LUCID Network Monitoring and Visualization Application

Claude Turner
Department of Computer Science
Norfolk State University
Norfolk, USA
cturner@nsu.edu

Dwight Richards
Dept. Engineering and Environmental Science
College of Staten Island of CUNY
Staten Island, USA
dwight.richards@csi.cuny.edu

Ruth Agada
Department of Computer Science
Bowie State University
ragada@bowiestate.edu

Jie Yan
Department of Computer Science
Bowie State University
jyan@bowiestate.edu

Rolston Jeremiah
Consultant
Deltona, USA
gtec.oses@gmail.com

Thomas Chapman
Norfolk State University
t.h.chapman74485@nsu.edu

Abstract—This work presents LUCID Network Monitoring and Visualization Application (LNMVA), a comprehensive visualization software application for cyber security visualization. The application consists of five component types: components for monitoring network traffic, components for reporting various network messages, data storage components plus a visualization component and an automated animation reporting component. LNMVA can serve as an aid in teaching complex concepts in cybersecurity or to visually demonstrate active security events on a network to an audience or participants in the classroom or cyber defense competitions at near real-time speed. Its flexibility enables it to visualize different kinds of cybersecurity concepts, protocols and ideas. LNMVA is a sub-system of LUCID, a visualization and broadcasting system that aims to improve understanding and sense-making to participants or an audience. The system is targeted to intermediary or expert users engaged in cyber security exercises. Preliminary results from subject testing show that LNMVA with embodied virtual commentator provided an engaging environment to improve participants' understanding and sense-making in active security events.

Keywords—cybersecurity, cyber exercise, education, network

I. Introduction

In recent years, a wide variety of tools for cybersecurity visualization have been developed [1][2][3][4][5][6][7][8]–[13]. However, adoption of these tools have been limited [6], for reasons that include: users distrust for cybersecurity visualization tools, challenges with respect to the usability of some tools, inability of some tools to meet the complex needs of cybersecurity professionals, and limited availability of comprehensive tools for cybersecurity visualization.

This work presents LUCID Network Monitoring and Visualization Application (LNMVA), a comprehensive visualization software application for cyber security visualization. The application consists of five component types: components for monitoring network traffic, components for reporting various network messages, data storage components, and a visualization component. It is augmented by an automated animation reporting component. LNMVA has the potential to serve as an aid in teaching complex concepts in cybersecurity in the classroom or to visually demonstrate active security events on a network to an audience (or to participants) in a cyber-defense competitions at near real-time. Its flexibility enables it to visualize different kinds of cybersecurity concepts, protocols and ideas. LNMVA is a sub-system of LUCID [14], a visualization and broadcasting system that aims to improve audience (or participants) sense-making at cyber defense competitions. The system is targeted to novice or intermediate users.

The remainder of this paper proceeds as follows: Section II provides brief summaries of selected, existing visualization systems in cybersecurity. Section III discusses the architecture and functionality of LNMVA. Section IV describes the automated animated subsystem. Section V provides preliminary results. Section VI provides concluding remarks.

II. Related Research

This section provides a summary of selected visualization systems discussed in the literature. Kyriakakis et al. [5] provide a description of how spectral techniques may be utilized to discern the nature of packets flowing over a network. For example, spectral analysis can be used to differentiate a DoS (single-source) attack from a DDoS (multi-sources) attack. The paper also proposes the use of immersive spatial audio representations of network events and introduced 3D interactive auto-stereoscopic (AS) displays.

Baxley et al. [15] presented a tool that uses animation to visualize network attacks on LANs. The tool is primarily meant for teaching the concepts of network attacks in the context of a LAN. It uses computer animation and student interactivity to demonstrate the nature of specific classes of network attacks on a LAN.

National Science Foundation.

Ball et al. [8] described VISUAL (Visual Information Security Utility for Administration Live), a tool that allows users to quickly spot communication patterns between internal hosts and external hosts. It also has a feature that uses virtualization to observe communication patterns among computers on the internal home network. The tool uses colors, size of objects, and connecting lines to quickly impart a mental picture of the status of ongoing network traffic.

Kazemi et al. [3] introduced the tool, IPsecLite, which demonstrates the functionality of IP Security (IPsec) standard. Built on many networking technologies and cryptographic techniques, IPsec provides services to secure network communication. The authors introduce IPsecLite through a series of labs that can be used in several security courses approach in computer science education.

Wang et al. [16] described UNIXvisual, which aims to help students learn access control in UNIX. UNIXvisual is aimed both at novice users, who need only to control access to their own files, and students of computer security, who need a deeper and more comprehensive understanding.

Yu et al. [13] proposed a visualization approach to address Domain Name System (DNS) security challenges, such as distributed denial of service (DDoS) and cache poisoning attacks. The authors proposed a methodology to identify, detect, classify, and analyze abnormal DNS querying behaviors by leveraging visualization and human visual perception capabilities. They allow the user to employ different visualization metaphors to analyze different aspects of the same dataset.

III. Network Monitoring and Visualization Application

A. Network Topology

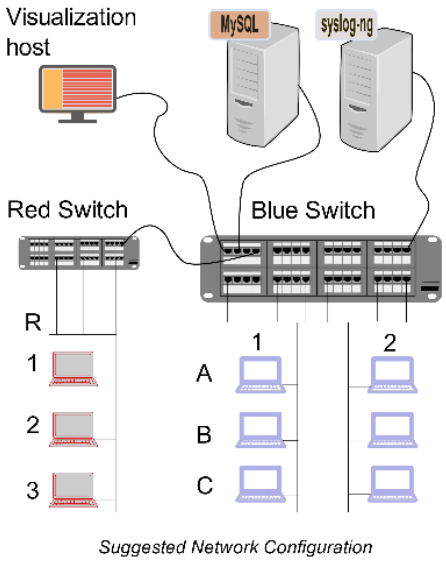

Fig. 1. LNMVA Network Topology

The network topology for the LNMVA exercise environment is depicted in Fig. 1. It shows red hosts, blue hosts, the visualization host, MySQL-server and a syslog-ng server. Servers are shown on separate physical hosts and comprise the administrative domain.

B. LNMVA Architecture

Fig. 2 illustrates the LNMVA architecture and the interaction of its core visualization component with its open source external sub-systems. The sub-system, *Node.js*, operates as a Web server and binds together the activities of the Redis server, MySQL server and the Web socket server sub-systems. *Monitoring* of the competition blue team hosts is accomplished through the Linux Auditd kernel facility [21], Snort intrusion detection and prevention system (IDPS), and Nagios subsystems. Reporting is carried out by syslog-ng server and clients. The visualization host receives log messages from the syslog-ng server, updates the visualization views, and sends the message to the MYSQL server.

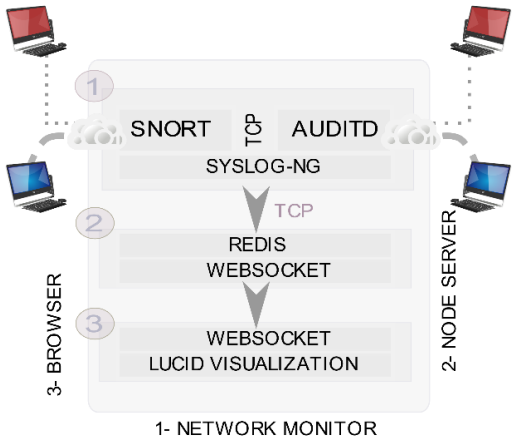

Fig. 2. LNMVA Components

More precisely, blue teams in the competition network are monitored by Auditd, Snort, and Nagios. Syslog-ng clients on the blue team machines watch log files generated by the respective monitors for events of interest (see Fig. 4). These events of interest are sent to a centralized syslog-ng server. The syslog-ng server in turn sends the data to a Redis server, also running in the administrative domain. Redis [22] is an in-memory database utilized by LNMVA to listen for messages submitted to channels marked by keys. Received messages are then transmitted to clients (browsers) over a web-socket connection. Specifically, they are sent to the core LNMVA visualization app, which processes each message, scores it, and displays it appropriately in a browser depending on its source or data type.

Fig. 3 is a concept mapping portrayal of interaction between syslog-ng clients, syslog-ng server, redis, and the visualization host.

C. Redis

Redis is an in-memory database that supports performance add-on features, including support for persistence storage (disk storage), replication in requester-requester and requester-responder modes, publish and subscribe (pub/sub) communication channels and its own

type of transaction. LNMVA makes use of Redis pub/sub feature to listen for messages submitted to channels marked by keys. Received messages are then transmitted to visualization clients over the web-socket connection. The role of Redis is depicted in Fig. 3.

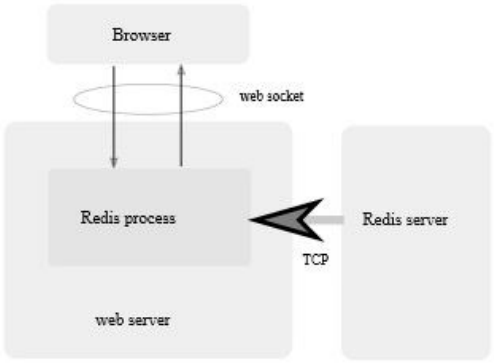

Fig. 3. Role of Redis

D. Syslog-ng

The Syslog-ng Open Source Edition application is a flexible and scalable centralized logging solution. It can be configured to operate in client, relay or server mode, which is determined by its prescribed role. LNMVA adapts the server mode, where several syslog-ng clients send log data to a single syslog-ng server (Fig. 4). The server runs on a computer (or virtual machine) assigned to the administrative domain. Each blue team host needs to run a syslog-ng client and be configured to send specific log file data to the single syslog-ng server. The main task performed by syslog-ng is connecting a source of log information to a specific destination or multiple destinations.

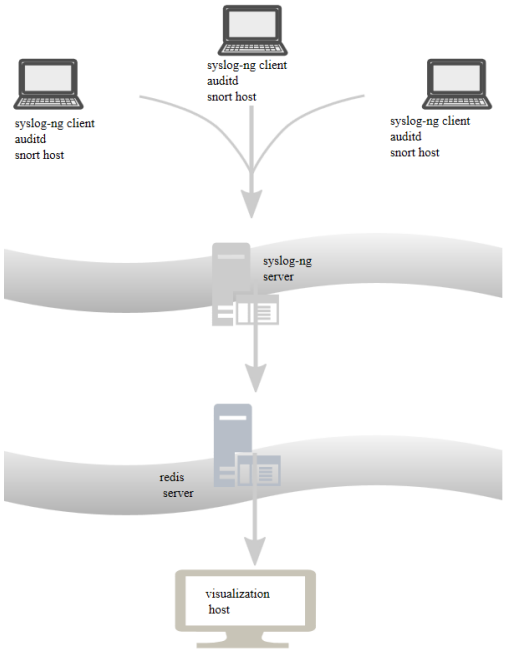

Fig. 4. LNMVA Conceptual Mapping

E. Nagios

Blue teams are expected to establish various network services on their host machines and defend them against nefarious attacks launched by the red team. How well a particular blue team is able to continuously maintain the network services is reflected by the team's score. Clearly, there is a need to monitor and record the status changes of the services running on the blue team computers. One proven solution is Nagios. Nagios is a tool that allows for centralized monitoring of the statuses of hosts and the services running on the same host machines. The main requirement is that all the blue team hosts are reachable from the computer running the Nagios service. In the LNMVA environment, Nagios is used to monitor pre-defined services running on the blue team host computers. Services can be in one of four states:

1) OK - The service is up and running
2) CRITICAL - The service is down
3) WARNING - The service is in an unstable state.
4) BUP - The service is in a "bring-up" state (not yet started)

In LNMVA initial setup, the Nagios application is used to monitor three network services running on all of the blue team computers: SSH, NTP, and MYSQL. Adding additional services is a relatively straightforward process.

F. Auditd

Unexpected changes to critical files on a host can also be monitored by LNMVA. It utilizes, Auditd, a kernel auditing facility, for this purpose. Auditd may be configured to monitor user space activities and report changes to a file's content or attributes, including permission and execution modes.

G. Snort Intrusion Detection and Prevention System

Snort is a signature-based intrusion detection and prevention system (IDPS). It is effective in detecting an attack with a known signature. Once a signature is known, a rule can be written to detect the attack characterized by the signature. Hence, Snort is sometimes referred to as a rule-based IDPS. In the initial iteration of LNMVA, Snort is used to detect denial of service (DoS) attacks; specifically, ping flooding DoS attack. This attack is characterized by flooding a network node with an excessive number of ICMP packets in an attempt to overwhelm that node and prevent it from carrying out normal services; hence denial of service to users. LNMVA ping flooding rule is based on the packet rate. If the packet rate exceeds a given rate, x, an alert is sent to the /var/log/snort/alert file. LNMVA then detects the alert through its syslog-ng client, which has been preconfigured to monitor the alert file. The syslog-ng client then parses the detected alert and forwards the pertinent information to the syslog-ng server. Snort runs on a single server monitoring all the blue teams via its rule.

H. Critical Services and Attack Visualization

The initial version of LNMVA offers monitoring for three types of attacks and three different critical services. The following are the three attacks:

- Denial-of-Service Attack
- Shadow File Compromise: A prohibited user or process alters one or more attributes of the password shadow file.
- SSHD Daemon Compromise: An unauthorized user or process escalates privilege and proceeds to shut down or to reconfigure the daemon.

The following are the three critical network services:

- MySQL
- Secure Shell (SSH):
- Network Time Protocol (NTP)

This paper provides sample visualizations for DoS and the three afore mentioned network services. The LNMVA interactive interface is depicted in Fig. 5. It has several vertical tabs that enable viewing of different kinds of data. Data related to critical services are viewable through the Service tab, while attacks are viewable through the Snort tab. The current view shows the state and associated scores for critical services. Specifically, for six blue hosts (A1, A2, B1, B2, C1 and C2), it shows MySQL is in the BUP state (blue), while SSHD and NTP are in the UP state (green) for the same hosts. The Score Chart, available on every tab, provides the updated score for the blue teams. The current score, 100, is the same for all three teams (HK-Harks, EG-Eagles and FX-Fox). Information for a specific team may be obtained by selecting the appropriate horizontal tab.

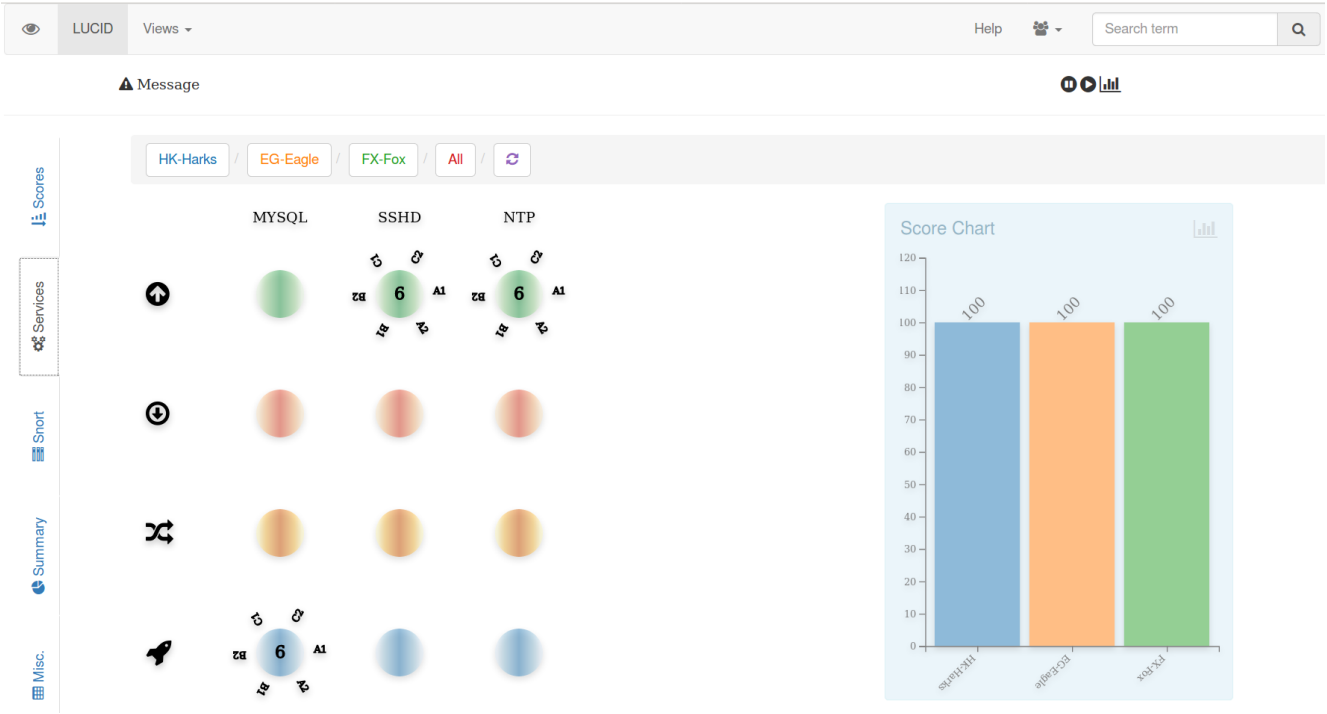

Fig. 5. Visualization of Critical Services

Fig. 6 portrays visualization of a DoS attack. When the Snort tab is selected, this graph would replace the critical service related information that appears in the main pain of Fig. 6. It is a simple line graph indicating the packet arrival rate. A red dotted line, indicating the threshold for denial of service, is superimposed over the packet rate graph. When the rate exceeds the threshold, it assumed that DoS has occurred.

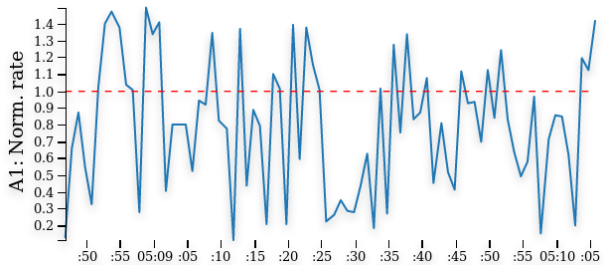

Fig. 6. Denial of Service Visualization

I. GUI for SQLite Database to Configure Tournaments

LNMVA has a graphical user interface (GUI) for its SQLite competition database that is used to store configuration, such as:

- Scheduled tournaments (competition table)
- Targeted host names and IP addresses
- Server names and IP addresses
- Available network services
- Player attributes, such as name, age and gender
- Team attributes, such as name, mascot, and institution.

J. Scoring

LNMVA scoring is derived from the statuses on the blue team hosts. In the case of DoS, a host could lie in one of two states: NORMAL or DOS. This state is determined from the information reported by Snort. A host is said to be in the DOS state if the traffic rate exceeds a prescribed value, x. Otherwise, it is assumed to be in the NORMAL state. Critical services are monitored by Nagios and may be in one of the following four states: UP, DOWN, WARNING, or BUP (bring up). File integrity is monitored by Auditd and may assume one of the following states: SECURED or COMPROMISED.

Scoring decisions are made based on packets meeting one of two conditions:

- The status of a monitored event changes from a desired state to an undesired state; e.g., UP to DOWN, NORMAL to DOS and SECURED to COMPROMISED
- A blue team host remains in an undesired state for a time period exceeding a preconfigured penalty time limit

IV. The Animated Commentator Subsystem

Considering the effectiveness of applying video games in education, the animated commentator subsystem uses a game-like framework [23] that aims to help non-expert audiences comprehend the concepts and engage them in cybersecurity-related events. It seeks to promote cybersecurity education and awareness among non-expert audiences. Specifically, the commentator is able to: (1) perform a variety of human-like behaviors, ranging from various valenced facial expressions, gestures, gaze and emotions conveyed in speech, (2) interact with audiences, and provide several types of feedback, including causal, congratulatory, deleterious, assistive, background, and motivational responses, and (3) provide visual cues when producing speech, using the lips, tongue, and jaw, which complement auditory cues. In addition, the virtual commentator is flexible enough to be employed in the Collegiate Cyber Defense Competitions (CCDC) environment [24].

The animated commentator subsystem takes video, images, and audio information, as well as computer and network visualization information, to generate semantic tags that control various behaviors from facial expressions to gestural motion of animated the agent to make it believable, personable and emotional. These behaviors are broadcast and displayed on the camera and audio subsystem. The architecture of the animated commentator subsystem is shown in Fig. 7.

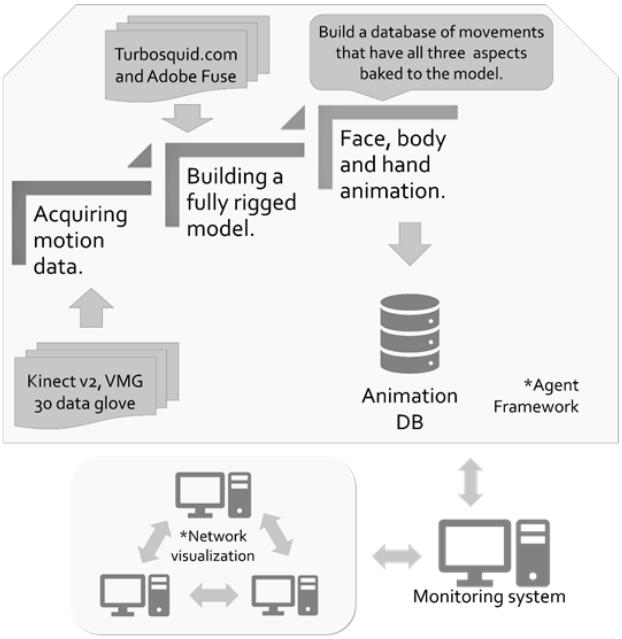

Fig. 7. Architecture of the Animated Commentator

A. Agent data collection and annotation

To enable the agent to simulate the behavior of a human commentator, video footage of contact sports commentators was initially used. Specifically, footage from National Football League (NFL) roundtable discussions, super bowl commentators and Apollo Robbins' TED talks have been utilized. Each video file is roughly 9 minutes in length. These contain commentator motion data that can be applied to the animated agent. In the years 2014 and 2015, 75 minutes of footage from the Maryland Cyber Challenge was collected, in which we interviewed (and recorded) several sponsors of the competition, as well as team coaches, competitors, participants and spectators [25].

We observed several motions/gestures across all the collected data. To annotate the footage, we used a tool called ELAN as seen in Fig. 8. With ELAN, we setup multiple tiers to investigate specific behaviors. Since the data is time-aligned, this allows us to mark the start and end time for each behavior.

We observed that in all these interactions, there are many different body gestures and valenced facial expressions to emphasize certain aspects of the competition. These are challenges that must be considered when modeling them for

the embedded virtual human in the intelligent commentary system [25].

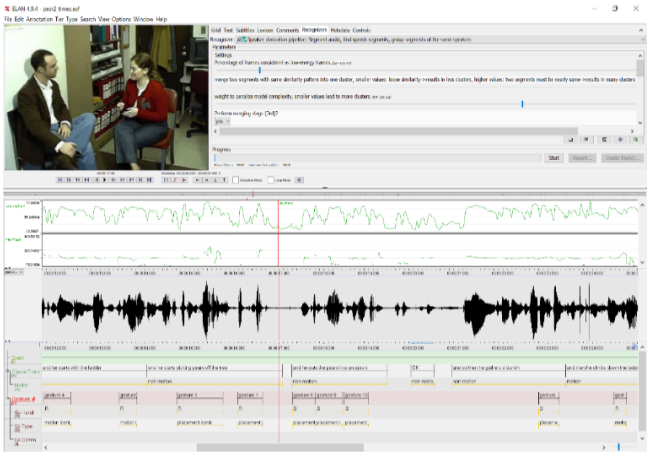

Fig. 8. ELAN Annotation Tool

V. Preliminary Results

Our preliminary results include: (1) developed expressions/gestures of an animated virtual commentator and (2) ongoing user study on the sense making ability of the animator commentator subsystem.

Participants in the evaluation were drawn from a mixture of 17 undergraduate and graduate students enrolled at Bowie State University and Florida's A&M University. Students were recruited by their teachers. Students interacted with the animated commentator subsystem. The testing sessions lasted an average of 15 minutes per participant. The current sample size is small, however, as the user study is still ongoing, we aim to collect at least 100 valid samples for reliable data analysis.

The study was conducted via multiple scheduled zoom meetings. The animated commentator subsystem runs in a Unity development environment. The User study sessions were delivered in phases: pre-survey skill/knowledge based assessment, animated commentator subsystem run, and post-survey subsystem assessment. The post-survey questionnaire allows the test subject to describe the impact of the subsystem on their skill set.

The current interfaces for the animated commentator subsystem environment are 3D mock-ups of the bridge and the engine room of the starship Enterprise NCC1707-D as seen in Fig. 9. On initialization of the commentator subsystem, the agent tries to establish a connection to the visualization network monitoring system. If there is any connection issue, the agent reports that to the user in randomly selected over emphasized gestures with matching speech generation. Barring any connection issues on initialization, the animated commentator subsystem would receive updates from the LNMVA and responds to the incoming input.

Fig. 9. Animated virtual commentator subsystem interface

Analysis of the on-going user study is illustrated in 2 parts: (1) the pre-survey skill/knowledge base assessment and (2) the post-survey subsystem assessment. From the 17 usable subject testing collection, a majority of the participants would consider their skill/knowledge base at the novice level, while the subjects at the competent (or intermediate) level are likely to be Computer Science majors with a leaning towards cybersecurity.

This distribution is further observable with respect to what aspects of prior knowledge/skills the participants bring. Based on the questions designed to gather prior knowledge, Table I further illustrates the impact of the above distribution.

TABLE I. Pre-survey skill / knowledge base testing

1.1 Prior security Courses	
None	76.5%
Novice	11.8%
Advanced Beginner	5.9%
Competent	5.9%

1.2 Related Course	
None	58.8%
Basic security protocol	11.8%
Programming	23.5%
System administrator	5.9%

1.3 Future Goal Alignment	
Yes	29.4%
No	70.6%

In the post-survey subsystem assessment, the subject's skill level was not found; however, the purpose was to gauge the impact of the commentator, given that the subject is either a spectator or a participant of the event. From the analysis of the post-survey user study, all participants engaged with the system as spectators. Hence, all the responses that follow address the impact of the subsystem on spectators. The COVID-19 pandemic further limited the means in which the spectators engaged with the subsystem. Responses provided, such as "I watched a video" and "The voice was low on the video", skewed the results. However, a majority of the participant comments trended toward the ability of the subsystem to provide sense-making opportunities for spectators to observe and gain knowledge of cyber competitions. Agada and Yan [25] references the impact that embodied agents have on its users. On its own, the intelligent commentary system is sufficient as an educational tool. However, in concert with other aspects of the entire competition environment, it has a potential to be a very powerful tool. Further subject testing and analysis of the impact on knowledge will be conducted in the future.

VI. Conclusion

This work presented the LUCID Network Monitoring and Visualization Application (LNMVA), a comprehensive visualization software application for cyber security visualization. LNMVA visualization of three critical services (NTP, SSH and MySQL) and ping flooding denial service of attack were discussed. An animated commentary system, which complements LNMVA, was also discussed. Preliminary results from subject testing show that LNMVA with the embodied virtual commentator provided an engaging environment to improve participants' understanding and sense-making in active security events. Future work for the LUCID system will include the following: (1) Establishment of a comprehensive interface that includes all of the of the LUCID components working synchronously and seamlessly, (2) expanding the number of attacks that LUCID can support, (3) expanding the number of network services that LUCID can support, (4) developing a manual that includes all the configuration details for a typical LUCID competition, (5) developing a manual that provides all the configuration details for specialized competitions that focus on a specific theme, such as a type of attack (say, denial of service) or a specific class of network services, (6) designing different competition/scenario setting, (7) conduct studies on the type of visualization and commentary that might be attractive to certain types of users, such as underrepresented minorities, women and African Americans, and (8) create and maintain a website/github repository.

Acknowledgement

This material is based upon work supported by the National Science Foundation under Grant No. DUE-1303424. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

[1] M. Wang, S. Carr, J. Mayo, C.-K. Shene, and C. Wang, "MLSvisual," in *Proceedings of the 2014 conference on Innovation & technology in computer science education - ITiCSE '14*, 2014, pp. 93–98.

[2] M. Wang, J. Mayo, C.-K. Shene, T. Lake, S. Carr, and C. Wang, "RBACvisual," in *Proceedings of the 2015 ACM Conference on Innovation and Technology in Computer Science Education - ITiCSE '15*, 2015, pp. 141–146.

[3] N. Kazemi and S. Azadegan, "IPsecLite," in *Proceedings of the 41st ACM technical symposium on Computer science education - SIGCSE '10*, 2010, p. 138.

[4] X. Yuan, P. Vega, Y. Qadah, R.Archer, H. Yu, and J. Xu, "Visualization Tools for Teaching Computer Security," *ACM Trans. Comput. Educ.*, vol. 9, no. 4, 2010.

[5] C. Papadopoulos, C. Kyriakakis, A. Sawchuk, and X. He, "CyberSeer: 3D audio-visual immersion for network security and management," in *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security - VizSEC/DMSEC '04*, 2004, p. 90.

[6] G. A. Fink, C. L. North, A. Endert, and S. Rose, "Visualizing cyber security: Usable workspaces," in *2009 6th International Workshop on Visualization for Cyber Security*, 2009, pp. 45–56.

[7] M. Wang, S. Carr, J. Mayo, C.-K. Shene, and C. Wang, "MLSvisual," in *Proceedings of the 2014 conference on Innovation & technology in computer science education - ITiCSE '14*, 2014, pp. 93–98.

[8] R. Ball, G. A. Fink, and C. North, "Home-centric visualization of network traffic for security administration," in *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security - VizSEC/DMSEC '04*, 2004, p. 55.

[9] T. Goldring, "Scatter (and other) plots for visualizing user profiling data and network traffic," in *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security - VizSEC/DMSEC '04*, 2004, p. 119.

[10] E. Glatz, "Visualizing host traffic through graphs," in *Proceedings of the Seventh International Symposium on Visualization for Cyber Security - VizSec '10*, 2010, pp. 58–63.

[11] W. Wang, B. Yang, and Y. V. Chen, "Detecting subtle port scans through characteristics based on interactive visualization," in *Proceedings of the 3rd annual conference on Research in information technology - RIIT '14*, 2014, pp. 33–38.

[12] N. Elmqvist and P. Tsigas, "TrustNeighborhoods in a nutshell," in *Proceedings of the 2006 ACM symposium on Software visualization - SoftVis '06*, 2006, p. 189.

[13] H. Yu, X. Dai, T. Baxliey, X. Yuan, and T. Bassett, "A visualization analysis tool for DNS amplification attack," in *2010 3rd International Conference on Biomedical Engineering and Informatics*, 2010, vol. 7, pp. 2834–2838.

[14] C. Turner, J. Yan, D. Richards, P. O'Brien, J. Odubiyi, and Q. Brown, "Lucid: A visualization and broadcast system for cyber defense competitions," *ACM Inroads*, vol. 6, no. 2, 2015.

[15] T. Baxley, J. Xu, H. Yu, J. Zhang, X. Yuan, and J. Brickhouse, "LAN attacker," in *Proceedings of the 3rd annual conference on Information security curriculum development - InfoSecCD '06*, 2006, p. 118.

[16] M. Wang, J. Mayo, C.-K. Shene, S. Carr, and C. Wang, "UNIXvisual," in *Proceedings of the 2016 ACM Conference on Innovation and Technology in Computer Science Education - ITiCSE '16*, 2016, pp. 356–356.

[17] G. A. Fink, C. L. North, A. Endert, and S. Rose, "Visualizing cyber security: Usable workspaces," in *Visualization for Cyber Security, 2009. VizSec 2009. 6th International Workshop on Visualization for Cyber Security*, 2009, pp. 45–56.

[18] F. Gutierrez, "Stingray," in *Proceedings of the 7th conference on Information technology education - SIGITE '06*, 2006, p. 53.

[19] "Node.js." [Online]. Available: https://nodejs.org/en/. [Accessed: 18-Jun-2018].

[20] "D3: Data-Driven Documents," *IT Security Community Blog*, 2018. [Online]. Available: https://d3js.org/. [Accessed: 04-Jan-2018].

[21] Scotpack, "A Brief Introduction to Auditd." [Online]. Available: https://security.blogoverflow.com/2013/01/a-brief-introduction-to-auditd/. [Accessed: 04-Jan-2018].

[22] Redis, [Online]. Available: https://redis.io/. [Accessed: 18-Jun-2018]

[23] Gifford Cheung and Jeff Huang. 2011. Starcraft from the stands: understanding the game spectator. *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.* (2011), 763–772. DOI: https://doi.org/10.1145/1978942.1979053

[24] Ruth Agada, Jie Yan, Weifeng Xu. A Virtual Animated Commentator Architecture for Cybersecurity Competitions. In the 2018 15th International Conference on Information Technology: New Generations (ITNG), April 16-18, 2018, Las Vegas, Nevada, USA

[25] Ruth Agada, Jie Yan, Leveraging Automated Animated Agent Commentary to Improve Sense-Making for Novice users at Cyber Security Environment. *National Cybersecurity Institute Journal*, 3 (1):47-56, 2016