requested 4 connections per second from 0 to 240 seconds through workstations and conducted DDoS attacks using a botnet from 60th seconds to 120th second. Figure 7 shows the simulated web server status from starting to end. Initially the domain web server is available until 61 second, until the DDoS attack began, it is not available during the DDoS attack, which lasted between 60th and 120th seconds. Once we stopped the cyberattack on 120th second the web server recovered at 123rd second. The same exact result was obtained when we conducted the DDoS attack on a real webserver using the botnet. The real web server's connection status and availability are shown in figures 8 and 9.

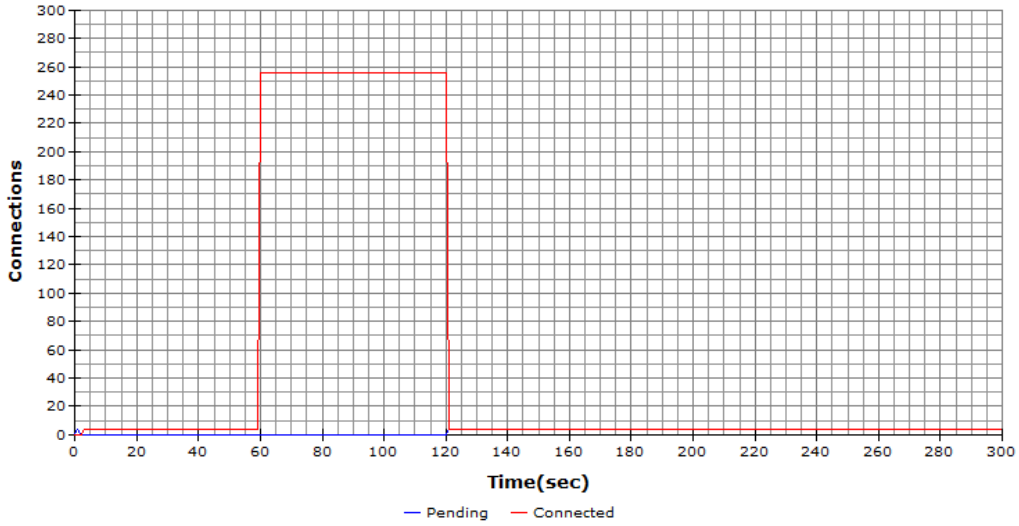

Figure 6: Status of the Simulated Domain Webserver (Connections)

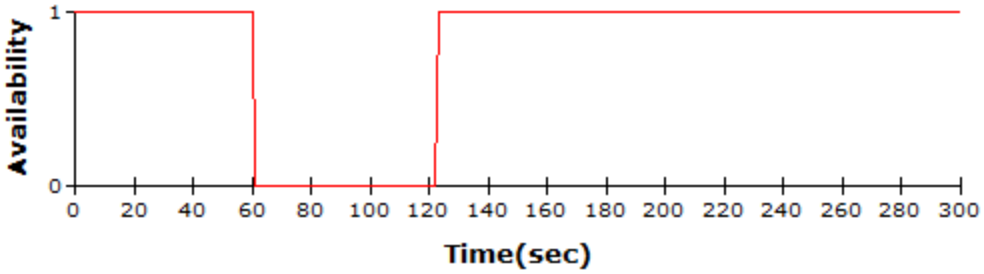

Figure 7: Status of the Simulated Domain Webserver (Availability)

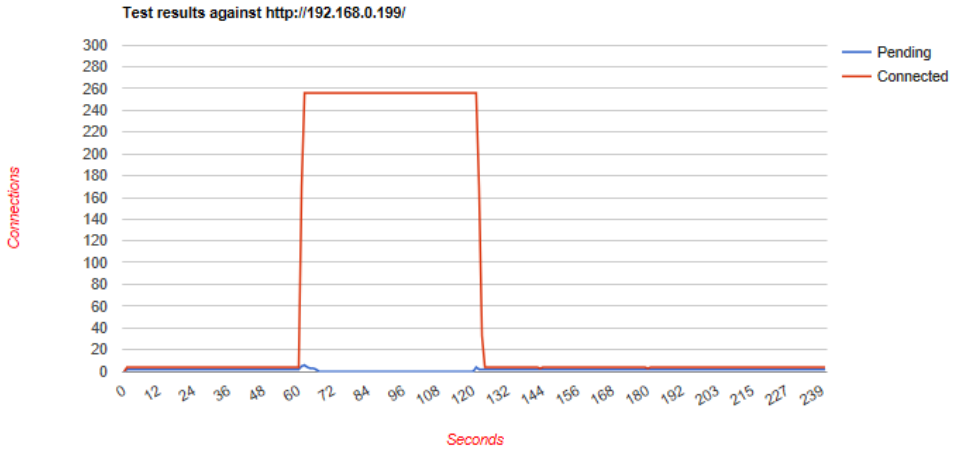

Figure 8: Status of the Domain Webserver (Connections)

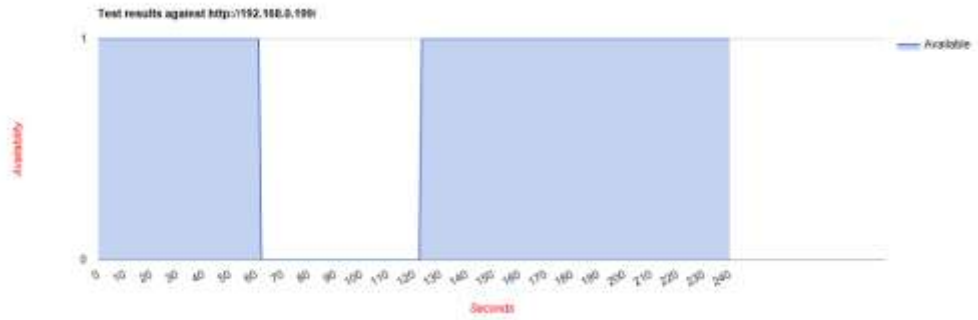

Figure 9: Status of the Domain Webserver (Availability)

From this it is evident that using SD simulation techniques we can model and predict application layer cyberattacks. This will help the network administrators to study the system risk exposure and get ready for future similar cyberattacks.

But as we already mentioned earlier, there are 32 million small companies in the U.S alone and about 81 percent of them do not have network administrators or cybersecurity experts. To support these small organizations our integrated model has a special unit called the reasoning system. Once the system detects the DDoS attack, the reasoning system figures out that one particular client (botnet in our case) occupies the majority of all available web server connections and recommends the network administrator or company owners (in the case of small businesses) to terminate all these connections from the botnet. If the administrator/owner fails/unable to terminate all these connections within 10 seconds the reasoning system will terminate all the connections from the web server (figure 10).

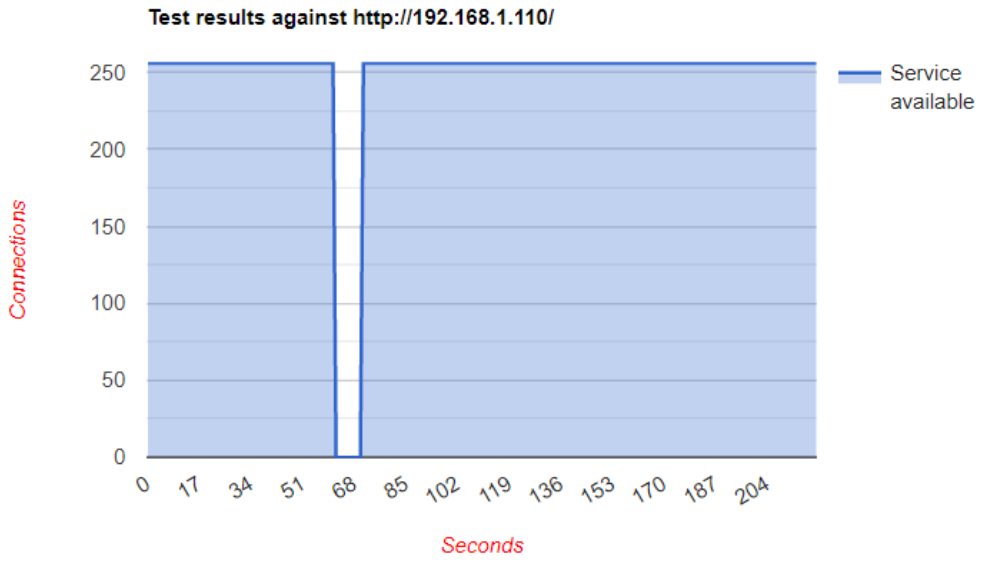

Figure 10: Status of the Reasoning System connected Domain Webserver (Availability)

6. Summary and Conclusions

In this paper, first we showed how system dynamics can be used to model a real-life application layer cybersecurity situation such as a hypothetical university's information technology model. To demonstrate our model, we developed a cybersecurity testbed, conducted a DDoS cyberattack, and showed how the SD modeling technique can be used to predict the future cyberattacks. This will be a very helpful tool for network administrators or cybersecurity personnel to study their system's risk exposure by trying various cyberattacks and possible cyber defenses using EBO. Today, there are 32 million small businesses across the U.S alone and most of them without cybersecurity experts or network administrators. In this extraordinary COVID-19 situation they need to keep their websites/applications online 24x7 to successfully run their business. To support these small business owners to identify and recover from possible cyberattacks, we introduced a reasoning system based integrated application layer security model.

Acknowledgement
Part of this work is supported by the United States National Science Foundation Grant No 1818722.

References

[1] International Organization for Standardization ISO/IEC 27033-1:2009(en), "Information technology — Security techniques — Network security".
[2] International Organization for Standardization (2012) ISO/IEC 27032:2012,"Information technology— Security techniques— Guidelines for cybersecurity".
[3] Jeh C. Johnson, "Let's pass cybersecurity legislation," http://thehill.com/opinion/op-ed/217151-lets-passcybersecurity-legislation
[4] "Measuring digital development: Facts and figures 2021," ITU Publications, ISBN: 978-92-61-35401-5, International Telecommunication Union, Place des Nations, CH-1211 Geneva Switzerland.
[5] "Frequently Asked Questions About Small Businesses," U.S. Small Business Administration Office of Advocacy, October 2020
[6] Felmetsger, V., Cavedon, L., Kruegel, C., Vigna, G., "Toward automated detection of logic vulnerabilities in web applications," In: Proceedings of the 19th USENIX Conference on Security. USENIX Association, Berkeley, CA, USA, 2010, p. 10.
[7] Li, X., Xue, Y., "Block: a black-box approach for detection of state violation attacks towards web applications," In: Proceedings of the 27th Annual Computer Security Applications Conference. ACM, New York, NY, USA, 2011, pp. 247–256.
[8] Doupé, A., Boe, B., Kruegel, C., Vigna, G., "Fear the EAR: discovering and mitigating execution after redirect vulnerabilities," In: Proceedings of the 18th ACM Conference on Computer and Communications Security. ACM, New York, NY, USA, 2011, pp. 251–262.
[9] Pellegrino, G., Balzarotti, D., "Toward black-box detection of logic flaws in web applications," In: Proceedings of 21st Network and Distributed System Security Symposium, San Diego, CA, USA, 2014.
[10] Balzarotti, D., Cova, M., Felmetsger, V.V., Vigna, G., "Multi-module vulnerability analysis of web-based applications," In: Proceedings of the 14th ACM Conference on Computer and Communications Security, ACM, New York, NY, USA, 2007, pp. 25–35.
[11] Cova, M., Balzarotti, D., Felmetsger, V., Vigna, G., "Swaddler: an approach for the anomaly-based detection of state violations in web applications," In: Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, pp. 63–86. volume 4637 of Lecture Notes in Computer Science, 2007.

[12]The Editorial Board, "2 stores, 100M hacks. Where's cybersecurity? Our view," 7:42 p.m. EDT September 14, 2014, http://www.usatoday.com/story/opinion/2014/09/14/home-depot-target-data-breach-credit-card-editorials debates/15642867/?utm_source=feedblitz&utm_medium=FeedBlitzRss&utm_campaign=news-opinion

[13]Kim Holl, "OSI Defense in Depth to Increase Application Security," SANS Security Essentials GSEC Practical Assignment Version 1.4b, SANS Institute, 2003

[14]OfirShaty, "Lessons learned from analyzing 100 data breaches," imperva.com

[15]Terry Ray, "Billions of Compromised Records and Counting: Why the Application Layer is Still the Front Door for Data Breaches," June 8, 2021, https://threatpost.com/billions-of-compromised-records-and-counting/166633/

[16]"Layer 7 DDoS protection: how to stop application layer attacks," https://datadome.co/bot-management-protection/ddos-layer-7-security-protection/

[17]Gary Stevens, "Eye on the End User: Application Layer Security," June 12, 2020, https://securityboulevard.com/2020/06/eye-on-the-end-user-application-layer-security/

[18]Uma Kannan, "Cyber Security System Dynamic Modeling," PhD Dissertation, Department Computer Science and Software Engineering, Auburn University, 2017, https://etd.auburn.edu/handle/10415/6064

[19]Sinclair, J. B, "Simulation of Computer Systems and Computer Networks: A Process-Oriented Approach," George R. Brown School of Engineering, Rice University, Houston, Texas, USA, 2004.

[20]Michael J McDonald, John Mulder, Bryan T Richardson, Regis H. Cassidy, Adrian Chavez, Nicholas D Pattengale, Guylaine M Pollock, Jorge Mario Urrea, Moses Daniel Schwartz, William Dee Atkins, Ronald D. Halbgewachs, "Modeling and Simulation for Cyber-Physical System Security Research, Development and Applications," Sandia Report, SAND2010-0568

[21]Dessouky, "System Simulation," lecture slides

[22]Wikipedia, "Computer simulation," https://en.wikipedia.org/wiki/Computer_simulation

[23]Romano Elpidio, Chiocca Daniela, Guizzi Guido, "An Integrating approach, based on simulation, to define optimal number of pallet in an Assembly Line," 20th Issat Conference, Reliability and quality design; 08/2014

[24]John H. Saunders, "Modeling the Silicon Curtain," SANS Institute 2001

[25]"Using Risk Modeling & Attack Simulation for Proactive Cyber Security: Predictive Solutions for Effective Security Risk Management," Skybox Security Inc., whitepaper, 2012.

[26]"System Modeling and Simulation," http://www4vip.inl.gov/research/system-modeling-and-simulation/d/system-modeling-and-simulation.pdf

[27]John H. Saunders, "Modeling the Silicon Curtain," SANS Institute 2001

[28]Villarreal Gonzalo L., De Giusti Marisa R., Texier José, "GPSS Interactive Learning Environment," 2012 Published by Elsevier Ltd.

[29]Jay Wright Forrester, "Industrial dynamics," MIT Press; 1961

[30]Al Sweetser, "A Comparison of System Dynamics (SD) and Discrete Event Simulation (DES)," albert.sweetser@ac.com

[31]Barlas Y, "System dynamics: systemic feedback modeling for policy analysis in knowledge for sustainable development—an insight into the encyclopedia of life

support systems," UNESCO Publishing-Eolss Publishers, 2002

[32] Uma Kannan, Rajendran Swamidurai, David Umphress, "Modeling Host OSI Layers Cyber-Attacks Using System Dynamics", Proceedings of The 2016 International Conference on Security and Management, SAM'16, vol. 2016, pages 96-100, ISBN: 1-60132-445-6, CSREA Press.

[33] Coyle RG, "System dynamics modelling: a practical approach," Chapman & Hall, 1996

[34] Sterman JD, "Business dynamics: systems thinking and modeling for a complex world," McGraw-Hill, 2000

[35] Dimitrios Vlachos, Patroklos Georgiadis, and Eleftherios Iakovou, "A system dynamics model for dynamic capacity planning of remanufacturing in closed-loop supply chains," Computers & Operations Research 34 (2007) 367–394.

[36] Sweetser, Albert, "A comparison of system dynamics (SD) and discrete event simulation (DES)," 17th International Conference of the System Dynamics Society. 1999.

[37] Dimitrios Vlachos, Patroklos Georgiadis, Eleftherios Iakovou, "A system dynamics model for dynamic capacity planning of remanufacturing in closed-loop supply chains," Computers & Operations Research, 34, 2007, 367–394.

[38] Sinclair, J. B, "Simulation of Computer Systems and Computer Networks: A Process-Oriented Approach," George R. Brown School of Engineering, Rice University, Houston, Texas, USA (2004).

[39] Maris McCrabb, "Effects-based Coalition Operations: Belief, Framing and Mechanism," Ft. Belvoir Defense Technical Information Center, APR 2002.

[40] R. Swamidurai, U. Kannan, A. Raglin and L. Scott, "Smart City Internet of Things Reasoning System for Emergency Responders," 2019 SoutheastCon, 2019, pp. 1-5, doi: 10.1109/SoutheastCon42311.2019.9020580.

[41] Franklin S. Reeder and Katrina Timlin, "Recruiting and Retaining Cybersecurity Ninjas," Washington, DC: CSIS, October 2016, https://csis-website-prod.s3.amazonaws.com/s3fspublic/publication/161011_Reeder_CyberSecurityNinjas_Web.pdf.

[42] George I. Seffers, "National Security Agency Program Fills Critical Cyber Skills Gaps," Signal Magazine, June 1, 2014, https://www. afcea.org/content/national-security-agency-program-fills-critical-cyber-skillsgaps

[43] S. Hochreiter and J. Schmidhuber, "Long short-term memory," Neural Computing, 9:1735–1780, 1997.

[44] Juliane Müller, Jangho Park, ReetikSahu, Deborah Agarwal, CharulekaVaradharajan, Bhavna Arora, Boris Faybishenko, "Surrogate Optimization of Deep Neural Networks for Groundwater Predictions," Journal of Global Optimization, February 5, 2020, arXiv:1908.10947v3