Aravind Machiry

Affiliation Assistant Professor, Department of Electrical and Computer Engineering, Purdue University.

Contact Information

Purdue University
EE 333, School of Electrical and Computer Engineering
S465 Northwestern Ave.
West Lafayette, IN 47907.
United States of America

amachiry@purdue.edu
machiry.github.io
machiry
Google Scholar

Research Interests My research focuses on various aspects of system security, such as vulnerability detection, mobile security, trusted execution environments, static and dynamic analysis of source code, and binaries. I am also interested in developing novel static/dynamic program analysis techniques for system security problems. My research resulted in various Open-source security tools and several Common Vulnerability Exposures (CVEs) in critical system software such as kernel drivers and bootloaders.

Positions & Education

Assistant Professor (PurS3 Lab) Jan 2021-Present
Department of Electrical and Computer Engineering
Purdue University, West Lafayette, USA

Postdoctoral Researcher Aug 2020-Dec 2020
University of Pennsylvania, Philadelphia, PA, USA
Advisor: Mayur Naik

Ph.D in Computer Science Sep 2014- Aug 2020
University of California, Santa Barbara, USA
Advisors: Christopher Kruegel and Giovanni Vigna
Thesis: Securing smart devices from the bottom-up
Supported by:
Symantec Research Labs Graduate Fellowship
UCSB Graduate Division Dissertation Fellowship

Publications

[43] N. Kumar K, K. Mohan C, **Aravind Machiry**. "Precision Guided Approach to Mitigate Data Poisoning Attacks in Federated Learning." *Proceedings of the 14th ACM Conference on Data and Application Security and Privacy (**CODASPY**)*, **2024**

[42] S. Sharma, S.R. Tanksalkar, S. Cherupattamoolayil, **Aravind Machiry**. "Fuzzing API Error Handling Behaviors using Coverage Guided Fault Injection." *Proceedings of the ACM ASIA Conference on Computer and Communications Security (**AsiaCCS**)*, **2024**

[41] P. Amusuo, R. Méndez, Z. Xu, **Aravind Machiry**, J. Davis. "Systematically Detecting Packet Validation Vulnerabilities in Embedded Network Stacks." *Proceedings of the 38th ACM International Conference on Automated Software Engineering (**ASE**)*, **2023**

[40] J. Srinivasan, R. Tanksalkar, P. Amusuo, J. Davis, **Aravind Machiry**. "Towards rehosting embedded applications as Linux applications." *53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (**DSN-Disrupt**)*, **2023**

[39] M. Shen, J. Davis, **Aravind Machiry**. "Towards Automated Identification of Layering Violations in Embedded Applications." *Proceedings of the 24th ACM SIGPLAN/SIGBED International Conference on Languages, Compilers, and Tools for Embedded Systems (**LCTES**)*, **2023**

[38] S. Muralee, I. Koishybayev, A. Nahapetyan, G. Tystahl, B. Reaves, A. Bianchi, W. Enck, A. Kapravelos, **Aravind Machiry**. "ARGUS: A Framework for Staged Static Taint Analysis of GitHub Workflows and Actions." *Proceedings of the 31st USENIX Security Symposium (**USENIX Security**)*, **2023**

[37] J. Majors, E. Barsallo Yi, A. Maji, D. Wu, S. Bagchi, **Aravind Machiry**. "Security Properties of Virtual Remotes and SPOOKing their violations." *Proceedings of the ACM ASIA Conference on Computer and Communications Security (**AsiaCCS**)*, **2023**

[36] M. Busch, M. Payer, **Aravind Machiry**, C. Kruegel, G. Vigna, C. Spensky. "TEEzz: Fuzzing Trusted Applications on COTS Android Devices." *Proceedings of the 44nd IEEE Symposium on Security and Privacy (**S&P**)*, **2023**

[35] V. Singhal, A. Pillai, C. Saumya, M. Kulkarni, **Aravind Machiry**. "Cornucopia: A Framework for Feedback Guided Generation of Binaries." *Proceedings of the 37th ACM International Conference on Automated Software Engineering (**ASE**)*, **2022**

[34] I. Koishybayev, A. Nahapetyan, R. Zachariah, S. Muralee, B. Reaves, A. Kapravelos, **Aravind Machiry**. "Characterizing the Security of Github CI Workflows." *Proceedings of the 31st USENIX Security Symposium (**USENIX Security**)*, **2022**

[33] D. Das, P. Bose, **Aravind Machiry**, S. Mariani, Y. Shoshitaishvili, C. Kruegel and G. Vigna. "Hybrid Pruning: Towards A Precise Static Analysis." *Proceedings of the 16th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (**DIMVA**)*, **2022**

[32] P. Pashakhanloo, **Aravind Machiry**, H. Choi, A. Canino, K. Heo, I. Lee, M. Naik. "PacJam: Securing Dependencies Continuously via Package-Oriented Debloating." *Proceedings of the ACM ASIA Conference on Computer and Communications Security (**AsiaCCS**)*, **2022**

[31] **Aravind Machiry**, J. Kastner, M. McCutchen, A. Eline, K. Headley, M. Hicks. "C to Checked C by 3C." *Proceedings of the Object-oriented Programming, Systems, Languages, and Applications (**OOPSLA**)*, **2022**. Won **Distinguished Paper Award**.

[30] D. Quarta, M. Ianni, **Aravind Machiry**, Y. Fratantonio, E. Gustafson, D. Balzarotti, M. Lindorfer, C. Kruegel, and G. Vigna. "Tarnhelm: Isolated, Transparent and Confidential Execution of Arbitrary Code in ARM's TrustZone." *Proceedings of the ACM Workshop on Research on Offensive and Defensive Techniques in the Context of Man At The End Attacks (**CheckMate**)*, **2021**

[29] C. Garg, **Aravind Machiry**, A. Continella, C. Kruegel, and G. Vigna. "Toward a Secure Crowdsourced Location Tracking System." *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (**WiSec**)*, **2021**

[28] Z. Li, **Aravind Machiry**, B. Chen, M. Naik, K. Wang, and L. Song. "ARBITRAR: User-Guided API Misuse Detection." *Proceedings of the 42nd IEEE Symposium on Security and Privacy (**S&P**)*, **2021**

[27] C. Spensky, **Aravind Machiry**, N. Burow, H. Okhravi, R. Housley, Z. Gu, H. Jamjoom, C. Kruegel, and G. Vigna. "Glitching Demystified: Analyzing Control-flow-based Glitching Attacks and Defenses." *Proceedings of the 51st International Conference on Dependable Systems and Networks (**DSN**)*, **2021**

[26] N. Redini, A. Continella, D. Das, G.De Pasquale, N. Spahn, **Aravind Machiry**, A. Bianchi, C. Kruegel, and G. Vigna. "DIANE: Identifying Fuzzing Triggers in Apps to Generate Under-constrained Inputs for IoT Devices." *Proceedings of the 42nd IEEE Symposium on Security and Privacy (**S&P**)*, **2021**

[25] D. Meng, M. Guerriero, **Aravind Machiry**, H. Aghakhani, P. Bose, A. Continella, C. Kruegel and G. Vigna. "Bran: Reduce Vulnerability Search Space in Large Open Source Repositories by Learning Bug Symptoms." *Proceedings of the ACM ASIA Conference on Computer and Communications Security (**AsiaCCS**)*, **2021**

[24] C. Spensky, **Aravind Machiry**, N. Redini, C. Unger, G. Foster, E. Balsband, H. Okhravi, C. Kruegel and G. Vigna. "Conware: Automated Modeling of Hardware Peripherals." *Proceedings of the ACM ASIA Conference on Computer and Communications Security (**AsiaCCS**)*, **2021**

[23] C. Salls, **Aravind Machiry**, A. Doupe, Y. Shoshitaishvili, C. Kruegel, and G. Vigna. "Exploring Abstraction Functions in Fuzzing." *Proceedings of the 2020 IEEE Conference on Communications and Network Security (**CNS**)*, **2020**

[22] C. Spensky, **Aravind Machiry**, M. Busch, K. Leach, R. Housley, C. Kruegel, and G. Vigna. "TRUST.IO: Protecting Physical Interfaces on Cyber-physical Systems." *Proceedings of the 2020 IEEE Conference on Communications and Network Security (**CNS**)*, **2020**

[21] **Aravind Machiry**, N. Redini, E. Cammellini, C. Kruegel and G. Vigna. "SPIDER: Enabling Fast Patch Propagation in Related Software Repositories." *Proceedings of the 41st IEEE Symposium on Security and Privacy*

*(**S&P**)*, **2020**

[20] N. Redini, **Aravind Machiry**, R. Wang, C. Spensky, A. Continella Y. Shoshitaishvili, C. Kruegel and G. Vigna. "KARONTE: Detecting Insecure Multi-binary Interactions in Embedded Firmware." *Proceedings of the 41st IEEE Symposium on Security and Privacy (**S&P**)*, **2020**

[19] **Aravind Machiry**, H. Touma, R. Chen, M. Hicks. "(POSTER) Automated conversion of legacy code to Checked C." *Proceedings of the IEEE Secure Development Conference (**SecDev**)*, **2019**

[18] E. Gustafson, M. Muench, C. Spensky, N. Redini, **Aravind Machiry**, Y. Fratantonio, D. Balzarotti, A. Francillon, Y. E. Choe, C. Kruegel, G. Vigna. "Toward the Analysis of Embedded Firmware through Automated Re-hosting." *Proceedings of the 22nd International Symposium on Research in Attacks, Intrusions and Defenses (**RAID**)*, **2019**

[17] N. Redini, R. Wang, **Aravind Machiry**, Y. Shoshitaishvili, C. Kruegel and G. Vigna. "BinTrimmer: Towards Static Binary Debloating Through Abstract Interpretation." *Proceedings of the 16th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (**DIMVA**)*, **2019**

[16] **Aravind Machiry**, N. Redini, E. Gustafson, H. Aghakhani, C. Kruegel and G. Vigna. "Detecting Deceptive Reviews using Generative Adversarial Networks." *Proceedings of the 2nd Binary Analysis Research Workshop (**BAR**)*, **2019**.

[15] **Aravind Machiry**, N. Redini, E. Gustafson, Y. Fratantonio, Y. E. Choe, C. Kruegel and G. Vigna. "Using Loops For Malware Classification Resilient to Feature-unaware Perturbations." *Proceedings of the 34th Annual Application Security Application Conference (**ACSAC**)*, **2018**

[14] H. Aghakhani, **Aravind Machiry**, S. Nilizadeh, C. Kruegel and G. Vigna. "Detecting Deceptive Reviews using Generative Adversarial Networks." *Proceedings of the 1st Deep Learning and Security Workshop (**DLS**)*, **2018**.

[13] A. Bianchi, Y. Fratantonio, **Aravind Machiry**, C. Kruegel, G. Vigna, S. Chung, W. Lee. "Broken Fingers: On the Usage of the Fingerprint API in Android." *Proceedings of the ISOC Network and Distributed System Security Symposium (**NDSS**)*, **2018**.

[12] A. Bianchi, K. Borgolte, J. Corbetta, F. Disperati, A. Dutcher, J. Grosen, P. Grosen, **Aravind Machiry**, C. Salls, N. Stephens, G. Vigna, R. Wang (Authors listed alphabetically). "Mechanical Phish: Resilient Autonomous Hacking." *IEEE Security & Privacy Magazine - **SPSI: Hacking without Humans 2018***.

[11] N. Redini, **Aravind Machiry**, D. Das, Y. Fratantonio, A. Bianchi, E. Gustafson, Y. Shoshitaishvili, C. Kruegel, G. Vigna. "BootStomp: On the Security of Bootloaders in Mobile Devices." *Chaos Communication Congress (**34C3**)*, **2017**.

[10] J. Corina, **Aravind Machiry**, C. Salls, Y. Shoshitaishvili, Shuang Hao, C. Kruegel, and G. Vigna. "DIFUZZING Android Kernel Drivers." *Black Hat Europe London, UK December (**BH EU**)*, **2017**.

[9] J. Corina, **Aravind Machiry**, C. Salls, Y. Shoshitaishvili, Shuang Hao, C. Kruegel, and G. Vigna. "DIFUZE: Interface Aware Fuzzing for Kernel Drivers." *Proceedings of the 24th ACM Conference on Computer and Communications Security (**CCS**)*, **2017**. Finalist for **CSAW Applied Research Competition**.

[8] **Aravind Machiry**, C. Spensky, J. Corina, N. Stephens, C. Kruegel, G. Vigna. "DR.CHECKER: A Soundy Analysis for Linux Kernel Drivers." *Proceedings of the 26th USENIX Security Symposium (**USENIX Security**)*, **2017**. Runner up for **Facebook Internet Defense Prize**

[7] N. Redini, **Aravind Machiry**, D. Das, Y. Fratantonio, A. Bianchi, E. Gustafson, Y. Shoshitaishvili, C. Kruegel, G. Vigna. "BootStomp: On the Security of Bootloaders in Mobile Devices." *Proceedings of the 26th USENIX Security Symposium (**USENIX Security**)*, **2017**.

[6] **Aravind Machiry**, E. Gustafson, C. Spensky, C. Salls, N. D. Stephens, R. Wang, A. Bianchi, Y. E. Choe, C. Kruegel, G. Vigna. "BOOMERANG: Exploiting the Semantic Gap in Trusted Execution Environments." *Proceedings of the ISOC Network and Distributed System Security Symposium (**NDSS**)*, **2017**.

[5] R. Wang, Y. Shoshitaishvili, A. Bianchi, **Aravind Machiry**, J. Grosen, P. Grosen, C. Kruegel, G. Vigna.

"Ramblr: Making Reassembly Great Again." *Proceedings of the ISOC Network and Distributed System Security Symposium (**NDSS**)*, **2017**. Won **Distinguished Paper Award**.

[4] A. Bianchi, K. Borgolte, J. Corbetta, F. Disperati, A. Dutcher, J. Grosen, P. Grosen, **Aravind Machiry**, C. Salls, N. Stephens, G. Vigna, R. Wang (Authors listed alphabetically). "Cyber Grand Shellphish." ***Phrack***, **2017**.

[3] Y. Fratantonio, **Aravind Machiry**, A. Bianchi, C. Kruegel, G. Vigna. "CLAPP: Characterizing Loops in Android Applications." *Proceedings of the ACM Symposium on Foundations of Software Engineering (**FSE**)*, **2015**.

[2] Y. Fratantonio, **Aravind Machiry**, A. Bianchi, C. Kruegel, G. Vigna. "CLAPP: Characterizing Loops in Android Applications (Invited Talk)." *Proceedings of the International Workshop on Software Development Lifecycle for Mobile (**DeMobile**)*, **2015**.

[1] **Aravind Machiry**, R. Tahiliani, M. Naik. "Dynodroid: An Input Generation System for Android Apps." *Proceedings of the ACM Symposium on Foundations of Software Engineering (**FSE**)*, **2013**. Won **Distinguished Artifact Award**.

Talks

- Unleashing D on Android Kernel Drivers — Nullcon 2018
- Piston: Uncooperative Remote Runtime Patching — ACSAC 2018
- Cyber Grand Shellphish — DEFCON, USA, 2016
- Million Dollar Baby: Towards ANGRly conquering DARPA CGC — Nullcon 2016

Honors & Awards

- **Test of Time Award** for Dynodroid — FSE 2023
- **Amazon Research Award** for Securing CI Workflows — 2023
- **Distinguished Paper Award** for 3c — OOPSLA 2022
- **CS Outstanding Dissertation Award** — UCSB 2020
- **CSAW Applied Research** Finalist for DIFUZE — CSAW 2017
- **Internet Defense Prize** Runner up for DR.CHECKER — USENIX Security 2017
- **Distinguished Paper Award** for Ramblr — NDSS 2017
- **Best Paper Award** for CLAPP — Grad Workshop 2016
- **Distinguished Artifact Award** for Dynodroid — FSE 2013
- **College of Computing MS Research award** — 2013

Professional Activities

Technical Program Committe Member

Conferences (under-approximated):

- **2025:** ISOC NDSS
- **2024:** IEEE S&P, ACM CCS, USENIX Security, USENIX ATC, ACM ACSAC, ISOC NDSS, DIMVA, RAID, USENIX WOOT
- **2023:** ACM CCS, ACSAC, SecDev, AsiaCCS, WOOT, EuroSec, ESORICS
- **2022:** AsiaCCS, Middleware, RAID, WOOT, EuroSec

Organizing Member (Chair)

Workshops:

BAR Workshop (Co-located with NDSS) (2023, 2022)

Teaching

ECE 26400 - Advanced C Programming, Purdue University — Sp'2023
ECE 46900 - Operating Systems Engineering, Purdue University — Sp'2022, Sp'2021
ECE 69500 - Holistic Software Security, Purdue University — Fa'2022, Fa'2021

References

Christopher Kruegel
Professor at University of California, Santa Barbara
chris@cs.ucsb.edu

Giovanni Vigna
Professor at University of California, Santa Barbara
vigna@cs.ucsb.edu

Mayur Naik
Associate Professor at University of Pennsylvania
mhnaik@cis.upenn.edu

Michael Hicks
Professor at University of Maryland, College Park
mwh@cs.umd.edu

Antonio Bianchi
Assistant Professor at Purdue University
antoniob@purdue.edu

Yan Shoshitaishvili
Assistant Professor at Arizona State University
yans@yancomm.net