CYMADA: Cybersecurity Assessment, Risk Management, Training Technologies and Data Analytics

Special session at CYBER 2016, Venice, Italy, Oct 9-13, 2016
http://www.iaria.org/conferences2016/CYBER16.html

Thomas Klemas
Principal Engineer
SimSpace Corporation
Boston, USA
tklemas@alum.mit.edu

***Abstract*—Cybersecurity is an important risk management consideration by any entity that uses computers. However, Cybersecurity is a complex subject because it comprises organizational, technological, structural, and human factors. Furthermore, the risks are compounded by the inherent contradiction that the primary benefit of using computer networks is connectivity to a seemingly infinite amount of resources, yet, it is this very connectivity that is a primary driver for cyber risk. As any complicated subject, it is crucial to study and assess Cybersecurity factors in order to understand the risks posed. Cyber analytics are an invaluable tool to assess cyber factors. One key element of such an assessment is to evaluate the proficiency of the organization's Cybersecurity operators. Cyber training is a key way to improve the skills and capabilities of Cybersecurity operators. Frequently, cyber training and assessment go hand in hand, as training events are used to assess an organizations Cybersecurity team. This special session will focus on topics related to Cybersecurity, cyber assessment, cyber risk management, cyber analytics, and cyber training.**

Keywords-Cybersecurity, Cybersecurity risk assessment, risk management, cyber training, cyber analytics, Sensemaking

I. Introduction

The Cyber 2016 special session for Cybersecurity Assessment, Risk Management, Training Technologies and Data Analytics (CYMADA) was proposed in order to provide coverage for the topics suggested by its name: Cybersecurity, cyber assessment, cyber risk management, cyber analytics, and related topics. Based on the submissions and accepted papers, the CYMADA session of Cyber 2016 will primarily focus on combined training and assessment technologies, a variety of cyber analytic methods, imaging applications, and network complexity measures. This diverse set of subtopics will provide a rich context for deeper discussion and thought on these categories, as well as the broader subjects that comprise the overall field and how they relate.

The first paper in the session delves into Cybersecurity Assessment topics [3] [4] and presents a training and evaluation architecture that enables decision makers to understand the composition and proficiency strengths of their Cyber workforce and to ascertain the skills and experience of new applicants or perspective hires. Cyber training assessment is important to help entities determine the level of skill and ability of the Cybersecurity operators that defend the entities' vital computer systems. By evaluating how the Cybersecurity operators respond to simulated threats on a network that is designed to emulate the entity's actual systems, the organization can gain understanding of a key component of its overall Cybersecurity posture.

There have been many previous attempts to develop certifications to establish that an individual possesses a minimum level of proficiency or skill. [7] However, the innumerable certifications differ in difficulty and comprehensiveness and yet, at the end of the day, only provide a pass-fail, binary evaluation of an individual's skills or proficiency. In order to gain greater insight into the fine-grained details and to quantify the degree of knowledge an skill, it is important to relate each of the questions contained in the assessment to skill areas and job specialty categorizations that are either standard, common, or traditional for the organization.

Cyber Sensemaking analytic methods play a critical role in developing insight from the data provided by the cyber assessor system. The Cyber Analytic techniques include an architecture, approach, and algorithms for collecting, labeling, and preprocessing the critical assessment data required to support the measures and metrics that help characterize the overall performance of the teams participating in the training event or assessment. Crucial insights are achieved by mapping every criteria against which the Cybersecurity operators are tested to the categories which are important and relevant to the entity.

The second paper in this session will concern novel imaging approaches and analytics related to them. Imaging is a critical visualization capability for many important applications. Three dimensional imagine techniques [2] and the systems that implement them, enable our armed forces during reconnoitering operations, empower our military weapons systems, reduce workload for architects by capturing accurate representations of a structure, including areas that may be hard to access, vastly improve our medical care, and achieve many more benefits that are derived from providing perspectives otherwise unavailable or images not accessible by any other means.

The serendipitous concurrence of inexpensive circuit boards, ubiquitous and inexpensive sensors, open system architecture advances, the Internet of Things, efficient data streaming, and sophisticated front-end web technology enable a vast variety of distributed, relatively inexpensive, modular, and even heterogeneous systems to be assembled that can solve problems using a collective, multi-element, or team approach. In particular, swarm imaging is an efficient alternative to 3-D cameras, drones, and other technologies that have been used for three-dimensional imaging. Advanced cyber analytical and processing methods can be combined with distributed swarms of cybernetic, robotic systems to provide inexpensive but highly effective visualization and imaging capabilities.

The third and final paper in this session will explore a key element that pertains to understanding the cyber environment, which is network complexity. Previous work focuses on physical and operational aspects of network complexity. [1] Most network theory texts will describe related concepts such as centrality, between-ness, degree [6], but do not have a definition for complexity. This may because complexity is a concept that is highly dependent on the application area for which it is intended. [5] [8] The network complexity definition that will be presented is intended for Cybersecurity applications and was designed to enable comparison between cyber training and assessment events, as well as between cyber systems.

Basically, the best definition for network complexity will be one that is useful for its intended application. For the purposes of Cybersecurity assessment and training, network complexity will be defined in terms of network attributes that contribute to cyber defensive difficulty or elevate the challenge of defending the network. This research leverages key ideas from information theory, probability, and applied mathematics to develop a definition for network complexity that provides excellent differentiation between networks based on critical defensive security attributes. This definition is useful when comparing cyber training events that are different and when comparing Cybersecurity assessments between entities.

II. Conclusion

The CYMADA session will cover a diverse collection of Cybersecurity subjects that will appeal to industry executives, practitioners, academics, and government officials, alike. The CYMADA session's broad appeal is also based on the extreme urgency of these topics to the executives and decision makers in industry and government. The material will be presented by industry and government presenters that have hands-on experience developing new technologies and approaches to address the challenges that comprise the CYMADA topic area. Thus, the audience will benefit from learning about innovative concepts presented by speakers with direct understanding of the challenges and the advances derived from solving them.

Acknowledgment

I would like to thank my colleagues at SimSpace for sharing their expertise and our CEO William Hutchinson "Hutch" for the tremendous support that motivated me to tackle the challenges and led me to contribute to the topics presented in this session. Collectively, these experiences, shared knowledge, and the exposure to so many new approaches allowed me to gain the broader experience necessary to chair a session as diverse as this one.

References

[1] M. Behringer, "Classifying Network Complexity", ACM 978-1-70668-749-3/09/12, 2009

[2] B. Javidi, F. Okano, and J.Y. Son, "Three-Dimensional Imaging, Visualization, and Display", Springer Publishing, 2009.

[3] FFIEC, "FFIEC Cybersecurity Assessment Tool,", https://www.ffiec.gov/cyberassessmenttool.htm, June 2015.

[4] FFIEC, "Overview for Chief Executive officers and Boards of Directors", https://www.ffiec.gov/cyberassessmenttool.htm, June 2015.

[5] M. Mitchell, "Complex Systems: Network Thinking", Santa Fe Institute, SFI Working Paper, 2006.

[6] M. Newman, Networks, An Introduction. Oxford : Oxford University Press, 2010.

[7] National Initiative for Cybersecurity Careers and Studies (NICCS), "Professional Certifications", Department of Homeland Security, https://niccs.us-cert.gov/training/professional-certifications

[8] Wikipedia Community, "Complexity", Wikipedia, https://en.wikipedia.org/wiki/Complexity, 2002.