Sanjeev Kumar Das

Research Scientist

GitHub LinkedIn Website Google_Scholar

das.sanjeevk001@gmail.com, 1(919)-869-0354

Work Experience

IBM Research, T.J. Watson Research Center, Yorktown Heights, NY USA
Research Scientist, Security Research **April 2020 - Present**

- Leading a project on developing a scalable fuzzing framework towards finding vulnerabilities.
- Development of malware analysis framework using static analysis.

Department of Computer Science, University of North Carolina at Chapel Hill, USA
Postdoctoral Research Associate **Feb. 2017 - Mar. 2020**

- I led the project on building a novel coverage-guided fuzzing framework, using hardware performance counters and machine learning.
- Developed a fuzzing approach that learns from past vulnerabilities and finds new vulnerabilities faster ($> 3\mathbf{x}$) than the existing approaches, and moreover, finds more unique bugs.
- Reported a number of new vulnerabilities in popular open source programs, leading to 3 CVE assignments.
- In the recent past, I led the project on the systematic assessment of the usage of hardware performance counters for security applications, including defense against Return Oriented Programming (ROP) attacks, side-channel attacks, and malware detection.
- Developed an adversarial model to demonstrate how performance counters can be manipulated to bypass certain security defenses.

Research Scholar, **Cybersecurity Lab**, NTU, Singapore **Aug. 2012 - Dec. 2016**

- Developed a practical system-level defense against Return Oriented Programming (ROP) attacks at runtime using hardware performance counters.
- Developed a system-level defense to detect malware at runtime using machine learning algorithm by leveraging the system call patterns of malicious samples.
- Designed a control flow integrity approach to enforce integrity at the basic block level to defend against runtime memory attacks (e.g., code reuse attacks) for embedded systems.

System Engineer, **IBM**, Bangalore, India **May 2010 - July 2012**

- As an application developer at IBM, I worked with the development team to build Java based web applications.

Education

Ph.D., Computer Engineering, Nanyang Technological University, Singapore, 2017
Field: Computer Security
Thesis: *Hardware-Assisted Online Defense Against Malware and Exploits*
B.Tech., Electronics Engineering, National Institute of Technology, Surat, India, 2010

Technical Skills

- Programming: C, C++, Python, Bash, Java, ASM (x86/IA64)
- Proficiency in fuzzing on open, closed source programs
- Experience with crash triage and root cause analysis
- Experience with exploit development, API hooking, DLL injection
- Device driver development on Windows, Linux
- Static Analysis (e.g., IDA, Ghidra), Dynamic Analysis (e.g., PIN, DynamoRIO)
- Debugger: x64, WinDbg, Immunity, GDB, Mozilla rr, Valgrind, Sanitizers
- Experience with application security tools: Metasploit framework, Wireshark, Kali Linux

CVEs

- CVE-2020-13790: Heap-based buffer over-read in libjpeg-turbo 2.0.4 and mozjpeg 4.0.0.
- CVE-2020-21674: Out-of-bounds write in Libarchive-3.4.1dev.
- CVE-2019-19221: Out-of-bounds read in Libarchive 3.4.0.
- CVE-2019-14615: Information leakage in Intel Integrated GPU.

Selected Publications

- A Flexible Framework for Expediting Bug Finding by Leveraging Past (Mis-)Behavior to Discover New Bugs. In *Proc. of Annual Computer Security Applications Conf. (ACSAC)*, 2020.
- iGPU Leak: An Information Leakage Vulnerability on Intel Integrated GPU. In *Proceedings of Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2020.

- SoK: The Challenges, Pitfalls, and Perils of Using Hardware Performance Counters for Security. In *Proceedings of IEEE Symposium on Security & Privacy (S&P)*, 2019.
- BBB-CFI: Lightweight CFI Approach Against Code-Reuse Attacks Using Basic Block Information. *ACM Transactions on Embedded Computing Systems (TECS)*, 2020.
- ROPSentry: Runtime Defense against ROP Attacks using Hardware Performance Counters. *Computers & Security*, 2018.
- Sgxlinger: A new side-channel attack vector based on interrupt latency against enclave execution. In *Proceedings of International Conference on Computer Design (ICCD)*, 2018.
- No-Jump-into-Basic-Block: Enforce Basic Block CFI on the Fly for Real-world Binaries. In *Proceedings of Design Automation Conference (DAC)* (**Best paper nomination**), 2017.
- Semantics-based Online Malware Detection: Towards Efficient Real-time Protection Against Malware. *IEEE Trans. on Information Forensics and Security (TIFS)*, 2016.
- A Fine-Grained Control Flow Integrity Approach Against Runtime Memory Attacks for Embedded Systems. *IEEE Trans. on Very Large Scale Integration Systems (TVLSI)*, 2016.
- Online Malware Defense Using Attack Behavior Model. In *Proceedings of Int'l Symposium on Circuits & Systems (ISCAS)*, 2016.
- Reconfigurable dynamic trusted platform module for control flow checking. In *Proceedings of IEEE Computer Society Annual Symposium on VLSI*, 2014.