SafeConfig'17: Applying the Scientific Method to Active Cyber Defense Research

Nicholas J. Multari
Pacific Northwest National Lab,
Richland, WA, USA
nick.multari@pnnl.gov

Anoop Singhal
National Inst for Standards and
Technology, Rockville, MD, USA
anoop.singhal@nist.gov

Erin Miller
Pacific Northwest National Lab,
Richland, WA, USA
erin.miller@pnnl.gov

ABSTRACT

The focus of this workshop is the application of scientific practices to cyber security research. The objective of this workshop is examine the implementation of science practices in cyber defense research and understand the ramification of tradeoffs between simplifications to obtain interpretable results vs. observational studies of systems in the wild where the results can lead to ambiguous interpretations. The research papers accepted addressed a wide variety of technical questions in the cyber domain and the maturity of the work spanned the range of initial ideas and proofs of concept to mature work that is ready for operational implementation. Papers were evaluated for the reproducibility of the work as represented by the documentation of methods and testing environments.

CCS CONCEPTS

• General and reference~Experimentation • Security and privacy • Networks~Network security • Networks~ Network experimentation • Software and its engineering~Software verification and validation

KEYWORDS

SafeConfig; Testing; Validation; Security; Resilience; cyber; testbeds; metrics; cyber experimentation; science of cybersecurity

1 INTRODUCTION

Recently, there has been a great deal of interest about the science of cybersecurity[1,2,3,4]. In order to be considered scientific, the processes from concept through testing must follow a series of steps to ensure repeatable, reproducible and therefore verifiable results.

These steps include:

- Define a tractable problem.
- Ensure falsifiability
- Obtain ground truth
- Document assumptions and test them
- Start with simple experiments
- Assess progress to the larger problem

Upon completing this cycle, the process repeats with previous results incorporated into the problem and assumptions.

The focus of this workshop is the application of scientific practices to cyber security research. The objective of this workshop is examine the implementation of science practices in cyber defense research and understand the ramification of tradeoffs between simplifications to obtain interpretable results vs. observational studies of systems in the wild where the results can lead to ambiguous interpretations.

2 TOPICS

This workshop will consist of papers, presentations, and a panel discussing cyber security research and the means of applying the scientific processes to that research. To obtain a broad swath of areas in which these process could be applied, the following topics are of interest of this workshop:

- Configuration testing, forensics, debugging and evaluation.;
- Continuous monitoring and response;
- Cyber resiliency, agility and moving target defense;
- Cost effectiveness;
- Resilience/ agility effectiveness;
- Testbeds;
- Research Infrastructure;
- Verification techniques;
- Validation techniques;
- Testing & evaluation methods;
- Cyber-physical systems security;
- Security configuration verification and economics;
- Security metrics including adversarial and user measures;
- Security policy management;
- Theory of defense-of-depth;
- Mission metrics to include mission assurance, mission measures, and conflicting mission management.

CCS'17, October 30-November 3, 2017, Dallas, TX, USA.

ACM ISBN 978-1-4503-4946-8/17/10.
DOI: https://doi.org/10.1145/3133956.3137054

3 PROGRAM

The workshop will consist of a combination of peer-reviewed and invited papers, a keynote presentation and a panel.

The keynote presentation will be given by Dr. William (Bill) Sanders. Bill is the Department Head of the Electrical and Computer Engineering Department at the University of Illinois at Urbana/Champaign. His presentation will discuss the processes in going from good science to good engineering in the context of cyber security and cyber resilience. The panel will consist of Bill and professors from University of Texas at Dallas, the University of Colorado at Boulder, and at least one other panellist to be named shortly. In addition, each of the panellist will present their introductory remarks as invited talks.

The remainder of the program will consist of 15 and 30 minute presentations by the authors of accepted papers. Full papers authors will receive the 30 minutes each while the short paper authors will get 15 minutes each.

4 PROGRAM COMMITTEE

Steering Committee

Ehab Al-Shaer, UNC Charlotte, USA
Chris Oehmen, Pacific Northwest National Lab, USA
Krishna Kant, Temple University, USA

Technical Committee

Michael Atifhetchi, Raytheon Corp BBN, USA
Salman Baset, IBM, USA
Steve Borbash, US Department of Defense, USA
Eric Burger, Georgetown University, USA
Seraphin Calo, IBM, USA
Thomas Carroll, Pacific Northwest National Lab, USA
Andrea Ceccarelli, Universita degli Studi di Firenze, IT
Yung Ryn Choe, Sandia National Lab, USA
Naranker Dulay, Imperial College, UK
Thomas Edgar, Pacific Northwest National Lab, USA
Alwyn Goodloe, NASA Langley Research Center, USAYong Guan, Iowa State University, USA
Krishna Kant, Temple University, USA
DongSeong Kim, University of Canterbury, NZ
Richard Kuhn, National Institute of Standards & Technology, USA
Alex Liu, Michigan State University, USA
Peng Liu, Penn State University, USA
Emil Lupu, Imperial College, UK
Luigi Mancini, Universita di Roma La Sapienza, Italy
Mohammad Rahman, Tennessee Tech, USA
Walid Saad, Virginia Tech, USA
Mahesh Tripunitara, University of Waterloo, CA
Carlos Westphall, Federal University of Santa Catarina, BR
Geoffrey Xie, Naval Postgraduate School, USA
Jeff Yan, Lancaster University, UK
Daphne Yao, Virginia Tech, USA

5 WORKSHOP CHAIRS

Nicholas J. Multari provides programmatic and technical guidance to cybersecurity research programs at the Pacific Northwest National Lab (PNNL). Prior to joining PNNL, he led the trusted cyber technology research at Boeing Research and Technology in Seattle, Washington. In 2008, he served as a consultant to the USAF Scientific Advisory Board (SAB) investigating the effects of the contested cyber environment on the USAF mission. Other positions held include five years as a Senior Security Engineer with Scitor Corporation in Northern Virginia, and 20 years as a computer scientist in the Air Force retiring as a Lt. Col. He is a member of external advisory boards at University of Washington and Iowa State University and is an associate editor of the Data and Knowledge Engineering Journal by Elsevier. He received his PhD in computer science from the University of Texas at Austin.

Anoop Singhal, is currently a Senior Computer Scientist in the Computer Security Division at the National Institute of Standards and Technology (NIST) in Gaithersburg, MD. He received his Ph.D. in Computer Science from Ohio State University, Columbus, Ohio. His research interests are in network security, network forensics, cloud computing security and data mining systems. He is a member of ACM, senior member of the IEEE and he has co-authored over 50 technical papers in leading conferences and journals. He has two patents in the area of attack graphs and he has also co-edited a book on Secure Cloud Computing.

Erin Miller is the current chair of PNNL's Science Council, a group consisting of empirical researchers whose purpose is bringing science-based practices to cyber security research. She is a research scientist in the Radiation Detection & Nuclear Sciences group at PNNL, and the Technical Team Lead for Radiation Imaging and Materials Science. She has lead projects developing methods for gratings-based x-ray imaging for explosives detection; gamma emission tomography for verification of nuclear fuel; and inverse problems in radiation detection: localizing and describing radioactive sources in aerial survey, pedestrian search, and in combination with radiographic data in cargo containers. She holds a PhD in Physics from the University of Washington.

REFERENCES

[1] Tardiff et al., "Applying the Scientific Method to Cybersecurity Research" (2016), *in* Proceedings of the 2016 IEEE International Symposium on Technologies for Homeland Security, Boston, MA.

[2] https://www.afcea.org/committees/cyber/documents/ScienceofSecurityFinal_000.pdf

[3] https://www/nsf.gov/news/news_summ.jsp?cntn_id=190444

[4] http://webhost.laas.fr/TSF/IFIPWG/Workshops&Meetings/67/index.htm