Sanjeev Kumar Das

Research Scientist

GitHub LinkedIn Website Google_Scholar

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

Research Interests

Software and System Security, Vulnerability Research, Exploit Development and Mitigation, Malware Analysis, Program Analysis, Reverse Engineering

Work Experience

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

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

Cybersecurity Lab, NTU, Singapore
Research Assistant — **Aug. 2016 - Jan. 2017**

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

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

Education

Nanyang Technological University (NTU), Singapore
Ph.D., Computer Engineering — **Fall 2012 - 2016**

- Thesis: *Hardware-Assisted Online Defense Against Malware and Exploits*
- *Advisors:* Professor Yang Liu and Professor Wei Zhang
- GPA: 4.25/5

National Institute of Technology, Surat, India
B.Tech., Electronics Engineering — **Fall 2006 - 2010**

- GPA: 8.64/10

Security Advisories

- CVE-2020-28203: Improper validation of array index in Foxit Reader/PhantomPDF v10.1.0.37527.
- 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

Peer Reviewed Conferences & Journals

- **A Flexible Framework for Expediting Bug Finding by Leveraging Past (Mis-)Behavior to Discover New Bugs.**
  Sanjeev Das, Kedrian James, Jan Werner, Manos Antonakakis, Michalis Polychronakis, and Fabian Monrose. In *Proceedings of Annual Computer Security Applications Conference (ACSAC)*, 2020.
- **iGPU Leak: An Information Leakage Vulnerability on Intel Integrated GPU.**
  HE Wenjian, Wei Zhang, Sharad Sinha, and **Sanjeev Das**. In *Proceedings of Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2020.
- **BBB-CFI: Lightweight CFI Approach Against Code-Reuse Attacks Using Basic Block Information.**
  Wenjian He, **Sanjeev Das**, Wei Zhang, and Yang Liu. In *ACM Transactions on Embedded Computing Systems (TECS)*, 2020.
- **SoK: The Challenges, Pitfalls, and Perils of Using Hardware Performance Counters for Security**
  Sanjeev Das, Jan Werner, Manos Antonakakis, Michalis Polychronakis, and Fabian Monrose. In *Proceedings of the 40th IEEE Symposium on Security & Privacy (S&P). May 2019, San Francisco, CA.*
- **SGXlinger: A New Side-channel Attack Vector Based on Interrupt Latency against Enclave Execution**
  Wenjian He, Wei Zhang, **Sanjeev Das** and Yang Liu. In *36th IEEE International Conference on Computer Design (ICCD), 2018.*

- **ROPSentry: Runtime Defense against ROP Attacks using Hardware Performance Counters.**
  Sanjeev Das, Chen Bihuan, Mahintham Chandramohan, Yang Liu, and Wei Zhang. *Computers & Security 73, 374-388 (2018).*
- **No-Jump-into-Basic-Block: Enforce Basic Block CFI on the Fly for Real-world Binaries.**
  Wenjian He, **Sanjeev Das**, Wei Zhang, Yang Liu. In *Proceedings of Design Automation Conference* (**DAC**) (**Best paper nomination**), *2017.*
- **Semantics-based Online Malware Detection: Towards Efficient Real-time Protection Against Malware.**
  Sanjeev Das, Yang Liu, Wei Zhang and Mahintham Chandramohan. *IEEE Transactions on Information Forensics and Security* (**TIFS**) *11.2 (2016): 289-302.*
- **A Fine-Grained Control Flow Integrity Approach Against Runtime Memory Attacks for Embedded Systems.**
  Sanjeev Das, Wei Zhang, and Yang Liu. *IEEE Transactions on Very Large Scale Integration Systems* (**TVLSI**), *24.11 (2016): 3193-3207.*
- **Online Malware Defense Using Attack Behavior Model.**
  Sanjeev Das, Hao Xiao, Yang Liu, Wei Zhang. In *Proceedings of IEEE International Symposium on Circuits & Systems* (**ISCAS**), *2016.*
- **Reconfigurable Dynamic Trusted Platform Module for Control Flow Checking.**
  Sanjeev Das, Wei Zhang, Yang Liu. In *Proceedings of IEEE Computer Society Annual Symposium on VLSI* (**ISVLSI**), *2014.*

Technology Disclosure

- **Semantics-Based Online Malware Detection: Towards Efficient Real-Time Protection Against Malware.**
  Yang Liu, Thambipillai Srikanthan, **Sanjeev Das**. *Technology Disclosure for Nanyang Technological University* (**TD/098/16**), *2016.*
- **Malware Defense Using Attack Behavior Model.**
  Yang Liu, Thambipillai Srikanthan, **Sanjeev Das**. *Technology Disclosure for Nanyang Technological University* (**TD/099/16**), *2016.*
- **Runtime Security Protection Using Hardware Specific Features.**
  Yang Liu, Thambipillai Srikanthan, **Sanjeev Das**. *Technology Disclosure for Nanyang Technological University* (**TD/100/16**), *2016.*

Professional Services

Program Committee Member:

- The 22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID), Beijing, China, September 23-25, 2019.

Journal Reviewer:

- ACM Computing Survey
- Computer & security
- International Journal of Information Security
- IET Information Security
- IEEE Access
- IET Computers & Digital Techniques

Conference Talks

A Flexible Framework for Expediting Bug Finding by Leveraging Past (Mis-)Behavior to Discover New Bugs.
In *Proceedings of Annual Computer Security Applications Conference (ACSAC)*, Dec. 2020.
SoK: The Challenges, Pitfalls, and Perils of Using Hardware Performance Counters for Security.
In *IEEE Symposium on Security & Privacy (S&P), May 2019, San Francisco, CA.*
Online Malware Defense Using Attack Behavior Model.
In *IEEE Int'l Symposium on Circuits & Systems (ISCAS), Montreal, Canada, May 2016.*

Awards & Fellowship

Singapore International Graduate Award (SINGA) **Aug. 2012 - July 2016**

- Full scholarship to pursue PhD study at Nanyang Technological University.

Nepal Aid Fund Scholarship **2006 - 2010**

- Selected in top 70 students (out of 10,000) to pursue undergraduate study by Ministry of External Affairs, India, with a full scholarship.

IBM

- **Roll of Honor** for the excellence in design and coding of the application.
- **GEM (Great Ericsson Minds)** award by the joint collaboration of IBM and the client Ericsson.

Academic Experience

School of Computer Science and Engineering, NTU, Singapore

Teaching Assistant **Jan. 2015 - April 2015**

- CZ2005: Operating Systems

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