HAL open science

Cognitive Task Analysis Based Training for Cyber Situation Awareness

Zequn Huang, Chien-Chung Shen, Sheetal Doshi, Nimmi Thomas, Ha Duong

To cite this version:

Zequn Huang, Chien-Chung Shen, Sheetal Doshi, Nimmi Thomas, Ha Duong. Cognitive Task Analysis Based Training for Cyber Situation Awareness. 9th IFIP World Conference on Information Security Education (WISE), May 2015, Hamburg, Germany. pp.27-40, 10.1007/978-3-319-18500-2_3 . hal-01334285

HAL Id: hal-01334285

https://hal.science/hal-01334285v1

Submitted on 20 Jun 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Cognitive Task Analysis Based Training for Cyber Situation Awareness

Zequn Huang[1], Chien-Chung Shen[1], Sheetal Doshi[2], Nimmi Thomas[2], and Ha Duong[2]

[1] Computer and Information Sciences, University of Delaware, USA
[2] Scalable Network Technologies, Inc., USA

Abstract. Cyber attacks have been increasing significantly in both number and complexity, prompting the need for better training of cyber defense analysts. To conduct effective training for cyber situation awareness, it becomes essential to design realistic training scenarios. In this paper, we present a Cognitive Task Analysis based approach to address this training need. The technique of Cognitive Task Analysis is to capture and represent knowledge used by experts to perform complex tasks. Accurate characterization of cyber security experts' cognitive processes can be incorporated into training materials to teach novice cyber analysts how to think and act like experts. After performing Cognitive Task Analysis of cyber situation awareness, we identify the steps necessary for designing training scenarios and training workflows. In order to address the challenge of information overload confronting the cyber analysts, we identify and design attack-specific watch list items. During training, cyber analysts can tailor their own watch list items and triggering thresholds in order to detect cyber attacks faster. As the time it takes for cyber analysts to recognize, analyze, and respond to attacks is critical, we evaluate cyber analysts' performance based on their response time compared with the ideal attack timeline.

Keywords: Cognitive Task Analysis, Cyber Situation Awareness, Cyber Situation Awareness Training Scenario

1 Introduction

Cyber attacks, which refers to any computer-to-computer attacks that undermine the confidentiality, integrity, or availability of computer or information resident on it, have increased significantly in number and in complexity in recent years. Typically, a cyber attacker first exploits a system's vulnerabilities and infiltrates its network and/or hosts. Once the attacker gained entrance into the system, he may use it to monitor communications, steal critical data, discover new avenues of attack in related systems, take control of assets managed by the system or disable vulnerable networks, computers, and associated systems. Harmful outcomes of a successful attack include the attacker's ability to access sensitive data on the network and to control the hosts and network resources.

Situation awareness involves perception of evolving status and attributes of elements, comprehension of combined observations to evaluate the current situation in order to make predictions of possible future outcomes based on past experience and knowledge. Specifically, situation awareness in the cyberspace (Cyber Situation Awareness [1, 2], or CSA for short) is an immensely cognitive task which is embedded in a large multi-layered sociotechnical system of cyber analysts, computers, and networks. In CSA, cyber analysts have to collect data and seek cues that form attack tracks, estimate impact of observed attack tracks, and anticipate moves (actions, targets, time) of attackers. Presently, effective performance in CSA is hampered by the enormous size and complexity of the network, by the adaptive nature of intelligent adversaries, by the high number of false alarms generated by intrusion detection systems, by the lack of ground truth to assess defense performance, by organizational stove-pipes thwarting collaboration, and by technologies that lack an adequate understanding of the human needs.

In particular, in contrast to environments that are bounded by physical constraints and/or geographical features, cyberspace possesses the following unique features which further impose extraordinary cognitive challenges on cyber analysts. First, while a cyber analyst is fully aware of the boundaries of his/her managed networks, the external cyberspace is boundless with minimal geographical features. As a result, the environment from which a cyber analyst has to perceive salient cues is vastly larger and more difficult to comprehend. Comprehending even a small segment of cyberspace is challenging. Second, the speed at which the cyberspace changes is much faster, where new vulnerabilities and their corresponding exploits are continuously emerging, and new offensive technologies are constantly being developed. Furthermore, modern exploits are either employed via misdirection (e.g., a DDoS attack is conducted by a Botnet of compromised computers) or delivered passively via embedded malware. Third, everything a cyber analyst knows about the environment is a virtual representation of the cyberspace in terms of digital information (e.g., intrusion alerts and firewall logs). In addition, the cyber analyst only sees the information that his/her (software) sensors are capable of detecting in a form that can be rendered on monitor screen. Because perception and comprehension of cyberspace is inherently constrained by technology artifacts, cyber analysts' ability to develop situation awareness is greatly limited by the degree to which the network's sensors are correctly configured and capturing data.

Furthermore, cyber analysts are faced with extraordinary amounts of information (such as various IDS and audit logs) to sift through, and CSA demands that various pieces of information be connected in both space and time. This connection necessitates team collaboration among cyber analysts working at different levels and on different parts of the system. It is anticipated that team CSA can be carried out to systematize information coordination and team collaboration for CSA effectiveness and resilience. As cyber attacks are becoming more frequent and more complex, the need for more effective training of cyber ana-

lysts and their collaborative efforts to protect critical assets and ensure system security is also elevated.

Cognitive Task Analysis (CTA [4]) is the extension of traditional task analysis techniques to yield information about the knowledge, thought processes and goal structures that underlie observable task performance. The outcome of CTA describes the performance objectives, equipment, conceptual knowledge, procedural knowledge and performance standards used by experts as they perform a task. Accurate identification of cyber security experts' cognitive processes can be adapted into training materials to teach novices how to perform like experts. In this paper, we present a solution for cyber training which uses a CTA based approach to gain insight into the cognitive demands and workflow of cyber analysts and design cyber security training scenario and training workflow. Then, we evaluate cyber analysts' performance based on their response time of detecting cyber attacks comparing with estimated attack ideal timeline.

The remainder of the paper is organized as follows: Section 2 describes related work and background. Section 3 introduces the Cyber security training and assessment framework infrastructure. In Section 4, we identified the steps necessary for designing cyber security training scenarios and training workflow after performing Cognitive Task Analysis. Section 5 describes two cyber security training scenarios. The scoring algorithm to evaluate the performance of cyber defense analysts is presented in Section 6. To evaluate the usability of the training system, Section 7 presents the questionnaire that cyber analysts are asked to answer in order to evaluate the cognitive validity of training. Finally, Section 8 concludes the paper.

2 Related Work and Background

General reviews of current simulation-based cyber security training systems are given in [5]. CyberCog [6] is a synthetic task environment for understanding and measuring individual and team situation awareness, and for evaluating algorithms and visualization intended to improve cyber situation awareness. CyberCog provides an interactive environment for conducting human-in-the-loop experiment in which the participants of the experiment perform the tasks of a cyber analyst in response to a cyber attack scenario. CyberCog generates performance measures and interaction logs for measuring individual and team performance. CyberCog has been used to evaluate team-based situation awareness. CyberCog utilizes a collection of known cyber defense incidents and analysis data to build a synthetic task environment. Alerts and cues are generated based on emulation of real-world analyst knowledge. From the mix of alerts and cues, trainees will react to identify threats (and vulnerabilities) individually or as a team. The identification of attacks are based on knowledge about the attack alert patterns.

Designed for better understanding of the human in a cyber-analysis task, idsNETS [7], built upon the NeoCITIES Experimental Task Simulator (NETS), is a human-in-the-loop platform to study situation awareness for intrusion detec-

tion analysts. Similar to CyberCog, NETS is also a synthetic task environment. The realistic scenarios are compressed and written into scaled world definitions and the simulation engine is capable of interpreting the scaled world definitions into a simulated environment, running the simulation, and responding to user interaction. In [7], several human subjects experiments have been performed using the NETS simulation engine, to explore human cognition in simulated cyber-security environments. The study indicates that the teams who had more similar skill sets displayed a more cohesive collaboration via frequent communication and information sharing.

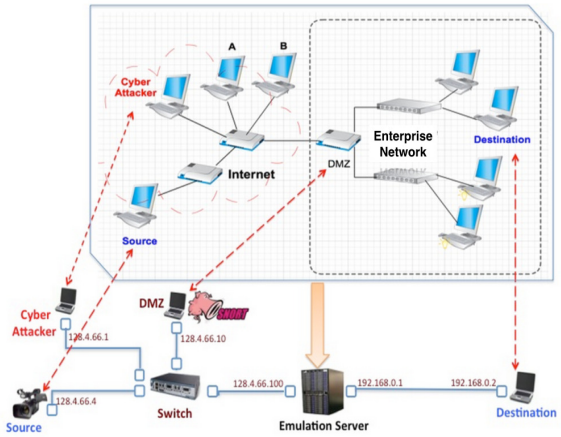

Fig. 1: Usage example of Live-Virtual-Constructive (LVC) framework

The main difference between CyberCog/IdsNETS and LVC framework (Live-Virtual-Constructive [8]) is that while CyberCog and IdsNETS are synthetic task environments, the LVC framework is an actual simulator/emulator. A synthetic task environment may rely on previous incidents to generate the sequence of alerts and cues corresponding to those incidents, The LVC framework is able to simulate previous incidents as well as generate new simulated or emulated incidents on the fly. The LVC framework supports a hybrid network of actual and virtual machines so that attacks can be launched from an actual or a virtual host, targeting an actual or a virtual host. Figure 1 illustrate the usage examples of the LVC framework that combines physical machines and virtual network environment to perform cyber attacks and defense.

3 Cyber Situation Awareness Training and Assessment Framework Infrastructure

The system infrastructure for the proposed Cyber Situation Awareness training and assessment framework is shown in Figure 2. As shown in the figure, lesson database contains different kinds of cyber attack scenarios with different difficulty levels. We apply Cognitive Task Analysis on a set of tasks and use the information to generate scenarios for training purposes. For each task, we identify major events and watch list items needed for decision making. The trainees are able to to tailor their watch list and triggering threshold conditions.

With the proceeding of training scenario, data such as IDS log, network flow, and trainee specified trigger alerts will be reported to the trainee. After analyzing these data, the trainee should think whether it is an attack or false alarm based on prior knowledge and decide the type of attack through attack model matching. Interactions and team discussions can be conducted through the Shared Events Viewer and team communication module. If the team members still cannot achieve agreement, the fuzzy logic based team consensus decision making module can help chose the most acceptable solution for the entire team.

The assessment metrics will include trainee response time with respect to critical cues and evaluate the actions taken or decisions made to determine potential attacks. By comparing trainees' response time and estimated attack ground truth timeline, we can identify if the response is fast or slow. The performance evaluation module can provide performance score and feedback to trainees, as well as adjust the next training lesson's difficulty level based on trainees' performance. Furthermore, Situation Awareness Global Assessment Technique (SAGAT) is used to get feedback from trainees in order to evaluate training system usability and effectiveness.

4 Cyber Situation Awareness Training Scenarios Design

We propose realistic training scenarios for Cyber Situation Awareness training and assessment based on the LVC framework, which enables cyber analysts to experience cyber attacks and to learn how to detect ongoing cyber attacks. Designing cyber security lessons to involve cyber analysts in activate learning requires careful planning. Cognitive Task Analysis technique [9] is a prominent approach that captures knowledge representation used by experts to perform complex tasks. We utilized a combination of three knowledge capture techniques: observing cyber security competitions, examining critical incidents, and reviewing relevant papers of structured interviews with cyber security experts and information assurance analysts [10]. We elicit the knowledge about how, when, where, and why when performing cyber defense task. This knowledge can be applied into design consideration for cyber security training scenarios.

Notice that human cyber analysts have to check thousands of events each day from many sources such as system logs, configurations, traffic logs, IDS log, and audit logs in order to determine whether there are real attacks or false positives;

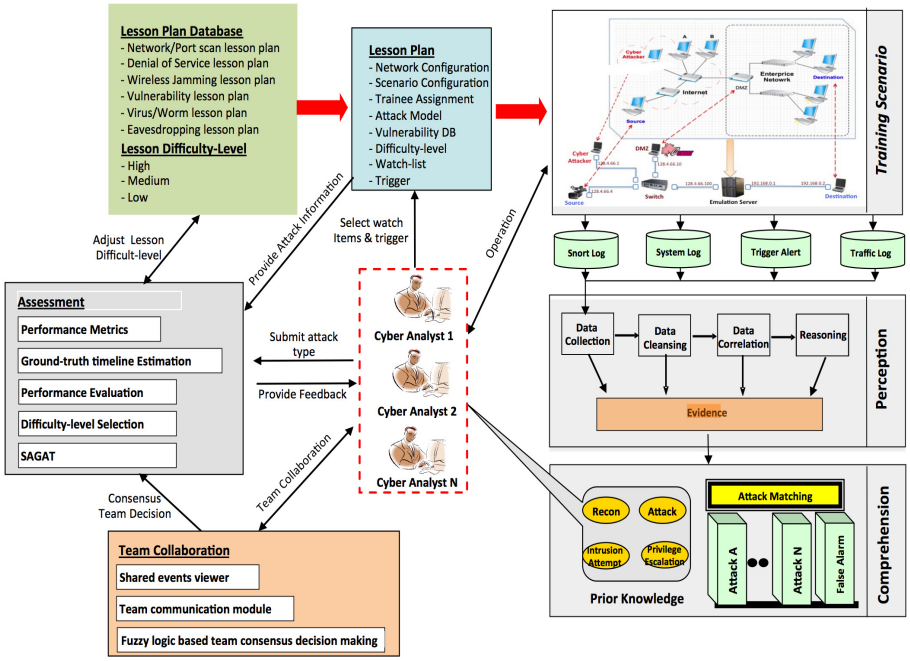

Fig. 2: CSA Training and Assessment System Infrastructure

therefore, they would be soon overwhelmed by tremendous data and forced to ignore potentially significant evidences introducing errors in the detection process. In order to solve the tremendous cognitive demand faced by cyber analysts, we identify and design watch list items relating to cyber attacks. Cyber analysts can tailor their own watch list items and triggering thresholds in order to detect cyber attacks faster.

Six steps necessary for building training lessons are as follows:

1. Previous related work review
2. Training objective definition
3. Training scenario creation
4. Cyber analyst watch-list definition
5. Cyber analyst response recording
6. Performance assessment

Based on the design steps, the training workflow is shown in Figure 3, which contains the following steps:

Step 1: Instructor creates a training scenario for the cyber security training that includes a cheat sheet for the cyber attack/defense aspect based on the lesson objective. The Cheat Sheet includes the watch list items critical to the cyber attack and the attack ideal timeline denoting the attack start and success time. Cyber analyst should react to the cyber events in simulation and perform certain actions that demonstrate his/her understanding of cyber attacks.

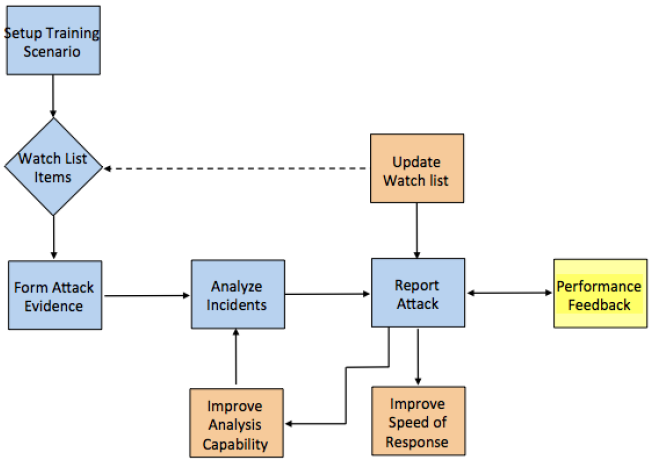

Fig. 3: Workflow for training system

Step 2: Instructor sets up training scenario with the tool providing the widgets to enable the instructor to enter in the information from the cheat sheet.

Step 3: When training scenario begins, the specified trigger alert and other log data specified by cyber analyst will be sent to cyber analyst side. After analyzing these data, cyber analyst should think whether it is an attack or false alarm based on prior knowledge and decide the type of attack through attack model matching.

Step 4: During the training, with cyber analyst's actions being logged continuously, the training system can determine whether the response actions of cyber analyst are following the ideal timeline enumerated by instructor in the cheat sheet.

Step 5: Based on cyber analyst's response and the ideal timeline, the score for cyber analyst will be computed using devised scoring mechanisms, and provided to cyber analyst as part of after action review.

Step 6: After obtaining performance assessment report, cyber analysts should think about selecting different watch list items or improving analysis capability for the next lesson.

Based on the tailored lesson scenario, cyber analyst will learn the knowledge required to monitor network conditions and identify ongoing attacks. After completing the cyber security training, cyber analysts will be able to do the following with respect to a given set of known attacks:

- List the relevant parameters to monitor and know the characteristics of these parameters under normal and abnormal operations.
- Recognize symptoms of network attacks. Specifically, cyber analyst will be able to isolate common characteristics of network under attack and be able to distinguish the characteristics that are particular to each attack.

- Given a particular set of current conditions (monitored parameters), be able to analyze what kind of attack is occurring and how the attack was launched.
- Demonstrate proper procedure of remedial actions, including selection of countermeasures to apply and where in the network to apply them.

5 Cyber Situation Awareness Training Scenarios

Guided by the lesson design steps and goals of cyber security training, we propose port/network scan and denial of service cyber security training scenarios for the Cyber Situation Awareness training and assessment system.

5.1 Port/Network scan Training Scenario

Usually an attacker first attempts to obtain information concerning a network in order to choose the following malicious actions. Specifically, after network scan, an attacker is able to discover the number of hosts, the IP addresses and the network topology. The next step an attacker may take is to perform a port scan [11] to discover which hosts are critical and what services are running on the various hosts. The obtained information can be used by an attacker to plan attack attempts targeting various vulnerabilities.

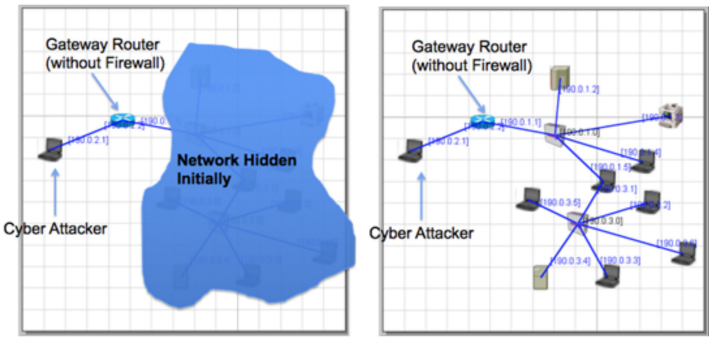

Fig. 4: Port/network scan lesson scenario

An example of lesson scenario on how to perform network and port scan is illustrated in Figure 4. Initially, the core gateway router is configured without firewall. Before performing a network scan, the "inside" network is not visible to the outside world. The attacker then attempts to obtain information on the internal network by launching a network scan. Without firewall protection at the router, the network scan is able to discover the number of hosts, IP addresses and the network topology by sending a bunch of probe packets. Once an attacker learns the IP addresses of hosts and network connectivity, he/she can launch port

scan to discover applications such as web server, FTP server running on the hosts and other devices connected to the hosts.

For the purpose of facilitating cyber analysts' analysis, we define network scan as a procedure for identifying active hosts on a network. After observing the network traffic that contains certain numbers of distinct probes within a short period of time from a single anomalous source, it might be a potential network scan attack. The port scan is defined as an attack that sends requests to a range of server port addresses on a host with the goal of finding open ports and corresponding services running on the ports. By observing several requests to a range of port addresses, it might be a potential port scan attack.

5.2 Denial of Service Training Scenario

Denial of Service (DoS [12]) attacks aim at stopping the target system from working properly through recruiting a large number of "zombie" machines to send high volumes of ordinary traffic. The DoS lesson objective is to train cyber analysts to understand DoS attacks and their detection methods. In this lesson, we will study three types of DoS attacks:

- Basic DoS attack: the attackers send large volume of UDP traffic to the victim host or network. Such traffic consumes network bandwidth, buffer memory as well as CPU resources.
- TCP SYN DoS attack: the attackers send TCP SYN packets to the victim host. Each TCP SYN packet opens a new TCP connection at the victim computer; thus, consuming transport-layer resource.
- IP Fragmentation DoS attack: the attackers send partially fragmented IP packets to the victim host. The victim computer buffers these fragmented packets and wait for remaining segments.

To identify DoS attacks, cyber analysts first need to differentiate attacks from normal bursts of network requests in order to reduce the rate of false alarms. Therefore, we need to compare burst requests with behavior of normal requests. In general, requests from DoS attacks share the same target, such as tens of thousands requests are trying to access a specific address. Once cyber analysts identify the incoming requests are indeed DoS attacks, the next information cyber analysts need to acquire is what kind of DoS attack it is and what attack techniques it is employing. Since cyber analysts already know about the details of the requests from the system logs, cyber analysts can determine the type of DoS attacks and then take corresponding defending actions.

As introduced previously, cyber analysts should consider three DoS attack scenarios: basic DoS attack, TCP SYN DoS attack, and IP Fragmentation DoS attack. Basic DoS attacks involve sending a large volume of traffic to the host, exhausting the host's processing and memory resources and making unable to serve more normal traffic. As a result of sharp increasing in the size of memory and CPU usage of server hosts. TCP SYN attack happens when attackers send a flood of TCP/SYN packets with faked sender addresses. Each packet is treated

as a connection request and the server maintains a half-open connection for each request. The server send TCP/SYN ACK packets back to the faked senders and waits for the responses. Since the sender addresses are faked, the responses will never come. And the number of half-open connections quickly saturate the buffer resources of the server, rendering it unable to serve future legitimate requests. Another technique of DoS attack is via IP fragmentation. Observing larger IP fragments in the IP buffer indicate the potential IP Fragmentation DoS attack.

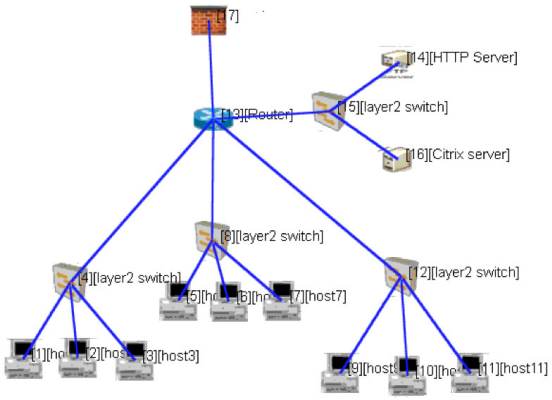

Fig. 5: DoS lesson scenario

Figure 5 shows an example DoS exercise scenario, which includes nine "zombie" machines that can send high volumes of ordinary traffic to the target victim machine. An attack targeting at the HTTP server typically involves sending a large number of requests, each of which consumes significant resources. This then limits the ability of the server to respond to requests from other users. Besides, HTTP requests may make database queries. When costly queries are constructed, a large number of requests could severely overload the server and limit its ability to respond to legitimate requests. The attackers can start either one of the three types of DoS attacks. The magnitude and difficulty level of the exercise scenario can be controlled by the number of "zombie" machines as well as traffic volume.

To perform DoS attack detection, traffic flow monitoring is the key. Example watch list items about system information and traffic flow include CPU and memory resource usage, number of incoming flows, and aggregated traffic rate as shown in Table 1.

6 Performance Metrics and Scoring Algorithms

To monitor the activities of and provide feedback to a cyber analyst during training sessions, we adapt the method of *timeline analysis* for performance

Table 1: DoS exercise watching list

CPU Utilization	CPU utilization is calculated by CPU load as a percentage of the CPU capacity
Memory Usage	Memory consumed during certain period
Network Traffic	- Network-FIFO,Total packets queued - Network-FIFO,Average queue length - Network-FIFO,Longest time in queue - IP,Number of IP Fragments received - IP,Number of IP Fragments dropped - IP,Buffer Size - UDP, Number of packets received - UDP, Number of bytes received - TCP, Number of packets received - TCP, Number of bytes received - TCP, Number of SYN packets received - TCP, Number of SYN ACK packets sent

assessment. The ideal timeline of a training exercise is gauged based on the specific attack scenario and its configuration. After a training exercise starts, all of an cyber analyst's actions are continuously logged so that the training system can determine whether actions taken by the cyber analyst follow the ideal timeline and match the expected activities. This evaluation can be provided as feedback to the cyber analyst during training. For instance, if a cyber analyst fails to identify attacks in time, the system can proactively provide hints to the analyst, or share the views of other cyber analysts. A cyber analyst may also ask for hints from the instructor. The performance of a cyber analyst is evaluated based on the response time of correctly identifying specific cyber attacks.

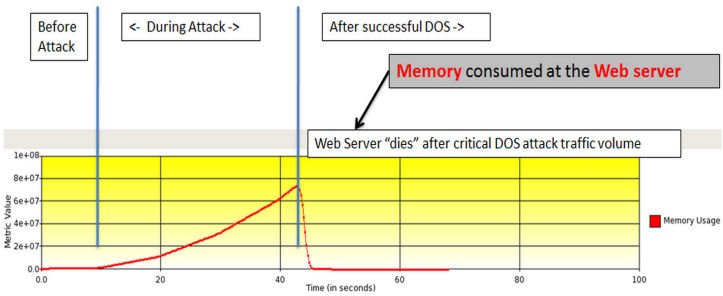

Fig. 6: Use memory usage metric to gauge ideal timeline for a DoS attack

Figure 6 depicts how the measurement of memory usage can be used to characterize the ideal timeline for a DoS attack. The time period is divided by two

memory usage thresholds into three phases: before attack, during attack, and after successful DoS attack. Based on the pre-defined memory usage thresholds and the DoS training lesson's configuration (such as the number of packets to be sent, the frequency of sending packets, the start and end times), a DoS attack's start time and its time of successful attack can be determined. Similarly, the method can be applied to other DoS metrics such as CPU usage, number of incoming flows, and aggregated traffic rate to generate their corresponding timelines. By combining these timelines together, an ideal timeline for the DoS attack can be generated.

Based on the response of cyber analysts and the ideal timeline, scores for the performance of cyber analysts can be computed using the devised scoring mechanisms, and provided to the cyber analysts as one component of their after action review. By comparing cyber analysts' response time against the ideal timeline, we can determine whether a cyber analyst responds in a timely manner. For instance in Figure 6, assuming a DoS attack starts at time 10 second and sustains for 35 seconds, and the victim host shuts down at time 45 second due to DoS attack, cyber analyst has a time window of 35 seconds to identify the ongoing DoS attack. If cyber analyst identifies this DoS attack at time 20 second, cyber analyst's response is considered fast enough to score a higher point. In contrast, if cyber analyst does not identify the DoS attack until the victim host shuts down, no point will be given.

To evaluate the performance of cyber analysts, a set of performance metrics has been adopted:

- Lesson magnitude and difficulty levels (W_D): stands for the severity of attacks or the difficulty level of achieving an attack goal. A scenario's difficulty level is specified in one of three categories: high, medium, or low.
- Response time (W_T): measures cyber analysts' responsiveness to correctly recognizing cyber attacks.
- Correct detection of attacks (W_C): identifies the existence of a real attack and its type.
- Damage impact (W_I): measures attacks' impact on victim's confidentiality, integrity, and/or availability.

Based on the performance metrics, the performance score of cyber analysts can be calculated by the following formula:

$$Score = W_D * (\sum_{k \in \{T,C,I\}} W_k * K_k)$$

where $K_k, k \in \{T, C, I\}$ is the weight factor for each performance metric. Notice that the lesson difficulty level W_D is separated from other performance metric during score calculation. This is because the more difficult of the lesson, the higher score is given since cyber analysts have to spent more time and effort to perform the defense task. For the purpose of consistent computation, each weight factor is normalized to the value between 0 and 1. Take difficulty level W_D as an example, training lesson labeled with "Low" difficulty has weight factor value 0.4 and "Medium" difficulty training lesson is given weight value 0.7.

7 Evaluate Cognitive Validity of Training

In order to evaluate the usability of the training system and the effectiveness of training, Situation Awareness Global Assessment Technique (SAGAT [13]) is used. SAGAT covers the three levels of CSA including Level 1 (perception of data), Level 2 (comprehension of meaning), and Level 3(projection of the near future). Typically, a set of CSA queries regarding the current situation is asked and participants are required to answer each query based upon their knowledge and understanding of the situation at that point. The questions to be asked are as follows:

1. CSA related queries
   (a) An IDS alert based on traffic from 192.168.2.42 destined to 192.168.1.252 is best classified as?
   (b) Which watch list item is abnormal?
   (c) Is it an attack or false alarm?
   (d) What is the impact for the current attack? Any confidentiality, integrity, or availability loss?
   (e) What actions should be performed to stop this attack?
2. Participant satisfaction
   (a) Is the training tool easy to use?
   (b) Is the information displayed in a way that is easy to comprehend?
   (c) Does the tool provide information needed to achieve lesson goals?
   (d) Are the lesson contents at the appropriate difficulty level for the cyber analysts?
   (e) Are the hints useful?
3. Knowledge acquisition
   (a) Does the cyber analysts grasp the main objectives of the lesson?
   (b) Does the lesson learned lead to intended decision-making skills?
4. Behavior changes
   (a) How does the acquired knowledge affect the cyber analysts in future operations?
   (b) Will the cyber analysts be able to detect and identify DoS attacks faster?

8 Conclusion and Future Work

Accurate characterization of cyber security experts' cognitive processes can be adapted into training materials. In this paper, we described two cyber security training scenarios: port/network scanning and denial of service after performing Cognitive Task Analysis. We also defined the metrics for performance evaluation and the corresponding scoring algorithm. For a comprehensive CSA training system, it is more than just an abstract notion of how well people respond to attacks, but also, evaluates on the basis of how damaging certain attacks are, how long it takes for those attacks to manifest themselves, and how quickly recovery needs to take place in order to restore service to acceptable levels.

9 Acknowledgements

This material is based upon work supported by US Army Research Office under contract W911NF-14-C-0140. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the US Army Research Office.

References

1. Jajodia, S., Liu, P., Swarup, V., and Wang, C.: Cyber Situational Aware- ness: Issues and Research. Springer (2010)
2. Kott, A., Wang, C., and Erbacher, R.: Cyber Defense and Situational Awareness. Springer (2014)
3. Tyworth, M., Giacobe, N., Mancuso, V., and Dancy, C.: The distributed nature of cyber situation awareness. in IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (2012).
4. Mahoney, S., Roth, E., Steinke, K., Pfautz, J., Wu, C., and Farry, M.: A Cognitive Task Analysis for Cyber Situational Awareness. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (2010)
5. Pastor, V., Diaz, G., and Castro, M.: State-of-the-art simulation systems for information security education, training and awareness. in IEEE Education Engineering (2010)
6. Rajivan, P.: CyberCog:A Synthetic Task Environment for Measuring Cyber Situation. in Master Thesis of Arizona State University (2011)
7. Giacobe, N. A., McNeese, M. D., Mancuso, V. F., and Minotra, D.: Capturing human cognition in cyber-security simulations with NETS. in IEEE International Conference on Intelligence and Security Informatics (2013)
8. Varshney, M., Pickett, K., and Bagrodia, R.: A Live-Virtual-Constructive (LVC) framework for cyber operations test, evaluation and training. in IEEE Military Communications Conference (2011)
9. Cooke, J. N., D'Amic, A., Endsley, R. M., Roth, E., and Salas, E.: Perspectives on the Role of Cognition in Cyber Security. in Proceedings of the Human Factors and Ergnomics Society 56th Annual Meeting (2011)
10. D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., and Roth, E.: Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts. in Proceedings of the Human Factors and Ergonomics Society Annual Meeting (2005)
11. Panjwani, S., Tan, S., and Jarrin, M. K.: An Experimental Evaluation to Determine if Port Scans Are Precursors to an Attack. in Proceedings of the 2005 International Conference on Dependable Systems and Networksn (2005)
12. Sekar, V., Duffield, N., Spatscheck, O., Merwe, J., and Zhang, H.: LADS: Large-scale Automated DDOS Detection System. in Proceedings of the Annual Conference on USENIX '06 Annual Technical Conferencen (2006)
13. Endsley, M.R., and Garland, D.J.: Situation awareness analysis and measurement. CRC Press(2000)