IEEE SecDev ’18 Accepted Tutorials

2. Secure Your Things: Secure Development of IoT Software with Frama-C. Allan Blanchard (Inria Lille – Nord Europe, France), Nikolai Kosmatov (CEA, Software Reliability and Security Lab, France), Frédéric Loulergue (School of Informatics Computing and Cyber Systems, Northern Arizona University)
3. Continuous Verification of Critical Software. Mike Dodds, Stephen Magill, Aaron Tomb (Galois, Inc.)
4. DeepState: Bringing Vulnerability Detection Tools into the Development Cycle. Peter Goodman, Gustavo Grieco (Trail of Bits, Inc.), Alex Groce (School of Informatics, Computing & Cyber Systems, Northern Arizona University)
5. Parry and RIPOSTE: Honing Cybersecurity Skills with Challenge-Based Exercises. Jan Werner (University of North Carolina at Chapel Hill), Fabian Monrose (University of North Carolina at Chapel Hill)
7. Building Secure Consortium Blockchains for Decentralized Applications. Cong Wang, Chengjun Cai (City University of Hong Kong)

IEEE SecDev ’18 Accepted Papers

1. Tyche: A Risk-Based Permission Model for Smart Homes. Amir Rahmati (Samsung Research America/Stony Brook University), Earlene Fernandes (University of Washington), Kevin Eykholt (University of Michigan), and Atul Prakash (University of Michigan)
2. BP: Formal Proofs, the Fine Print and Side Effects. Toby Murray (University of Melbourne) and Paul van Oorschot (Carleton University)
3. BP: Security Concerns and Best Practices for Automation of Software Deployment Processes - An Industrial Case Study. Vaishnavi Mohan (Deloitte Analytics Institute), Lotfi ben Othmane (Iowa State University), and Andre Kres (IBM)
4. Checked C: Making C Safe by Extension. Archibald Samuel Elliott (University of Washington), Andrew Ruef (University of Maryland), Michael Hicks (University of Maryland), and David Tarditi (Microsoft Research)
5. Transforming Code to Drop Dead Privileges. Xiaoyu Hu (BitFusion.io Inc.), Spyridoula Gravani (University of Rochester), Jie Zhou (University of Rochester), and John Criswell (University of Rochester)
7. **BP: DECREE: A Platform and Benchmark Corpus for Repeatable and Reproducible Security Experiments.** Lok Yan (Air Force Research Laboratory), Benjamin Price (MIT Lincoln Laboratory), Michael Zhivich (MIT Lincoln Laboratory), Brian Caswell (Lunge Technology), Christopher Eagle (Naval Postgraduate School), Michael Frantzen (Kudu Dynamics), Holt Sorenson (Google Inc.), Michael Thompson (Naval Postgraduate School), Timothy Vidas (Carnegie Mellon University), Jason Wright (Thought Networks), Vernon Rivet (MIT Lincoln Laboratory), Samuel Colt VanWinkle (MIT Lincoln Laboratory), and Clark Wood (MIT Lincoln Laboratory)

8. **There’s a Hole in the Bottom of the C: On the Effectiveness of Allocation Protection.** Ronald Gil (MIT CSAIL), Hamed Okhravi (MIT Lincoln Laboratory), and Howard Shrobe (MIT CSAIL).

9. **Light-touch Interventions to Improve Software Development Security.** Charles Weir (Lancaster University, UK), Lynne Blair (Lancaster University, UK), Ingolf Becker (University College London, UK), Angela Sasse (University College London, UK), and James Noble (Victoria University of Wellington, NZ)

10. **SGL: A domain-specific language for large-scale analysis of open-source code.** Darius Foo, Ang Ming Yi, Jason Yeo, and Asankhaya Sharma (SourceClear, Inc.)

11. **A Lingua Franca for Security by Design.** Alexander van den Berghe (imec-DistriNet, KU Leuven), Koen Yskout (imec-DistriNet, KU Leuven), Riccardo Scandariato (Software Engineering Division, University of Gothenburg), and Wouter Joosen (imec-DistriNet, KU Leuven).


13. **Towards Understanding the Adoption of Anti-Spoofing Protocols in Email Systems.** Hang Hu, Peng Peng, and Gang Wang (Virginia Tech)

14. **BP: Profiling Vulnerabilities on the Attack Surface.** Christopher Theisen, Hyunwoo Sohn, Dawson Tripp, and Laurie Williams (North Carolina State University)