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. June 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, mentoring intern research projects and conducting university collaboration on research projects.

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.

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
PhD Dissertation: Protecting Programs During Resource Access
Advisor: Dr. Trent Jaeger

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

PEER-REVIEWED PUBLICATIONS

Google Scholar: https://scholar.google.com/citations?user=4y3hTDMAAAAJ&hl=en
dblp: http://dblp.uni-trier.de/pers/hd/v/Vijayakumar:Hayawardh

[1] 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)].

[2] 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)].

[3] 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.

[4] 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.

[5] 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)].

[6] 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.

[7] 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.

[8] 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.

[9] 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)].

[10] 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.

[11] 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.

[12] 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)].

[13] 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)].

[14] 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.

[15] 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)].

[16] 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%].

[17] 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.

[18] 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.

[19] 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)].

[20] 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.

[21] 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

I have served on the program committee of the following conferences and workshops:

- (NDSS 2015) Network and Distributed System Security Symposium
- (CCS 2018) ACM Conference on Computer and Communications Security
- (ACSAC 2014, 2015, 2016, 2017, 2018) Annual Computer Security Applications Conference
- (ASIACCS 2014, 2015) ACM Symposium on Information, Computer, and Communications Security
- (WiSec 2018) ACM Conference on Security and Privacy in Wireless and Mobile Networks
- (ICISS 2018) International Conference on Information Systems Security
- (MoST 2016, 2017) IEEE Workshop on Mobile Security Technologies
- (RESEC 2018) The First Radical and Experiential Security Workshop

SECURITY VULNERABILITIES REPORTED

I have found and reported the following security vulnerabilities. Three of these are in software that is widely deployed. I provide links to records in the major vulnerability tracking systems and vendor reports.

- Apache apachectl (privilege escalation (CVE-2013-1048))
  - http://www.securityfocus.com/bid/58325/info
  - http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2013-1048
  - https://vuldb.com/?id.7869
- Ubuntu lightdm (privilege escalation (CVE-2011-4406))
  - http://www.securityfocus.com/bid/51770
  - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4406
  - https://vuldb.com/?id.69375
- Ubuntu init scripts (arbitrary file create vulnerability (CVE-2011-3151))
  - https://bugs.launchpad.net/ubuntu/+source/selinux/+bug/876994
- Icecat browser - GNU version of Firefox (Untrusted library search path)
  - http://thread.gmane.org/gmane.comp.gnu.gnuzilla/2000
- x2go VNC server/client (Untrusted library search path)
  - http://lists.x2go.org/pipermail/x2go-dev/2012-January/003164.html

AWARDS AND SCHOLARSHIPS

- Outstanding Teaching Assistant Award, Computer Science and Engineering Department, Penn State University
- Medal for being placed 6th in the Asia region of The 31st Annual ACM International Collegiate Programming Contest (ACM ICPC 2006).
- Awarded scholarship in first semester of undergraduate study for outstanding performance.

TEACHING

- **CSE 543 Fall 2013** (Graduate-level Introduction to Computer and Network Security): **Co-instructor for course**. Prepared assignments and lectured on cryptography, software security and web security. Received an outstanding teaching assistant award for the same.
- **CSE 544 Spring 2013** (Graduate-level Advanced Systems Security): Delivered lectures on the MULTICS operating system.
- **CSE 543 Spring 2013** (Undergraduate-level Introduction to Computer and Network Security): Delivered lectures on web and cloud computing security.