2/27

The CHERI capability model: Revisiting RISC in an age of risk. Jonathan Woodruff et al. 2014 IEEE Symposium Security and Privacy, May 2014.

3/13

Effective and Efficient Malware Detection at the End Host. Clemens Kolbitsch, Paolo Milani Comparetti, Christopher Kruegel, Engin Kirda, Xiaoyong Zhou, and XiaoFeng Wang, 18th USENIX Security Symposium, 2009.

3/15

DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning. Min Du, Feifei Li, Guineng Zheng, Vivek Srikumar. In Proceedings of the 24th ACM Conference on Computer and COmmunications Security, 2017.

Using Hardware Features for Increased Debugging Transparency. Fengwei Zhang, Kevin Leach, Angelos Stavrou, Haining Wang, and Kun Sun, IEEE Symposium on Security and Privacy, 2015.

3/20

Producing Hook Placements to Enforce Expected Access Control Policies. Divya Muthukumaran, Nirupama Talele, Trent Jaeger, and Gang Tan. In Proceedings of the 2015 International Symposium on Engineering Secure Software and Systems (ESSoS), Mar. 2015.

DIFC Programs by Automatic Instrumentation. William R. Harris, Somesh Jha, and Thomas Reps, in Computer and Communications Security (CCS), 2010.

3/22

Sharing Mobile Code Securely With Information Flow Control. Owen Arden, Michael D. George, Jed Liu, K. Vikram, Aslan Askarov, Andrew

Myers. In Proceedings of the 2012 IEEE Symposium on Security and Privacy, 2012.

3/27

AEG: Automatic Exploit Generation. Thanassis Avgerinos, Sang Kil Cha, Brent Lim Tze Hao and David Brumley, in Proceedings of the 2011 Network and Distributed System Security Symposium, Feb. 2011.

3/29

Driller: Augmenting Fuzzing Through Selective Symbolic Execution. Nick Stephens, John Grosen, Christopher Salls, Andrew Dutcher, Ruoyu Wang, Jacopo Corbetta, Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna. Proceedings of the Network and Distributed System Security Symposium (NDSS), February 2016.

4/3

TrustShadow: Secure Execution of Unmodified Applications with ARM TrustZone. Le Guan, Peng Liu, Xinyu Xing, Xinyang Ge, Shengzhi Zhang, Meng Yu, and Trent Jaeger. In Proceedings of the 15th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys), June 2017.

4/5

VC3: Trustworthy Data Analytics in the Cloud using SGX. Felix Schuster, Manuel Costa, Cedric Fournet, Christos Gkantsidis, Marcus Peinado, Gloria Mainar-Ruiz, Mark Russinovich, IEEE Symposium on Security and Privacy, 2015.

4/10

Hacking in Darkness: Return-oriented Programming against Secure Enclaves. Jaehyuk Lee et al. In Proceedings of the 26th USENIX Security Symposium. August 2017.

Inferring Fine-grained Control Flow Inside SGX Enclaves with Branch

Shadowing. Sangho Lee, Ming-Wei Shih, Prasun Gera, Taesoo Kim, and Hyesoon Kim. In Proceedings of the 26th USENIX Security Symposium. August 2017.

4/12

SPROBES: Enforcing Kernel Code Integrity on the TrustZone Architecture. Xinyang Ge, Hayawardh Vijayakumar, and Trent Jaeger, Mobile Security Technologies Workshop, 2014.

LMP: Light-Weighted Memory Protection with Hardware Assistance. Wei Huang, Zhen Huang, Dhaval Miyani and David Lie. In Proceedings of the 2016 Annual Computer Security Applications Conference (ACSAC 2016), December 2016.

4/19

Policy-Sealed Data: A New Abstraction for Building Trusted Cloud Services. Nuno Santos, Rodrigo Rodrigues, Krishna P. Gummadi, Stefan Saroiu, in Proceedings of the 21st USENIX Security Symposium, 2012.

Unicorn: Two-Factor Attestation for Data Security. Mohammad Mannan, Beom Heyn Kim, Afshar Ganjali and David Lie, in Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS 2011). Pages 17-28. October 2011.

4/24

Security Analysis of Emerging Smart Home Applications. Earlence Fernandes, Jaeyeon Jung, Atul Prakash. Proceedings of the IEEE Symposium on Security and Privacy, 2016.

ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms. Yunhan Jack Jia, Qi Alfred Chen, Shiqi Wang, Amir Rahmati, Earlence Fernandes, Z. Morley Mao, Atul Prakash. Proceedings of the Network and Distributed Systems Symposium, 2017.