SafeConfig 2015: Workshop on Automated Decision Making for Active Cyber Defense

Ehab Al-Shaer
University of North Carolina at Charlotte, USA
ealshaer@uncc.edu

Christopher Oehmen
Pacific Northwest National Laboratory, USA
chris.oehmen@pnnl.gov

M. Ashiqur Rahman
Tennessee Tech University, USA
marahman@tntech.edu

ABSTRACT

The 8th SafeConfig Workshop is held in Denver, Colorado USA on October 12, 2015 and being run with the conjunction of the 22nd ACM Conference on Computer and Communications Security (CCS). The title of this year's SafeConfig is "Automated Decision Making for Cyber Security". Today, the use of cyber technology is evolving rapidly. The computing and networking is everywhere, public to private organizations, large enterprises to individuals, and data centers to smart phones and Internet-of-Things. The highly growing use of the Internet also leads to newly evolving security threats. The automated decision making should be able to determine the security and resiliency of networked information systems and services. The integration of security requirements, capabilities, and deployment constraints in a unified framework will enable intelligent response, automated defense, and network resiliency.

Categories and Subject Descriptors

A.m [**General Literature**]: Miscellaneous

General Terms

Algorithms, Design, Economics, Experimentation, Human Factors, Management, Measurement, Performance, Reliability, Security, Theory, Verification

Keywords

Active cyber defense; automated decision making; security and resiliency systems.

1. INTRODUCTION

The high growth of cyber connectivity significantly increases the potential and sophistication of cyber-attacks. The new capabilities based on active cyber defense (ACD) are required to offer automated, intelligently-driven, agile, and resilient cyber defense. Both accurate "sense-making" based security analytics of the system artifacts (e.g., traces, configurations, logs, incident reports, alarms and network traffic), and provably-effective "decision-making" based on robust reasoning are required to enable ACD for cyber security and resiliency. Cyber security requires automated and scalable analytics in order to normalize, model, integrate, and analyze large and complex data to make correct decisions on time about security measures against threats.

The automated decision making goals is to determine and improve the security and resiliency of cyber systems and services. As the current technology moves toward 'smart' cyber-physical infrastructures as well as open networking platforms (e.g., software defined networking and virtual/cloud computing), the need for large-scale security analytics and automation for decision making significantly increases.

CCS'15, October 12-16, 2015, Denver, CO, USA
ACM 978-1-4503-3832-5/15/10.
http://dx.doi.org/10.1145/2810103.2812624

2. OBJECTIVE

The objective of this workshop is to offer a unique opportunity by bringing together researchers from academia, industry as well as government agencies to discuss the active cyber defense challenges, to exchange experiences, and to propose joint plans for promoting research and development in this area. SafeConfig was started in 2009 and has been continuously running since then. It provides a distinct forum to explore theoretical foundations, algorithmic advances, modeling, and evaluation of configuration related challenges for large scale cyber and cyberphysical systems.

3. TOPIC OF INTERESTS

This workshop looks for submissions from academia, industry, as well as government agencies presenting novel research results in all practical and theoretical aspects of automated decision making for security and resiliency of systems. Papers should reflect the construction, evaluation, application, or operation of automated decision making analytics for secure and resilient systems.

The following topics (but are not limited to) are of interest of this workshop:

- Analytics of attacks motive and attribution
- Accountability and provenance
- Attack prediction and attribution
- Attack forensics and automated incident analysis
- Big data analytics for cyber security
- Bio-inspired security
- Configuration testing, debugging, and evaluation
- Continuous monitoring and response
- Cyber agility and moving target defense

- Cyber resiliency
- Cyber-physical systems security
- Formal semantics of security policies
- Formal security analytics
- Model composition and integration
- Risk-aware and context-aware security
- Software defined networking and cloud computing security
- Security configuration verification and economics
- Security hardening and optimization
- Security games
- Security metrics
- Security policy management
- Theory of defense-of-depth

4. PROGRAM

The workshop is a one-day workshop. We have invited one keynote, in which Wende Peters from Johns Hopkins University Applied Physics Laboratory, USA will talk about the state of the art of security and resiliency requirements and the challenges and future directions for active cyber defense. There will be nine research paper presentations.

There was a total of 27 valid submissions. Unfortunately, we were not able to accommodate all worthy papers. We have accepted eight full papers and one short papers for the workshop presentation after a rigorous review process and a discussion phase. The acceptance rate of regular papers is around 29% only. The presentations are grouped in two sessions based on topics.

The program also includes a panel discussion. In this panel session, a collection of academic, government, and national laboratory representatives will discuss current drivers and emerging research priorities for automated and active cyber defense technologies for resilient systems. Scheduled panelists include Phil Quade (NSA), Arlette Hart (FBI), Ehab Al-Shaer (UNCC), and Chris Oehmen (PNNL).

5. ORGANIZERS

5.1 Program Chairs

Ehab Al-Shaer is a Professor and the Director of the Cyber Defense and Network Assurability (CyberDNA) Center in the College of Computing and Informatics at University of North Carolina Charlotte. He received his MSc and Ph.D. in Computer Science from the Northeastern University (Boston, MA) and Old Dominion University (Norfolk, VA) in 1998 and 1994 respectively. His primary research areas are network security, security management, fault diagnosis, and network assurability. Prof. Al-Shaer edited/co-edited more than 10 books and book chapters, and published about 150 refereed journals and conferences papers in his area. Prof. Al-Shaer is the General Chair and Co-Chair of many conferences and workshops including IM 2007, POLICY 2008, ANM-INFOCOM 2008, ACM CCS 2010.

Christopher Oehmen is the Chief Scientist of the Asymmetric Resilient Cybersecurity research initiative at Pacific Northwest National Laboratory (PNNL). He received a B.A. in Physics and Mathematics from Saint Louis University in 1995, and M.S. (1999) and Ph.D. (2003) in Biomedical Engineering from the Joint Graduate Program by the University of Memphis and the University of Tennessee Health Science Center. During his 11 years at PNNL, Dr. Oehmen has led a variety of research projects focused on applying fundamental sciences to challenges in national security, in particular cybersecurity. He has previously served as organizer for SIAM minisymposia on high performance sequence alignment in 2006 and 2008. Most recently he co-organized the Asymmetry in Resilience (AiR) meeting in 2014.

Mohammad Ashiqur Rahman received the BSc and MSc degrees in computer science and engineering from Bangladesh University of Engineering and Technology (BUET), Dhaka, in 2004 and 2007, respectively, and the PhD degree in computing and information systems from the University of North Carolina at Charlotte (UNC Charlotte), in 2015. He is currently assistant professor in the Department of Computer Science at Tennessee Tech University. His primary research interests include cyber infrastructure security analytics and automation, risk analysis and security hardening, resilient architecture synthesis, network security by deception and proactive defense modeling, and resource allocation and optimal management.

5.2 TPC Members

Alwyn Goodloe, NASA, USA
Ambareen Siraj, Tennessee Tech University, USA
Anupam Joshi, UMBC, USA
Brighten Godfrey, UIUC, USA
David Manz, Pacific Northwest National Laboratory, USA
Dong-Seong Kim, University of Canterbury, New Zealand
Errin Fulp, Wake Forest University, USA
Gail-Joon Ahn, Arizona State University, USA
Geoffrey Xie, Naval Postgraduate School, USA
Guevara Noubir, Northeastern University, USA
Hamed Okhravi, MIT Lincoln Laboratory, USA
HariGovind Ramasamy, IBM Research, USA
Hong Li, Intel Corporation, USA
John Goodall, Oak Ridge National Lab, USA
Julio Rodriguez, Idaho National Laboratory, USA
Indrajit Ray, Colorado State University, USA
Khaled Salah, KUSTAR, UAE
Krishna Kant, George Mason University, USA
Lisandro Granville, UFRGS, Brazil
Marco Carvalho, Florida Institute of Technology, USA
Mohamed Shehab, UNC Charlotte, USA
Michael Atighetchi, BBN Technologies, USA
Peng Liu, Pennsylvania State University, USA
Peter Mueller, IBM , Switzerland
Quanyan Zhu, New York University, USA
Rick Kuhn, NIST, USA
Rosalie McQuaid, MITRE, USA
Steven Borbash, National Security Agency, USA
Seraphin Calo, IBM Research, USA
Xinming Ou, Kansas State University, USA
Walid Saad, Virginia Tech, USA
Wende Peters, JHUAPL, USA
Yong Guan, Iowa State University, USA
Yung Ryn (Elisha) Choe, Sandia National Laboratories, USA

6. ACKNOWLEDGMENTS

We would like to thank all authors who submitted their contributions to SafeConfig'15. We are thankful to the anonymous external reviewers for their excellent work to review the submitted papers.