CSAW'21 Applied Research Competition

US-CANADA FINALIST PAPERS

Papers that are available online are linked in the title. Presenters are in bold. Papers are listed in order of paper number.

Paper 41 **Finding Bugs Using Your Own Code: Detecting Functionally-similar yet Inconsistent Code**
Reza Mirzazade Farkhani (Northeastern University), Mansour Ahmadi (Northeastern University), Ryan Williams (Northeastern University), Long Lu (Northeastern University)

Paper 56 **Bypassing memory safety mechanisms through speculative control flow hijacks**
Andrea Mambretti (Northeastern University), Alexandra Sandulescu (IBM Research Europe - Zurich), Alessandro Sorniotti (IBM Research Europe - Zurich), William Robertson (Northeastern University), Engin Kirda (Northeastern University), Anil Kurmus (IBM Research Europe - Zurich)

Paper 65 **When Malware Changed Its Mind: An Empirical Study of Variable Program Behaviors in the Real World**
Erin Avllazagaj (University of Maryland, College Park), Ziyun Zhu (Facebook), Leyla Bilge (NortonLifelock Research Group), Davide Balzarotti (EURECOM), Tudor Dumitras (University of Maryland, College Park)

Paper 69 **Fill in the blanks: Empirical analysis of the privacy threats of browser form autofill**
Xu Lin (University of Illinois Chicago), Panagiotis Ilia (University of Illinois Chicago), Jason Polakis (University of Illinois Chicago)

Paper 74 **Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits**
Brian Kondracki (Stony Brook University), Babak Amin Azad (Stony Brook University), Oleksii Starov (Palo Alto Networks), Nick Nikiforakis (Stony Brook University)

Paper 81 **STOCHFUZZ: Sound and Cost-effective Fuzzing of Stripped Binaries by Incremental and Stochastic Rewriting**
Zhuo Zhang (Purdue University), Wei You (School of Information, Renmin University), Guanhong Tao (Purdue University), Yousra Aafer (University of Waterloo), Xuwei Liu (Purdue University), Xiangyu Zhang (Purdue University)

Paper 90 **Systematic Evaluation of Privacy Risks of Machine Learning Models**
Liwei Song (Princeton University), Prateek Mittal (Princeton University)

Paper 93 **Доверяй, но проверяй: SFI safety for native-compiled Wasm**
Evan Johnson (UC San Diego), David Thien (UC San Diego), Yousef Alhessi (UC San Diego), Shravan Narayan (UC San Diego), Fraser Brown (Stanford and CMU), Tyler McMullen (Fastly Labs), Stefan Savage (UC San Diego), Deian Stefan (UC San Diego)

Paper 105 **Experiences Deploying Multi-Vantage-Point Domain Validation at Let's Encrypt**
Henry Birge-Lee (Princeton University), Liang Wang (Princeton University), Daniel McCarney (Square Inc.), Roland Shoemaker (Unaffiliated), Jennifer Rexford (Princeton University), Prateek Mittal (Princeton University)

Paper 109 **Zero Knowledge Proofs for Decision Tree Predictions and Accuracy**
Jiaheng Zhang (University of California Berkeley), Zhiyong Fang (Texas A&M University), Yupeng Zhang (Texas A&M University), Dawn Song (University of California Berkeley)