

Sanjeev Kumar Das

Department of Computer Science

University of North Carolina at Chapel Hill

201 South Columbia St, Sitterson Hall, Chapel Hill, NC 27599

Phone: 1(919) 869-0354

Email: sdas@cs.unc.edu

[Website](#) [Google Scholar](#) [Linkedin](#)

RESEARCH INTERESTS Software and System Security, Vulnerability Discovery, Exploit Development and Mitigation, Malware Analysis, Program Analysis, Reverse Engineering

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

- Project: *Microcontroller based Remote Weather/Pollution Monitoring System*
- GPA: 8.64/10

PUBLICATIONS **Peer Reviewed Conferences & Journals**

- **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). *Impact Factor* 2.849
- **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. *Impact Factor* 5.824.
- **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. *Impact Factor* 1.744.
- **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.

	<ul style="list-style-type: none"> • Reconfigurable Dynamic Trusted Platform Module for Control Flow Checking. Sanjeev Das, Wei Zhang, Yang Liu. In <i>Proceedings of IEEE Computer Society Annual Symposium on VLSI (ISVLSI)</i>, 2014. • FPGA Based Control Flow Checking. Sanjeev Das, Wei Zhang, Yang Liu. In <i>Proceedings of Design Automation Conference (DAC)</i>, 2014 (poster).
TECHNOLOGY DISCLOSURE	<ul style="list-style-type: none"> • Semantics-Based Online Malware Detection: Towards Efficient Real-Time Protection Against Malware. Yang Liu, Thambipillai Srikanthan, Sanjeev Das. <i>Technology Disclosure for Nanyang Technological University (TD/098/16)</i>, 2016. • Malware Defense Using Attack Behavior Model. Yang Liu, Thambipillai Srikanthan, Sanjeev Das. <i>Technology Disclosure for Nanyang Technological University (TD/099/16)</i>, 2016. • Runtime Security Protection Using Hardware Specific Features. Yang Liu, Thambipillai Srikanthan, Sanjeev Das. <i>Technology Disclosure for Nanyang Technological University (TD/100/16)</i>, 2016.
PROFESSIONAL SERVICES	<p>Program Committee Member:</p> <ul style="list-style-type: none"> • The 22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID), Beijing, China, September 23-25, 2019. <p>Journal Reviewer:</p> <ul style="list-style-type: none"> • ACM Computing Survey • Computer & security • International Journal of Information Security • IET Information Security • IEEE Access • IET Computers & Digital Techniques
CONFERENCE TALKS	<p>SoK: The Challenges, Pitfalls, and Perils of Using Hardware Performance Counters for Security. In <i>IEEE Symposium on Security & Privacy (S&P)</i>. May 2019, San Francisco, CA.</p> <p>Online Malware Defense Using Attack Behavior Model. In <i>IEEE Int'l Symposium on Circuits & Systems (ISCAS)</i>, Montreal, Canada, May 2016.</p>
AWARDS & FELLOWSHIP	<p>Singapore International Graduate Award (SINGA) Aug. 2012 - July 2016</p> <ul style="list-style-type: none"> • Full scholarship to pursue PhD study at Nanyang Technological University. <p>Nepal Aid Fund Scholarship 2006 - 2010</p> <ul style="list-style-type: none"> • Selected in top 70 students (out of 10,000) to pursue undergraduate study by Ministry of External Affairs, India, with a full scholarship. <p>IBM</p> <ul style="list-style-type: none"> • 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	<p>School of Computer Science and Engineering, NTU, Singapore</p> <p><i>Teaching Assistant</i> Jan. 2015 - April 2015</p> <ul style="list-style-type: none"> • CZ2005: Operating Systems
TECHNICAL SKILLS	<ul style="list-style-type: none"> • Languages: ASM (x86), C, C++, Python, Bash, L^AT_EX, Java • Architectures: x86, x86-64 • Experience with Fuzzing • Experience with crash dump analysis and exploit development • Device driver development on Windows/Linux

- API hooking, DLL injection
- Debugger: WinDbg, Immunity Debugger, GDB, Valgrind
- Operating Systems: Linux, Windows, Mac OS, Kali
- Virtualization tools: VMware, Virtualbox
- Web Platform: J2EE (JSP & Servlet), WebSphere Portal, HTML, jQuery, XML
- IDE: Eclipse, Visual Studio
- Security tools: Metasploit, IDA, Wireshark