Hayawardh Vijayakumar

Security Research Engineer
Samsung KNOX ◇ Samsung Research America
Office : 665 Clyde Ave ◇ Mountain View, CA 94043
Email : hayawardh@gmail.com ◇ **Homepage:** `http://hvijay.github.io`

WORK EXPERIENCE

Security Research Engineer *Samsung Research America*, Mountain View, CA. 2014 - Current

- Member of the Samsung KNOX security team. Broadly responsible for reviewing design and auditing code of Samsung KNOX features for security, developing tools for automated testing, incident response, mentoring intern research projects and collaborating with universities on research projects.
- Current areas of research include ARM TrustZone, full-system emulation, and fuzz testing.

Research Assistant to Trent Jaeger, *Pennsylvania State University*, University Park, PA. 2008 - 2014

- My PhD dissertation was in operating systems security. I analyzed program interaction with the operating system they are deployed in, and how mismatches between programmer expectations of OS access control and the actual OS access control policies can affect security.
- Other areas of research were infrastructures for providing transparent verification of the cloud, ARM TrustZone-based kernel runtime monitoring, and analyzing security policies at multiple layers for mediation and consistency properties.

Research Intern *NEC Labs America*, Princeton, NJ. Summer 2013

- Worked on logging and transforming runtime traces of systems within NEC into an information flow graph, and wrote a subsequent analysis framework. A novel feature of the information flow graph was modeling OS semantics that tracked information flow not directly visible in traces.

Technical Intern *Qualcomm Innovation Inc. (QuicInc)*, Raleigh, NC. Summer 2010

- Worked as part of team optimizing Linux kernel for Google Chrome netbooks on Qualcomm hardware. I developed software to probe and test graphic stack capabilities in a black-box way, using which several driver bugs were discovered.

EDUCATION

Doctor of Philosophy, Computer Science and Engineering *May 2014*
The Pennsylvania State University, University Park, PA, USA
Advisor: Dr. Trent Jaeger

Bachelor of Engineering, Computer Science and Engineering *May 2007*
Sri Venkateswara College of Engineering, Anna University, Chennai, India

PUBLICATIONS

Peer-Reviewed Publications

[1] Lee Harrison, Hayawardh Vijayakumar, Rohan Padhye, Koushik Sen, and Michael Grace. PARTEMU: Enabling Dynamic Analysis of Real-World TrustZone Software Using Emulation. In *Proceedings of the 29th USENIX Security Symposium (USENIX Security 2020) (To Appear)*, August 2020.

[2] Rohan Padhye, Caroline Lemieux, Koushik Sen, Laurent Simon, and Hayawardh Vijayakumar. FuzzFactory: Domain-Specific Fuzzing with Waypoints. In *Proceedings of the 2019 Object-oriented Programming, Systems, Languages, and Applications (OOPSLA 2019) (To Appear)*, October 2019.

[3] Dave (Jing) Tian, Grant Hernandez, Joseph Choi, Vanessa Frost, Christie Raules, Kevin Butler, Patrick Traynor, Hayawardh Vijayakumar, Lee Harrison, Amir Rahmati, and Mike Grace. ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands within the Android Ecosystem. In *Proceedings of the 27rd USENIX Security Symposium (USENIX Security 2018)*, August 2018. [acceptance rate: 19.1% (100524)].

[4] Yaohui Chen, Yuping Li, Long Lu, Yueh-Hsun Lin, Hayawardh Vijayakumar, Zhi Wang, and Xinming Ou. InstaGuard: Instantly Deployable Hot-patches for Vulnerable System Programs on Android. In *Proceedings of the 2018 Network and Distributed System Security Symposium (NDSS 2018)*, February 2018. [acceptance rate: 21.5% (71/331)].

[5] Yaohui Chen, Dongli Zhang, Ruowen Wang, Ahmed Azab, Long Lu, Hayawardh Vijayakumar, and Wenbo Shen. Norax: Enabling Execute-Only Memory for COTS Binaries on AArch64. In *Proceedings of the 38th IEEE Symposium on Security and Privacy (Oakland 2017)*, May 2017. [acceptance rate: 13.3% (60/450)].

[6] Trent Jaeger, Xinyang Ge, Divya Muthukumaran, Sandra Rueda, Joshua Schiffman, and Hayawardh Vijayakumar. Designing for Attack Surfaces: Keep Your Friends Close, but Your Enemies Closer. In *Proceedings of the 5th International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE 2015)*, October 2015.

[7] Yuqiong Sun, Giuseppe Petracca, Trent Jaeger, Hayawardh Vijayakumar, and Joshua Schiffman. Cloud Armor: Protecting Cloud Commands from Compromised Cloud Services. In *Proceedings of the 8th IEEE International Conference on Cloud Computing (CLOUD 2015)*, June 2015.

[8] Hayawardh Vijayakumar, Xinyang Ge, Mathias Payer, and Trent Jaeger. JIGSAW: Protecting Resource Access by Inferring Programmer Expectations. In *Proceedings of the 23rd USENIX Security Symposium (USENIX Security 2014)*, August 2014. [acceptance rate: 19.1% (67/350)].

[9] Hayawardh Vijayakumar, Xinyang Ge, and Trent Jaeger. Policy Models to Protect Resource Retrieval. In *Proceedings of the 19th ACM Symposium on Access Control Models (SACMAT 2014)*, June 2014.

[10] Xinyang Ge, Hayawardh Vijayakumar, and Trent Jaeger. SPROBES: Enforcing Kernel Code Integrity on the TrustZone Architecture. In *Proceedings of the 3rd IEEE Mobile Security Technologies Workshop (MoST 2014)*, May 2014.

[11] Joshua Schiffman, Yuqiong Sun, Hayawardh Vijayakumar, and Trent Jaeger. Cloud verifier: Verifiable auditing service for iaas clouds. In *Proceedings of the IEEE 1st International Workshop on Cloud Security Auditing (CSA 2013)*, June 2013.

[12] Hayawardh Vijayakumar, Joshua Schiffman, and Trent Jaeger. Process firewalls: Protecting processes during resource access. In *Proceedings of the 8th ACM European Conference on Computer Systems (EUROSYS 2013)*, April 2013. [acceptance rate: 17.9% (28/156)].

[13] Trent Jaeger, Divya Muthukumaran, Joshua Schiffman, Yuqiong Sun, Nirupama Talele, and Hayawardh Vijayakumar. Configuring cloud deployments for integrity. In *Proceedings of the Computer And Security Applications Rendezvous: Cloud and Security (CESAR 2012)*, November 2012.

[14] Hayawardh Vijayakumar and Trent Jaeger. The right files at the right time. In *Proceedings of the 5th IEEE Symposium on Configuration Analytics and Automation (SAFECONFIG 2012)*, October 2012.

[15] Divya Muthukumaran and Sandra Rueda and Nirupama Talele and Hayawardh Vijayakumar and Trent Jaeger and Jason Teutsch and Nigel Edwards. Transforming Commodity Security Policies to Enforce Clark-Wilson Integrity. In *Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC 2012)*, December 2012. [acceptance rate: 19.0% (44/231)].

[16] Hayawardh Vijayakumar and Joshua Schiffman and Trent Jaeger. STING: Finding Name Resolution Vulnerabilities in Programs. In *Proceedings of the 21st USENIX Security Symposium (USENIX Security 2012)*, August 2012. [acceptance rate: 19.4% (43/222)].

[17] Joshua Schiffman and Hayawardh Vijayakumar and Trent Jaeger. Verifying System Integrity by Proxy. In *Proceedings of the 5th International Conference on Trust and Trustworthy Computing (TRUST 2012)*, June 2012.

[18] Hayawardh Vijayakumar and Guruprasad Jakka and Sandra Rueda and Joshua Schiffman and Trent Jaeger. Integrity Walls: Finding Attack Surfaces from Mandatory Access Control Policies. In *Proceedings of the 7th ACM Symposium on Information, Computer, and Communications Security (ASIACCS 2012)*, May 2012. [acceptance rate: 22% (35/159)].

[19] Hayawardh Vijayakumar and Joshua Schiffman and Trent Jaeger. A Rose by Any Other Name or an Insane Root? Adventures in Name Resolution. In *Proceedings of 7th European Conference on Computer Network Defense (EC2ND 2011)*, September 2011. [acceptance rate: 32%].

[20] Joshua Schiffman and Thomas Moyer and Hayawardh Vijayakumar and Trent Jaeger and Patrick McDaniel. Seeding Clouds with Trust Anchors. In *Proceedings of the 2010 ACM Workshop on Cloud Computing Security (CCSW 2010)*, October 2010.

[21] Divya Muthukumaran and Sandra Rueda and Hayawardh Vijayakumar and Trent Jaeger. Cut Me Some Security. In *Proceedings of the 3rd ACM Workshop on Assurable and Usable Security Configuration (SAFECONFIG 2010)*, October 2010.

[22] Sandra Rueda and Hayawardh Vijayakumar and Trent Jaeger. Analysis of Virtual Machine System Policies. In *Proceedings of the 14th ACM Symposium on Access Control Models and Technologies (SACMAT 2009)*, June 2009. [acceptance rate: 32% (24/75)].

[23] Thanukrishnan Srinivasan and R. Balakrishnan and S. A. Gangadharan and Hayawardh Vijayakumar. A Scalable Parallelization of All-Pairs Shortest Path Algorithm for a High Performance Cluster Environment. In *Proceedings of the 13th IEEE International Conference on Parallel and Distributed Systems (ICPADS 2007)*, December 2007.

[24] Thanukrishnan Srinivasan and R. Balakrishnan and S. A. Gangadharan and Hayawardh Vijayakumar. Supervised Grid-of-Tries: A Novel Framework for Classifier Management. In *Proceedings of the 8th International Conference on Distributed Computing and Networking (ICDCN 2006)*, December 2006. [acceptance rate: 25.3% (62/245)].

PROFESSIONAL ACTIVITIES

- **Program Commitee Member**:
  - Network and Distributed System Security Symposium (NDSS 2015),
  - ACM Symposium on Computer and Communications Security (CCS 2018),
  - Annual Computer Security Applications Conference (ACSAC 2014, 2015, 2016, 2017, 2018, 2019),
  - ACM Symposium on Information, Computer, and Communications Security (ASIACCS 2014, 2015),
  - ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2018),
  - International Conference on Information Systems Security (ICISS 2018),
  - IEEE Workshop on Mobile Security Technologies (MoST 2016, 2017),

SECURITY VULNERABILITIES DISCLOSED

- Ubuntu init scripts (arbitrary file create vulnerability (CVE-2011-3151)),
- lightdm (privilege escalation (CVE-2011-4406)),
- Icecat browser - GNU version of Firefox (Untrusted library search path)
- x2go VNC server/client (Untrusted library search path),
- mountall (Untrusted search path),
- apachectl (privilege escalation (CVE-2013-1048))