16th Cyber Security Experimentation and Test Workshop

USC-ISI, August 7, 2023

Welcome to CSET'23!

- Workshop created in recognition of importance of experimentation and test to cybersecurity R&D
- 16th workshop:
  - 2008-2019 held with USENIX Security
  - 2020-2022 held virtually
  - 2023 held as hybrid, sponsored by USC-ISI in cooperation with USENIX
- Workshop – discussion and interaction are encouraged!!
- No-host dinner, 6pm tonight, Sapori Restaurant

Submission statistics

- 19 papers submitted
- Each paper was anonymized
- Each paper received between 3 and 4 reviews

Program statistics

- 9 papers accepted
  - 7 regular papers, 2 short papers
  - 8 research papers, one position paper
  - 5 papers will be presented in person, 4 will be presented live on Zoom
  - Country representation from the Belgium, Japan, Pakistan, and the US
- 3 papers have already released their research artifact
- In the spirit of a true workshop, we allocated 30 minutes for each paper

Program at-a-glance (1)

8:30-8:40	**Opening remarks** Terry Benzel, USC-ISI and Gianluca Stringhini, Boston University
8:40-9:45	**Keynote: Critical Consequences – Rethinking the Cyber Protection of Critical Infrastructure** Virginia Wright, Idaho National Laboratory
9:45-10:15	**Coffee break**
10:15-11:45	**Paper session 1 - Malware and vulnerabilities** (Session chair: Terry Benzel, USC-ISI) **Towards Reproducible Ransomware Analysis** Shozab Hussain (LUMS), Muhammad Musa (LUMS), Turyal Neeshat (LUMS), Rja Batool (LUMS), Omer Ahmed (LUMS), Fareed Zaffar (LUMS), Ashish Gehani (SRI), Andy Poggio (SRI), Maneesh Yadav (SRI) **An Attacker's Dream? Exploring the Capabilities of ChatGPT for Developing Malware** Yin Minn Pa Pa (Yokohama National University), Shunsuke Tanizaki (Yokohama National University), Tetsui Kou (Yokohama National University), Michel van Eeten (Delft University of Technology/ Yokohama National University), Katsunari Yoshioka (Yokohama National University), Tsumomu Matsumoto (Yokohama National University) **User Profiling and Vulnerability Introduction Prediction in Social Coding Repositories: A Dynamic Graph Embedding Approach** Agrim Sachdeva (Indiana University), Ben Lazarine (Indiana University), Hongyi Zhu (The University of Texas at San Antonio), Sagar Samtani (Indiana University)
11:45-1:00	**Lunch break**

Program at-a-glance (2)

1:00-2:30 **Paper session 2 - Simulators and security exercises** (Session chair: Ariana Mirian, UCSD)

Cadence: A Simulator for Human Movement-based Communication Protocols
Harel Berger (Georgetown University), Micah Sherr (Georgetown University), Adam Aviv (George Washington University)

Battle Ground: Data Collection and Labeling of CTF Games to Understand Human Cyber Operators
Geogel M. Savin (United States Naval Academy), Ammar Asseri (United States Naval Academy), Josiah Dykstra (National Security Agency), Jonathan Goohs (Cyber Strike Activity Sixty-Three, USN), Anthony Melaragno (United States Naval Academy), William Casey (United States Naval Academy)

BGPy: The BGP Python Security Simulator
Justin Furuness (University of Connecticut), Cameron Morris (University of Connecticut), Reynaldo Morillo (University of Connecticut), Amir Herzberg (University of Connecticut), Bing Wang (University of Connecticut)

2:30-3:00 **Coffee break**

3:00-4:30 **Paper session 3 - Research practices and risks** (Session chair: David Balenson, USC-ISI)

In the Line of Fire: Risks of DPI-triggered Data Collection
Ariana Mirian (UCSD), Alisha Ukani (UCSD), Ian Foster (DNS Coffee), Gautam Akiwate (Stanford University), Taner Halicioglu (Independent), Cindy Moore (UCSD), Alex C. Snoeren (UCSB), Geoffrey Voelker (UCSD), Stefan Savage (UCSD)

Analyzing Cyber Security Research Practices through a Meta-Research Framework
Victor Le Pochat (imec-DistriNet, KU Leuven), Wouter Joosen (imec-DistriNet, KU Leuven)

Designing and Conducting Usability Research on Social Media Misinformation with Low Vision or Blind Users
Filipo Sharevski (DePaul University), Aziz Zeidieh (University of Illinois Urbana-Champaign)

6:00 **No-Host Dinner at Sapori Restaurant**

Thanks to the program committee!

- Alefiya Hussain, USC Information Sciences Institute
- Alessandro Erba, CISPA Helmholtz Center for Information Security
- Alice Hutchings, University of Cambridge
- Amin Kharraz, Florida International University
- Ananta Soneji, Arizona State University
- Andreas Pitsillidis, Bridgewater Associates
- Brian Kondracki, Stony Brook University
- Cormac Herley, Microsoft Research
- Erik Kline, Information Sciences Institute
- Guilhem Lacombe, CEA LIST
- Inna Kouper, Indiana University
- Josiah Dykstra, National Security Agency
- Julio Hernandez-Castro, University of Kent
- Kimberly Tam, University of Plymouth
- Lianying Zhao, Carleton University
- Lorenzo De Carli, University of Calgary
- Marco Balduzzi, Trend Micro
- Matt Bishop, University of California at Davis
- Mohit Singhal, University of Texas at Arlington
- Nektarios Leontidis, Meta
- Prasad Calyam, University of Missouri-Columbia
- Thijs van Ede, University of Twente
- Urko Zurutuza, Mondragon Unibertsitatea
- Xueyuan Han, Wake Forest University
- Yun Shen, Netapp
- Yuping Wang, Boston University
- Zhibo "Eric" Sun, Drexel University

Thanks to the organizing committee!

Program chairs

- Deniz Gurkan, Kent State University
- Gianluca Stringhini, Boston University

Publication chair

- Giorgio Giacinto, University of Cagliari, Italy

Registration chair

- David Balenson, USC Information Sciences Institute

Steering committe

- Terry V. Benzel, USC Information Sciences Institute
- Jelena Mirkovic, USC Information Sciences Institute
- Sean Peisert, University of California, Davis, and Lawrence Berkeley National Laboratory
- Stephen Schwab, USC Information Sciences Institute