UIUC Advanced Computer Security - Spring 21

ECE 524 / CS 563 Spring 2021 Advanced Computer Security

Tags: HW/OS, SOFT, APP, THEORY, NET, DATA

Preliminary

- Lattice-based access control models. Ravi S. Sandhu.

First week

- The Geometry of Innocent Flesh on the Bone: Return-into-libc without Function Calls (on the x86) Hovav Shacham. CCS 2007.
- “Weird Machines” in ELF: A Spotlight on the Underappreciated Metadata. Rebecca Shapiro, Sergey Bratus, Sean W. Smith. WOOT 2013.

Language-based approach to software security

- Information-Flow Security for a Core of JavaScript Daniel Hedin, Andrei Sabelfeld. CSF 2012.
- Verifying policy-based security for web services Karthikeyan Bhargavan, Cédric Fournet, Andrew D Gordon. CCS 2004.
- Small World with High Risks: A Study of Security Threats in the npm Ecosystem. Markus Zimmermann, Cristian-Alexandru Staicu, Cam Tenny, Michael Pradel. Usenix Security 2019.
- Secure web applications via automatic partitioning Stephen Chong, Jed Liu, Andrew Myers, Xin Qi, K. Vikram, Lantian Zheng, Xin Zheng. SOSP 2007.
- Joe-E: A Security-Oriented Subset of Java Adrian Mettler, David Wagner, Tyler Close. NDSS 2010.
- Robust Declassification Steve Zdancewic Andrew C. Myers. CSF 2001.
- Certificate Transparency. Ben Laurie. Communications of the ACM, 2014.
- Transparency overlays and their applications. Melissa Chase, Sarah Meiklejohn. CCS 2016.
- CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds Kirill Nikitin, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, Linus Gasser, Ismail Khoffi, Justin Cappos, Bryan Ford. Usenix Sec 2017.
- Finding The Greedy, Prodigal, and Suicidal Contracts at Scale. Ivica Nikolic, Aashish Kolluri, Ilya Sergey, Prateek Saxena, Aquinas Hobor. ACSAC 2018.
- Securify: Practical Security Analysis of Smart Contracts. Ivica Nikolic, Aashish Kolluri, Ilya Sergey, Prateek Saxena, and Aquinas Hobor. CCS 2019
- ZEUS: Analyzing Safety of Smart Contracts. Sukrit Kalra, Seep Goel, Mohan Dhawan, and Subodh Sharma. NDSS 2018

Cutting edge of cryptography-based system design

- ZoKrates - Scalable Privacy-Preserving Off-Chain Computations Jacob Eberhardt, Stefan Tai. CPSCom 2018.
- PhotoProof: Cryptographic Image Authentication for Any Set of Permissible Transformations. Assa Naveh and Eran Tromer. SP 2016.
- MP-SPDZ: A Versatile Framework for Multi-Party Computation Marcel Keller. CCS 2020.
- Secure Evaluation of Quantized Neural Networks. Anders Dalskov, Daniel Escudero, and Marcel Keller. PoPETS 2020.
- Bulletproofs: Short Proofs for Confidential Transactions and More. Benedikt Bunz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. SP 2018.
- DIZK.
- xJsnark: a framework for efficient verifiable computation Ahmed Kosba, Charalampos Papamanthou, Elaine Shi. SP 2018

Usability in Security

- Rethinking Connection Security Indicators. Adrienne Porter Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, Maximilian Walker, Christopher Albert Thompson, Mustafa Emre Acer, Elisabeth Morant, Sunny Consolvo. SOUPS 2016.
- Modeling Users’ Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings Jialiu Lin, Bin Liu, Norman Sadeh, and Jason I. Hong. SOUPS2014.
- A Typology of Perceived Triggers for End-User Security and Privacy Behaviors. Sauvik Das, Laura A. Dabbish, Jason I. Hong. SOUPS 2019.
- Deja Vu-A User Study: Using Images for Authentication. Rachna Dhamija and Adrian Perrig. Usenix Security 2000.
- "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. I. Reyes, P. Wijesekera, J. Reardon, A. E. B. On, A. Razaghpanah, N. Vallina-Rodriguez, S. Egelman. PoPETS 2018.
- Better managed than memorized? studying the impact of managers on password strength and reuse Sanam Ghorbani Lyastani, Michael Schilling, Sascha Fahl, Michael Backes, Sven Bugiel. (USENIX'18)
- On Enforcing the Digital Immunity of a Large Humanitarian Organization Stevens Le Blond, Alejandro Cuevas, Juan Ramon Troncoso-Pastoriza, Philipp Jovanovic ´ Bryan Ford, Jean-Pierre Hubaux. Oakland 2018.

Security and social media infrastructure

- SATE: Robust and Private Allegation Escrows Venkat Arun, Aniket Kate, Deepak Garg, Peter Druschel, Bobby Bhattacharjee. NDSS 2020.
- The Many Kinds of Creepware Used for Interpersonal Attacks Kevin A. Roundy, Paula Barmaimon Mendelberg, Nicola Dell, Damon McCoy, Daniel Nissani, Thomas Ristenpart, Acar Tamersoy. IEEE SP 2020.
- The Spyware Used in Intimate Partner Violence. Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, Thomas Ristenpart. IEEE SP 2018.
- Disinformation’s spread: bots, trolls and all of us. Kate Starbird. Nature 571, 449 (2019).
- Trafficking fraudulent accounts: The role of the underground market in Twitter spam and abuse. Usenix security 2013.
- Detecting Fake Accounts in Online Social Networks at the Time of Registrations CCS 2019.
- Deceptive Previews: A Study of the Link Preview Trustworthiness in Social Platforms. Giada Stivala, Giancarlo Pellegrino. NDSS 2020.
- SoK: Hate, Harassment, and the Changing Landscape of Online Abuse Kurt Thomas Devdatta Akhawe Michael Bailey Dan Boneh Elie Bursztein Sunny Consolvo Nicola Dell Zakir Durumeric Patrick Gage Kelley Deepak Kumar Damon McCoy Sarah Meiklejohn Thomas Ristenpart Gianluca Stringhini. SP 2021.
- A taste of tweets: reverse engineering Twitter spammers Chao Yang, Jialong Zhang, Guofei Gu. ACSAC 2014.
- On the Detection of Disinformation Campaign Activity with Network Analysis. Luis Vargas, Patrick Emami, Patrick Traynor, Traynor. CCSW 2020.
- Information security: where computer science, economics and psychology meet Ross Anderson and Tyler Moore. Phil. Trans. R. Soc.

Other topics

- Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet. Stephen Herwig, Katura Harvey, George Hughey, Richard Roberts, Dave Levin. NDSS 2019.
- Practicing a Science of Security: A Philosophy of Science Perspective Jonathan M. Spring, Tyler Moore, David J Pym. NSPW 2017.
- The Security Impact of HTTPS Interception. Z Durumeric, Z Ma, D Springall, R Barnes, N Sullivan, E Bursztein. NDSS 2017.
- Spectre Attacks: Exploiting Speculative Execution Paul Kocher, Jann Horn, Anders Fogh, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, Yuval Yarom. IEEE SP 2019
- Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors Yoongu Kim, Ross Daly, Jeremie Kim, Chris Fallin, Hye Lee, Chris Wilkerson, Konrad Lai, Onur Mutlu.