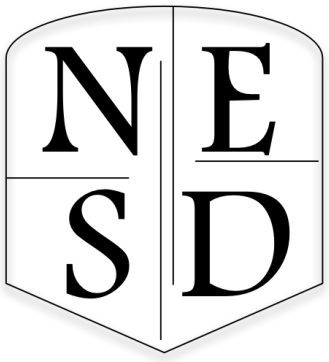
NEW ENGLAND SECURITY DAY FALL 2017
FRIDAY, SEPTEMBER 29, 2017

CONFERENCE ITINERARY AND INFORMATION

Interdisciplinary Science and Engineering Complex
Northeastern University
805 Columbus Avenue
Boston, MA 02115



Northeastern University
Cybersecurity and Privacy Institute

Northeastern University
College of Computer and Information Science

NEW ENGLAND SECURITY DAY FALL 2017

All speaker presentations will be held in the ISEC auditorium. Coffee, food breaks, and poster sessions will take place in the ISEC atrium.

CONFERENCE SCHEDULE

Friday, September 29, 2017

8:00am Breakfast and Registration

8:50am Opening Remarks

9:00am Session 1

Bog: An Ensemble Approach to Building Failure-Resistant Password-Based Key Derivation Functions

E. Heilman (Boston University), J. Hennessey (Boston University), S. Scheffler (Boston University), M. Varia (Boston University)

Reusable Key Derivation from the Iris

S. Simhadri (University of Connecticut), J. Steel (University of Connecticut), B. Fuller (University of Connecticut)

Algorand: Scaling Byzantine Agreements for Cryptocurrencies

Yossi Gilad (Boston University and MIT), Rotem Hemo (MIT), Silvio Micali (MIT), Georgios Vlachos (MIT) and Nickolai Zeldovich (MIT)

10:15am Coffee Break

10:45am Session 2

Timecop: Efficient Buffer Overflow Prevention

B. Powers (University of Massachusetts Amherst), E. Berger (University of Massachusetts Amherst)

A Modular, User-Centric Security Analysis of OpenStack

H. Maleki (University of Connecticut), K. Hogan (MIT), R. Rahaeimehr (University of Connecticut), J. Hennessey (Boston University), R. Canetti (Boston University), M. Varia (Boston University), M. van Dijk (University of Connecticut), H. Zhang (University of Connecticut)

Side-channel Attacks on SGX Enclaves

A. Moghimi (Worcester Polytechnic Institute)

12:00pm Lunch Break and Poster Session

1:30pm **Session 3**

Characterizing the Nature and Dynamics of Tor Exit Blocking
R. Singh (University of Massachusetts Amherst), R. Nithyanand (University of Massachusetts Amherst), S. Afroz (ICSI, UC Berkeley), P. Pearce (UC Berkeley), M. C. Tschantz (ICSI), P. Gill (University of Massachusetts Amherst), V. Paxson (ICSI, UC Berkeley)

Toward usable network traffic policies for IoT devices in consumer networks
N. DeMarinis (Brown University), R. Fonseca (Brown University)

A Longitudinal, End-to-End View of the DNSSEC Ecosystem
T. Chung (Northeastern University), R. van Rijswijk-Deij (University of Twente and SURFnet), B. Chandrasekaran (TU Berlin), D. Choffnes (Northeastern University), D. Levin (University of Maryland), B. M. Maggs (Duke University and Akamai Technologies), A. Mislove (Northeastern University), C. Wilson (Northeastern University)

2:45pm Coffee Break

3:15pm **Session 4**

Introducing the MassBrowser Censorship Circumvention System
A. Houmansadr (University of Massachusetts Amherst)

Identifier Binding Attacks and Defenses in Software-Defined Networks
A. S. Buyukkayhan (Northeastern University), A. Oprea (Northeastern University), Z. Li (RSA Laboratories), W. Robertson (Northeastern University)

Lens on the endpoint: Hunting for malicious software through endpoint data analysis
A. S. Buyukkayhan (Northeastern University), A. Oprea (Northeastern University), Z. Li (RSA Laboratories), W. Robertson (Northeastern University)

4:30pm Closing Remarks

LIST OF POSTERS

1. Apache Spot. *D. Kwok (Cloudera, Inc)*
2. How to Catch when Proxies Lie. *Z. Weinberg (CMU / UMass), N. Christin (CMU), V. Sekar (CMU)*
3. Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning
4. Better to use a lock screen than to worry about saving a few seconds of time: Effect of Fear Appeal in the Context of Smartphone Locking Behavior
5. Studying TLS Usage in Android using Lumen. *A. Razaghpanah (Stony Brook University), A. A. Niaki (University of Massachusetts Amherst)*
6. Estimation of Miner Hash Rates and Consensus on Blockchains. *A. P. Ozisik (UMass Amherst), G. Bissias (UMass Amherst), B. N. Levine (UMass Amherst)*
7. High Capacity Covert Communications Through Multimedia Social Networks. *A. Sepahi (University of Massachusetts Amherst), A. Houmansadr (University of Massachusetts Amherst), D. L. Goeckel (University of Massachusetts Amherst), D F. Towsley (University of Massachusetts Amherst)*
8. MassBrowser: A New Censorship Circumvention Tool. *A. Houmansadr (University of Massachusetts Amherst)*
9. Fingerprinting user behavior through mobile advertisements. *K. Sung (University of Massachusetts Amherst), B. Levine (University of Massachusetts Amherst), M. Corner (University of Massachusetts Amherst)*
10. A Churn for the Better: Localizing Censorship using Network-level Path Churn and Network Tomography. *S. Cho (Stony Brook University), R. Nithyanand (Stony Brook University), A. Razaghpanah (Stony Brook University), P. Gill (University of Massachusetts, Amherst)*
11. COMP 50 / PS 188: Cyber Security and Cyber Warfare at Tufts University. *M. Chow (Tufts University), J. Taliaferro (Tufts University)*
12. Cloud Privacy: Privacy Analysis of Cloud Monitoring Systems. *S. Krishnan (Northeastern University), A. Oprea (Northeastern University), C. Nita-Rotaru (Northeastern University)*
13. Compiler-Assisted Threshold Implementation Against Power Analysis Attacks. *P. Luo (Northeastern University), L. Zhang (Northeastern University), Z. H. Jiang (Northeastern University), Y. Fei (Northeastern University), A. A. Ding (Northeastern University), T. Wahl (Northeastern University)*
14. Practical Challenges of Type Checking in Control Flow Integrity. *R. M. Farkhani (Northeastern University), S. Arshad (Northeastern University), S. Jafari (Northeastern University)*

15. PTrix-AFL: PT-reinforced American Fuzzy Lop. *Y. Chen (Northeastern University)*
16. A New Proof-of-Work Target That Minimizes Blockchain Mining Time Variance. *G. Bissias (UMass Amherst), B. Levine (UMass Amherst)*
17. Privacy-Free Garbled Circuits for Formulas: Size Zero and Information-Theoretic. *Y. Kondi (Northeastern University), A. Patra (Indian Institute of Science)*
18. Automatic Vulnerability Finding in IoT/embedded device Firmware. *B. Feng (Northeastern University), L. Lu (Northeastern University)*
19. Scaling ORAM for Secure Computation. *J. Doerner (Northeastern University), A. Shelat (Northeastern University)*
20. Affordable and Comprehensive Remote Attestation for IoT Devices. *Z. Sun (Northeastern University), B. Feng (Northeastern University), L. Lu (Northeastern University)*
21. Covert Timing Channel on Renewal Packet Channels. *R. Soltani (UMass - ECE), D. Goeckel (UMass - ECE), D. Towsley (UMass - CICS), A. Houmansadr (UMass - CICS)*
22. A Longitudinal Study of PII Leaks Across Android App Versions. *J. Ren (Northeastern University)*
23. Off-path Man-in-the-Middle Attack on Tor Hidden Services. *A. Sanatinia (Northeastern University), G. Noubir (Northeastern University)*
24. Bog: An Ensemble Approach to Building Failure-Resistant Password-Based Key Derivation Functions. *E. Heilman (Boston University), J. Hennessey (Boston University), S. Scheffler (Boston University), M. Varia (Boston University)*
25. A Modular, User-Centric Security Analysis of OpenStack *H. Maleki (University of Connecticut), K. Hogan (MIT), R. Rahaeimehr (University of Connecticut), J. Hennessey (Boston University), R. Canetti (Boston University), M. Varia (Boston University), M. van Dijk (University of Connecticut), H. Zhang (University of Connecticut)*
26. Finding Constraint Logic Gadgets for Fuzzing. *J. Carlson (Veracode)*