REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
15-04-2019	Final Report	1-Aug-2013 - 31-Jul-2015

4. TITLE AND SUBTITLE
Final Report: An Infrastructure for Deploying and Testing Comprehensive Cyber Situational Awareness Solutions

5a. CONTRACT NUMBER
W911NF-13-1-0317

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611103

6. AUTHORS
Massimiliano Albanese

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
George Mason University
4400 University Drive, MSN 4C6

Fairfax, VA 22030 -4422

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
63387-CS-RIP.3

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Sushil Jajodia
UU	UU	UU	UU		19b. TELEPHONE NUMBER 703-993-1653

RPPR Final Report
as of 16-Apr-2019

Agency Code:

Proposal Number: 63387CSRIP **Agreement Number: W911NF-13-1-0317**
INVESTIGATOR(S):

Name: Sushil Jajodia
Email: jajodia@gmu.edu
Phone Number: 7039931653
Principal: Y

Name: Kun Sun
Email: ksun3@gmu.edu
Phone Number: 7039931715
Principal: N

Name: Massimiliano Albanese
Email: malbanes@gmu.edu
Phone Number: 7039931629
Principal: N

Organization: **George Mason University**
Address: 4400 University Drive, MSN 4C6, Fairfax, VA 220304422
Country: USA

DUNS Number: 077817450 EIN: 540836354
Report Date: 31-Oct-2015 Date Received: 15-Apr-2019
Final Report for Period Beginning 01-Aug-2013 and Ending 31-Jul-2015
Title: An Infrastructure for Deploying and Testing Comprehensive Cyber Situational Awareness Solutions
Begin Performance Period: 01-Aug-2013 **End Performance Period:** 31-Jul-2015
Report Term: 0-Other
Submitted By: Kun Sun Email: ksun3@gmu.edu
Phone: (703) 993-1715
Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees: **STEM Participants:**

Major Goals: Under the ARO funded MURI project entitled “Computer-Aided Human Centric Cyber Situation Awareness,” we at George Mason University developed an integrated Cyber Situation Awareness (CSA) solution to support cyber security analysts and fill the semantic gap between available monitoring data and the analysts’ mental processes. The comprehensive CSA framework we defined has the capability of automatically answering a number of questions that analysts may ask about current situation, impact and evolution of attacks, behavior of attackers, quality of available information and models, and possible future attacks.

With this DURIP award, our goal was to build a computing infrastructure that includes (i) highly available servers for deploying the monitoring systems and the novel components of the framework; (ii) redundant storage to reliably maintain all relevant information and data structures; and (ii) analyst workstations equipped with multiple large displays. This infrastructure was fundamental to demonstrate the feasibility of our approach by allowing the large scale implementation needed to thoroughly vet the proposed framework and direct our research and development towards demonstrating enterprise-wide scalability of our solutions. This infrastructure enabled us to realistically assess the effectiveness and efficiency of our approach and get valuable feedback from analysts. Additionally, it provided our students with the opportunity to gain valuable hands-on experience.

Accomplishments: We used the equipment acquired through this grant to build an infrastructure for deploying our CSA framework and test its scalability. While a prototypal implementation of the framework was fundamental to demonstrate the feasibility of our approach, a larger scale implementation was needed to thoroughly vet it and demonstrate scalability of our solution.

The infrastructure was configured as depicted in Figure 2. A total of 9 Dell PowerEdge R720 servers were organized into two separate sub-networks comprising 5 and 4 servers respectively, and virtualization technology

was adopted to enable us to use the underlying hardware resources to deploy both virtual machines running the different components of the framework and virtual machines simulating the networks to be monitored. To build a readily deployable system, and prove the potential for enterprise-wide applicability and commercialization, we needed to build redundancy and load balancing capabilities into the system. This motivated the choice to setup two different sub-networks, and replicate all processes across the two clusters. Connectivity within each sub-network was provided by a Dell Force10 S-Series network switch. The two switches were interconnected to guarantee high-speed data transfer between the two clusters, and they both provided connectivity to and from a shared Dell PowerVault MD3660i Storage array. Additionally, both switches were connected to the general GMU network, thus providing redundant network access.

Finally, 2 Dell Precision T5500 workstations were installed to create two analyst workstations. Each workstation was equipped with 3 large monitors, which enabled the analyst (or a student) to visualize the different information items (charts, graphs, and recommendations) that the suite of tools comprising the framework was automatically generating by analyzing raw network data. The workstations were physically deployed in one of our research labs in the Research Hall building, and connected to the system through the general GMU network. Instead, the servers were deployed in one of our dedicated racks in the Aquia data center, a state-of-the-art, secure data center offering the Mason research community colocation services designed to provide a secure operating environment dedicated to system availability and uptime.

Our research resulted in the several publications, some of which are listed below:

1. R. Ganesan, S. Jajodia, A. Shah, and H. Cam, “Dynamic scheduling of cybersecurity analysts for minimizing risk using reinforcement learning,” ACM Transactions on Intelligent Systems and Technology, vol. 8, no. 1, July 2016.
2. E. Serra, S. Jajodia, S. Pugliese, A. Rullo, and V.S. Subrahmanian, “Pareto-optimal adversarial defense of enterprise systems,” ACM Transactions on Information and System Security, vol. 17, no. 3, Article 11, March 2015.
3. S. Venkatesan, M. Albanese, K. Amin, S. Jajodia, and M. Wright, “A Moving Target Defense Approach to Mitigate DDoS Attacks against Proxy-Based Architectures,” in Proceedings of the 4th IEEE Conference on Communications and Network Security (IEEE CNS 2016), Philadelphia, Pennsylvania, USA, October 17-19, 2016.
4. M. Albanese, E. Battista, and S. Jajodia, “Deceiving Attackers by Creating a Virtual Attack Surface,” in Cyber Deception: Building the Scientific Foundation, S. Jajodia, V.S. Subrahmanian, V. Swarup, and C. Wang (Eds.), pages 169-201, Springer, 2016.
5. M. Albanese, E. Battista, and S. Jajodia, “A Deception Based Approach for Defeating OS and Service Fingerprinting,” in Proceedings of the 3rd IEEE Conference on Communications and Network Security (IEEE CNS 2015), pages 253-261, Florence, Italy, September 28-30, 2015.
6. S. Venkatesan, M. Albanese, and S. Jajodia, “Disrupting Stealthy Botnets through Strategic Placement of Detectors,” in Proceedings of the 3rd IEEE Conference on Communications and Network Security (IEEE CNS 2015), pages 55-63, Florence, Italy, September 28-30, 2015. [Best paper runner-up award]
7. M. Albanese, E. Battista, S. Jajodia, and V. Casola, “Manipulating the Attacker’s View of a System’s Attack Surface,” in Proceedings of the 2nd IEEE Conference on Communications and Network Security (IEEE CNS 2014), pages 472-480, San Francisco, California, USA, October 29-31, 2014.
8. L. Wang, M. Zhang, S. Jajodia, A. Singhal, and M. Albanese, “Modeling Network Diversity for Evaluating the Robustness of Networks against Zero-Day Attacks,” in Proceedings of the 19th European Symposium on Research in Computer Security (ESORICS 2014), pages 494-511, Wroclaw, Poland, September 7-11, 2014.
9. M. Albanese, H. Cam, and S. Jajodia, “Automated Cyber Situation Awareness Tools for Improving Analyst Performance,” in Cybersecurity Systems for Human Cognition Augmentation, R.E. Pino, A. Kott, and M. Shevenell (Eds.), vol. 62 of Advances in Information Security, pages 47-60, Springer, 2014.

Training Opportunities: The computing infrastructure provided our students with the opportunity to gain valuable hands-on experience.

RPPR Final Report
as of 16-Apr-2019

Results Dissemination: Our research resulted in the several publications, some of which are listed below:

1. R. Ganesan, S. Jajodia, A. Shah, and H. Cam, “Dynamic scheduling of cybersecurity analysts for minimizing risk using reinforcement learning,” ACM Transactions on Intelligent Systems and Technology, vol. 8, no. 1, July 2016.
2. E. Serra, S. Jajodia, S. Pugliese, A. Rullo, and V.S. Subrahmanian, “Pareto-optimal adversarial defense of enterprise systems,” ACM Transactions on Information and System Security, vol. 17, no. 3, Article 11, March 2015.
3. S. Venkatesan, M. Albanese, K. Amin, S. Jajodia, and M. Wright, “A Moving Target Defense Approach to Mitigate DDoS Attacks against Proxy-Based Architectures,” in Proceedings of the 4th IEEE Conference on Communications and Network Security (IEEE CNS 2016), Philadelphia, Pennsylvania, USA, October 17-19, 2016.
4. M. Albanese, E. Battista, and S. Jajodia, “Deceiving Attackers by Creating a Virtual Attack Surface,” in Cyber Deception: Building the Scientific Foundation, S. Jajodia, V.S. Subrahmanian, V. Swarup, and C. Wang (Eds.), pages 169-201, Springer, 2016.
5. M. Albanese, E. Battista, and S. Jajodia, “A Deception Based Approach for Defeating OS and Service Fingerprinting,” in Proceedings of the 3rd IEEE Conference on Communications and Network Security (IEEE CNS 2015), pages 253-261, Florence, Italy, September 28-30, 2015.
6. S. Venkatesan, M. Albanese, and S. Jajodia, “Disrupting Stealthy Botnets through Strategic Placement of Detectors,” in Proceedings of the 3rd IEEE Conference on Communications and Network Security (IEEE CNS 2015), pages 55-63, Florence, Italy, September 28-30, 2015. [Best paper runner-up award]
7. M. Albanese, E. Battista, S. Jajodia, and V. Casola, “Manipulating the Attacker’s View of a System’s Attack Surface,” in Proceedings of the 2nd IEEE Conference on Communications and Network Security (IEEE CNS 2014), pages 472-480, San Francisco, California, USA, October 29-31, 2014.
8. L. Wang, M. Zhang, S. Jajodia, A. Singhal, and M. Albanese, “Modeling Network Diversity for Evaluating the Robustness of Networks against Zero-Day Attacks,” in Proceedings of the 19th European Symposium on Research in Computer Security (ESORICS 2014), pages 494-511, Wroclaw, Poland, September 7-11, 2014.
9. M. Albanese, H. Cam, and S. Jajodia, “Automated Cyber Situation Awareness Tools for Improving Analyst Performance,” in Cybersecurity Systems for Human Cognition Augmentation, R.E. Pino, A. Kott, and M. Shevenell (Eds.), vol. 62 of Advances in Information Security, pages 47-60, Springer, 2014.

Honors and Awards: Nothing to Report

Protocol Activity Status:

Technology Transfer: Nothing to Report

CONFERENCE PAPERS:

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: IEEE CNS 2016
Date Received: 29-Oct-2016 Conference Date: 18-Oct-2016 Date Published: 18-Oct-2016
Conference Location: Philadelphia, PA, USA
Paper Title: A Moving Target Defense Approach to Mitigate DDoS Attacks against Proxy-Based Architectures
Authors: Sridhar Venkatesan, Massimiliano Albanese, Kareem Amin, Sushil Jajodia, Mason Wright
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 16-Apr-2019

Final Report

An Infrastructure for Deploying and Testing Comprehensive Cyber Situational Awareness Solutions

ARO Award No. W911NF-13-1-0317

Submitted by

Sushil Jajodia
Center for Secure Information Systems
George Mason University
Fairfax, VA 22030-4422
jajodia@gmu.edu

1. Introduction

Under the ARO funded MURI project entitled ***"Computer-Aided Human Centric Cyber Situation Awareness,"*** we at George Mason University, in collaboration with our research partners, have developed an integrated Cyber Situation Awareness (CSA) solution to support cyber security analysts and fill the semantic gap between available monitoring data and the analysts' mental processes. The comprehensive CSA framework we defined during the first two years of the project envisioned the capability of automatically answering a number of questions that analysts may ask about current situation, impact and evolution of attacks, behavior of attackers, quality of available information and models, and possible future attacks. Answering such questions automatically and efficiently requires specialized data structures and novel techniques for analyzing and correlating large amounts of data. Many such techniques have been developed during the 5-year MURI project.

With this DURIP award, we were able to build an infrastructure that includes (i) highly available servers for deploying the monitoring systems and the novel components of the framework; (ii) redundant storage to reliably maintain all relevant information and data structures; and (ii) analyst workstations equipped with multiple large displays. This infrastructure has been fundamental to demonstrate the feasibility of our approach by allowing the large scale implementation needed to thoroughly vet the proposed framework and direct our research and development towards demonstrating enterprise-wide scalability of our solutions. This infrastructure enabled us to realistically assess the effectiveness and efficiency of our approach and get valuable feedback from analysts. Additionally, it provided our students with the opportunity to gain valuable hands-on experience.

Additionally, the availability of the computing infrastructure built under this DURIP has provided critical support to other projects, including the ARO funded MURI project entitled

"Adversarial and Uncertain Reasoning for Adaptive Cyber Defense: Building the Scientific Foundations."

2. Overview of our Approach

Today, when a security incident occurs, the top three questions security administrators would ask are in essence: What has happened? Why did it happen? What should I do? Answers to the first two questions form the core of Cyber Situational Awareness. Whether the last question can be satisfactorily answered is greatly dependent upon the Cyber Situational Awareness capability of an enterprise. A variety of computer and network security research topics (especially some systems security topics) belong to or touch the scope of Cyber Situational Awareness. However, the CSA capability of an enterprise is still very limited for several reasons, including but not limited to: (i) inaccurate and incomplete vulnerability analysis, intrusion detection, and forensics; (ii) limited capability to quickly adapt to the evolving nature of networks and attacks; (iii) limited capability to transform large amounts of raw data into cyber intelligence; (iv) limited capability to handle uncertainty.

Network data and alerts are often uncertain, ambiguous, and even incorrect. Given large volumes of alerts from intrusion detection systems, these alerts need to be filtered to identify the most informative ones for analysis. Defenders need to quickly recognize real threats, understand their potential impact on missions, and respond quickly and accurately in order to minimize the impact. Furthermore, this needs to be done in the context of multi-step and potentially complex vulnerability paths through the network.

The goal of our project was to explore ways to elevate the Cyber Situational Awareness capability of an enterprise to the next level by measures such as developing holistic Cyber Situational Awareness approaches and evolving existing system designs into new systems that can achieve self-awareness. To provide advanced capabilities for cyber situational awareness in the face of attacks on complex network vulnerability landscapes, we proposed an integrated framework for automated attack modeling, dependency discovery, alert correlation, mission impact analysis, and network hardening. The innovative claims of our approach are the following:

- Innovative approach to Topological Vulnerability Analysis that overcomes the limitations of traditional point-wise vulnerability analysis.
- Capability of processing massive amounts of alerts/sensory data in real-time.
- Capability of forecasting possible futures, along with their probabilities and anticipate damage potential.
- Capability of hardening a network in a cost-effective and time-efficient manner against both known and zero-day vulnerabilities.

- Capability of assessing the completeness and quality of available attack models.
- Capability of accurately localizing attackers in mobile networks.

Figure 1 provides an overall view of the architecture of the framework we developed, showing both the software modules (blue boxes) and the data structures (green boxes) involved in the proposed CSA process.

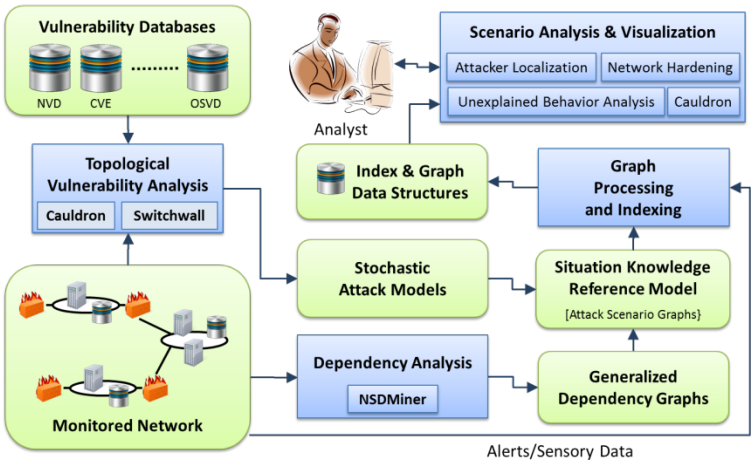

Figure 1 - Overall architecture of the proposed CSA framework

3. Laboratory Setup

We used the equipment acquired through this grant to build an infrastructure for deploying our CSA framework and test its scalability. While a prototypal implementation of the framework was fundamental to demonstrate the feasibility of our approach, a larger scale implementation was needed to thoroughly vet it and demonstrate scalability of our solution.

The infrastructure was configured as depicted in Figure 2. A total of 9 Dell PowerEdge R720 servers were organized into two separate sub-networks comprising 5 and 4 servers respectively, and virtualization technology was adopted to enable us to use the underlying hardware resources to deploy both virtual machines running the different components of the framework and virtual machines simulating the networks to be monitored. To build a readily deployable system, and prove the potential for enterprise-wide applicability and commercialization, we needed to build redundancy and load balancing capabilities into the system. This motivated the choice to setup two different sub-networks, and replicate all processes across the two clusters. Connectivity within each sub-network was provided by a Dell Force10 S-Series network switch. The two switches were interconnected to guarantee high-speed data transfer between the two clusters, and they both provided connectivity to and from a shared Dell PowerVault MD3660i Storage array. Additionally, both switches were connected to the general GMU network, thus providing redundant network access.

Finally, 2 Dell Precision T5500 workstations were installed to create two analyst workstations. Each workstation was equipped with 3 large monitors, which enabled the analyst (or a student) to visualize the different information items (charts, graphs, and recommendations) that the suite of tools comprising the framework was automatically generating by analyzing raw network data. The workstations were physically deployed in one of our research labs in the Research Hall building, and connected to the system through the general GMU network. Instead, the servers were deployed in one of our dedicated racks in the Aquia data center, a state-of-the-art, secure data center offering the Mason research community colocation services designed to provide a secure operating environment dedicated to system availability and uptime.

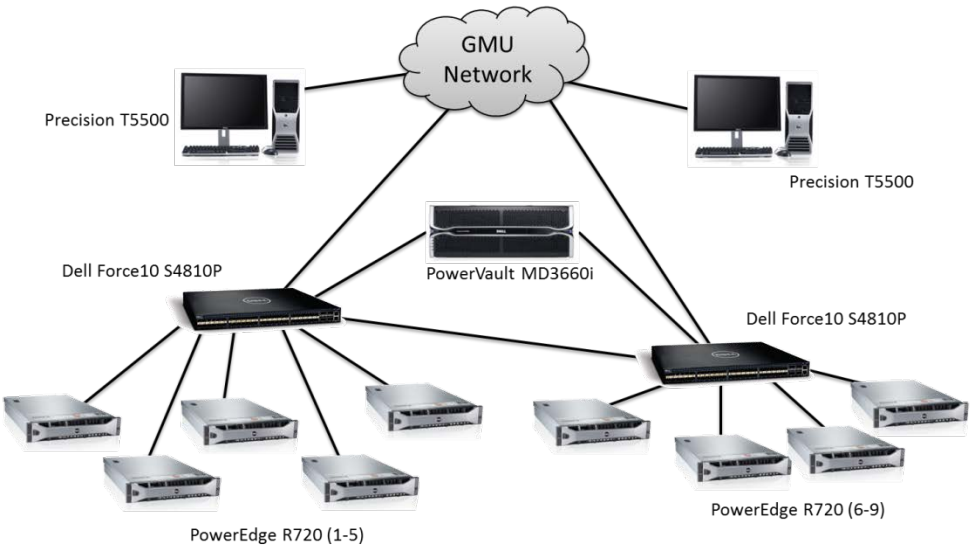

Figure 2 – Laboratory configuration

4. Publications

Our research resulted in the several publications, some of which are listed below:

1. R. Ganesan, S. Jajodia, A. Shah, and H. Cam, **"Dynamic scheduling of cybersecurity analysts for minimizing risk using reinforcement learning,"** *ACM Transactions on Intelligent Systems and Technology,* vol. 8, no. 1, July 2016.
2. E. Serra, S. Jajodia, S. Pugliese, A. Rullo, and V.S. Subrahmanian, **"Pareto-optimal adversarial defense of enterprise systems,"** *ACM Transactions on Information and System Security,* vol. 17, no. 3, Article 11, March 2015.
3. S. Venkatesan, M. Albanese, K. Amin, S. Jajodia, and M. Wright, **"A Moving Target Defense Approach to Mitigate DDoS Attacks against Proxy-Based Architectures,"** in *Proceedings of the 4th IEEE Conference on Communications and Network Security (IEEE CNS 2016)*, Philadelphia, Pennsylvania, USA, October 17-19, 2016.

4. M. Albanese, E. Battista, and S. Jajodia, **"Deceiving Attackers by Creating a Virtual Attack Surface,"** in *Cyber Deception: Building the Scientific Foundation*, S. Jajodia, V.S. Subrahmanian, V. Swarup, and C. Wang (Eds.), pages 169-201, Springer, 2016.

5. M. Albanese, E. Battista, and S. Jajodia, **"A Deception Based Approach for Defeating OS and Service Fingerprinting,"** in *Proceedings of the 3rd IEEE Conference on Communications and Network Security (IEEE CNS 2015)*, pages 253-261, Florence, Italy, September 28-30, 2015.

6. S. Venkatesan, M. Albanese, and S. Jajodia, **"Disrupting Stealthy Botnets through Strategic Placement of Detectors,"** in *Proceedings of the 3rd IEEE Conference on Communications and Network Security (IEEE CNS 2015)*, pages 55-63, Florence, Italy, September 28-30, 2015. [Best paper runner-up award]

7. M. Albanese, E. Battista, S. Jajodia, and V. Casola, **"Manipulating the Attacker's View of a System's Attack Surface,"** in *Proceedings of the 2nd IEEE Conference on Communications and Network Security (IEEE CNS 2014)*, pages 472-480, San Francisco, California, USA, October 29-31, 2014.

8. L. Wang, M. Zhang, S. Jajodia, A. Singhal, and M. Albanese, **"Modeling Network Diversity for Evaluating the Robustness of Networks against Zero-Day Attacks,"** in *Proceedings of the 19th European Symposium on Research in Computer Security (ESORICS 2014)*, pages 494-511, Wroclaw, Poland, September 7-11, 2014.

9. M. Albanese, H. Cam, and S. Jajodia, **"Automated Cyber Situation Awareness Tools for Improving Analyst Performance,"** in *Cybersecurity Systems for Human Cognition Augmentation*, R.E. Pino, A. Kott, and M. Shevenell (Eds.), vol. 62 of *Advances in Information Security*, pages 47-60, Springer, 2014.