Nicholas DeMarinis

Computer Science Dept. Box 1910, Brown University, Providence, RI, 02912
401-484-1525 | ndemarin@cs.brown.edu | https://vty.sh | US Citizen | he/him/his

Education

Ph.D. Computer Science, October 2021
Brown University, Dept. of Computer Science, Providence, RI
Advisors: Prof. Vasileios P. Kemerlis and Prof. Rodrigo Fonseca
Dissertation: Improving Application Security at Scale by Reducing System Call and Library Overprivilege

M.Sc. Computer Science, May 2019
Brown University, Providence, RI

M.S. Electrical & Computer Engineering, May 2015
Worcester Polytechnic Institute, Worcester, MA
Advisor: Prof. Alex Wyglinski

B.S. Electrical & Computer Engineering, May 2013
B.S. Computer Science, May 2013
Worcester Polytechnic Institute, Worcester, MA
Minor in Writing and Rhetoric

Academic Positions and Employment

Adjunct Instructor (Summer), Dept. of Electrical & Computer Engineering, WPI, Summer 2016–present

Research Assistant, Dept. of Computer Science, Brown University, Aug 2015–Oct 2021
Advisors: Prof. Vasileios P. Kemerlis, Prof. Rodrigo Fonseca

Teaching Assistant, Dept. of Electrical & Computer Engineering, WPI, Aug 2013–May 2015

Senior Tutor (Undergraduate), Dept. of Electrical & Computer Engineering, WPI, Mar 2012–May 2013

Senior Assistant (Undergraduate), Dept. of Computer Science, WPI, Aug 2012–May 2013

Peer Writing Tutor, Writing Center, WPI, Aug 2010–May 2015

Teaching

(Numbers in parenthesis indicate enrollment in the course.)

ECE2049 Embedded Computing in Engineering Design
Worcester Polytechnic Institute
In-person: Summer 2016 (15), Summer 2017 (14), Summer 2018 (14), Summer 2019 (10)
Online: Summer 2020 (24), Summer 2021 (30)

ECE2029 Introduction to Digital Circuit Design
Worcester Polytechnic Institute
Summer 2014 (3)

Honors & Awards for Teaching

TA of the Year Award, Eta Kappa Nu (WPI Chapter), 2015
Worcester Polytechnic Institute

Honorable Mention (top 3), WPI Teaching Assistant of the Year, 2015
Worcester Polytechnic Institute

Community Service Award for Outstanding Service to the Department, IEEE WPI Chapter, 2014
Worcester Polytechnic Institute

Projects

Secure Systems Lab, Brown University, 2017–present

- **Software Hardening** [1], [2]: Developed tools to automatically identify and reduce over-privilege in commodity (C/C++) applications using novel static binary analyses. `sysfilter`, presented at RAID 2020, addresses over-privilege in the OS system call (syscall) API by restricting the set of system calls available to a program to the set of syscalls identified in its function call graph. In doing so, `sysfilter` enforces the principle of least privilege with respect to the system call API, and reduces the OS kernel attack surface by limiting the set of system calls that can be invoked. Similarly, `libfilter`, published in DTRAP 2020, leverages this same analysis to debloat binary shared libraries, reducing the amount of code available to an attacker and overhead of other software-based defenses. I also conducted a set of large-scale studies of system call usage and code bloat, respectively, across a complete Linux distribution to exemplify these types of over-privilege "in the wild" as well as demonstrate potential security gains.
  `sysfilter`: `https://gitlab.com/brown-ssl/sysfilter`
  `libfilter`: `https://gitlab.com/brown-ssl/libfilter`

- **Robotics Security** [3]: Performed a series of Internet-wide scans for vulnerable research robots that use the Robot Operating System (ROS). I developed a custom framework for safely scanning the entire IPv4 address space for instances of ROS and passively gathering information about the robotic platforms identified by our scans. Our study, presented at ICRA 2019, revealed a number of vulnerable robots and research platforms worldwide that exposed sensitive devices such as cameras and various types of actuators. With permission, we conducted a proof of concept "attack" on one robot identified by our scans, demonstrating our ability to recover real-time sensor data and control the robot's actuators, potentially to unsafe values, to highlight the privacy and security risks. To our knowledge, our study was the first such Internet-wide scan of robotic platforms—since publication, our scan methodology and results have been replicated by other research groups.
  Press: Kapersky. *A glimpse into the present state of security in robotics*. 14 Oct 2019. `https://bit.ly/372mkCF`
  Press: WIRED. *The Serious Security Problem Looming Over Robotics*. 24 Aug 2018. `https://bit.ly/3jKDaLq`

Systems Group, Brown University, 2015–2018

- **IoT Security on Consumer Networks** [4]: Developed a small-scale Internet of Things (IoT) testbed to collect network traffic from a set of consumer IoT devices. We conducted experiments measuring traffic from each device, identifying predictable patterns in DNS traffic and connection behavior in a 48 hour study. Presented in the IoT S&P workshop in 2017, our work demonstrates how small IoT devices have predictable traffic patterns compared to more general-purpose devices, arguing that this can make the enforcement of network traffic policies for these devices more tractable.

- **Stateful SDN Monitoring** [5]: Testing and debugging Software-Defined Networks (SDNs) is notoriously difficult, since the network is defined by a program, which may contain third-party or home-grown software. Our work, presented in HotNets 2016, aims to facilitate network debugging by exploring runtime checking of correctness properties about stateful network behavior. We focus on identifying requirements for checking stateful properties and exploring platforms for extending switches to support monitoring features, driven by our earlier work building stateful monitoring systems.

Publications

[1] Agadakos, I., **DeMarinis, N.**, Jin, D., Williams-King, K., Alfajardo, J., Shteinfeld, B., Williams-King, D., Kemerlis, V. P., and Portokalidis, G. Large-Scale Debloating of Binary Shared Libraries. *Digital Threats: Research and Practice*, 1(4):1–28, 2020

[2] **DeMarinis, N.**, Williams-King, K., Jin, D., Fonseca, R., and Kemerlis, V. P. *sysfilter*: Automated System

Call Filtering for Commodity Software. In *23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID) 2020*, pages 459–474, 2020

[3] **DeMarinis, N.**, Tellex, S., Kemerlis, V. P., Konidaris, G., and Fonseca, R. Scanning the Internet for ROS: A View of Security in Robotics Research. In *2019 International Conference on Robotics and Automation (ICRA)*, pages 8514–8521. IEEE, 2019

[4] **DeMarinis, N.** and Fonseca, R. Toward Usable Network Traffic Policies for IoT Devices in Consumer Networks. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy (IoTS&P)*, pages 43–48, 2017

[5] Nelson, T., **DeMarinis, N.**, Hoff, T. A., Fonseca, R., and Krishnamurthi, S. Switches Are Monitors Too!: Stateful Property Monitoring as a Switch Design Criterion. In *Proceedings of the 15th ACM Workshop on Hot Topics in Networks (HotNets)*, pages 99–105, 2016

Talks and Presentations

Guest Lectures

Networks and Communication Protocols, Nov 2019
CSCI1670: Operating Systems, Brown University
Instructor: Prof. Thomas Doeppner

Security Topics & TLS, Nov 2019
CSCI1680: Computer Networks, Brown University
Instructor: Prof. Rodrigo Fonseca

HTTP and The Web: How Browsers Work, Nov 2018
CSCI1680: Computer Networks, Brown University
Instructor: Prof. Rodrigo Fonseca

IP Routing and Address Translation, Nov 2017
CSCI1680: Computer Networks, Brown University
Instructor: Prof. Rodrigo Fonseca

Introduction to I/O concepts, Sep 2017
CSCI1600: Embedded and Real-Time Software
Instructor: Prof. Steven Reiss

Conference and Workshop Presentations

`sysfilter`: Automated System Call Filtering for Commodity Software [2], Oct 2020
23rd International Symposium on Research in Attacks (RAID), Virtual Event

Toward Usable Network Traffic Policies for IoT Devices in Consumer Networks [4], Nov 2017
IoT Workshop on Security and Privacy (IoT S&P), Dallas, TX, USA

Industry Experience

Co-op Engineer, Advanced Micro Devices (AMD), Boxborough, MA, Summer 2013
Worked closely with Sr. Software Engineer to design, develop and debug functional tests for Mantle low-level graphics API interfacing with AMD hardware. Identified performance enhancements for internal testing framework to help improve development team's regression testing process.

Engineering Intern, Hayward Industries, North Kingstown, RI, Summer 2012
Collaborated with Sr. Electrical Engineer and off-site QA engineers to perform rapid testing and debugging of software fixes for a variable-speed aquatic pump. Maintained a Jenkins CI server to facilitate the software team's development process, working closely with Project Manager to identify a useful configuration.

PGP Public Key Fingerprint

`nd@vty.sh` `B340:8889:7223:759A:EE19:91EC:2366:2E54:170B:1316`