

# Dipanjan Das

Security Researcher  
SecLab, UCSB

724 Kroeber Walk, Apt. 101  
Goleta, California 93117  
USA  
☎ +1 (805) 728 0706  
✉ [dipanjan@cs.ucsb.edu](mailto:dipanjan@cs.ucsb.edu)  
📄 [www.dipanjan.in](http://www.dipanjan.in)  
@sherlock

## Research Interests

My research is directed towards developing novel analysis techniques to uncover vulnerabilities in low-level system software, e.g. operating system kernels and boot-loaders. To work on various exploit mitigation techniques for such targets to improve their practicality is in my future research plan.

## Education

- 2016–Present **Ph.D.**, *University of California, Santa Barbara*, GPA – 4.0/4.0.  
Computer Security, advised by Prof. Giovanni Vigna & Prof. Christopher Kruegel
- 2013–2015 **M.Tech.**, *Indian Institute of Technology, Madras*, GPA – 8.81/10.0.  
Computer Science & Engineering, advised by Prof. PanduRangan Chandrasekaran
- 2006–2010 **B.Tech.**, *Institute of Engineering & Management, Kolkata*, GPA – 8.92/10.0.  
Computer Science & Engineering

## Professional Experience

- 2010–2012 **Assistant Systems Engineer**, *Tata Consultancy Services (TCS)*, Kolkata, India.
- 2012–2013 **Scientist Engineer - SC, Gazetted Officer, Class 'A'**, *Indian Space Research Organization (ISRO), Vikram Sarabhai Research Centre (VSSC)*, Trivandrum, India.  
○ To develop SPARCSIM, an instruction set simulator for a customized SPARC v8 based processor to be used on-board of next generation launch vehicles.
- 2013–2015 **Teaching Assistant**, *Indian Institute of Technology (IIT), Madras*, India.
- 2015–2015 **Software Developer**, *BrowserStack*, Mumbai, India.
- 2015–2016 **Post-Graduate Research Intern**, *National University of Singapore*, Singapore.  
○ Automatic patching of closed-source programs
- 2017–2017 **Interim Engineering Intern**, *Qualcomm Technologies, Inc*, San Diego.  
○ Developing a memory safe API in Rust to be used by *Qualcomm* drivers  
○ Developing an off-device fuzzing platform for a WLAN driver
- 2020–2020 **Research Intern**, *University of Minnesota (Prof. Kangjie Lu)*, Minneapolis.  
○ Kernel fuzzing technique to trigger order-inconsistency bugs

## Publications

- [9] P. Bose, **D. Das**, Y. Chen, Y. Feng, C. Kruegel, and G. Vigna, “Sailfish: Vetting Smart Contract State-Inconsistency Bugs in Seconds,” in *Proceedings of the IEEE Symposium on Security and Privacy (IEEE S&P)*, 2022.
- [8] **D. Das**, P. Bose, A. Machiry, S. Mariani, Y. Shoshitaishvili, C. Kruegel, and G. Vigna, “Hybrid Pruning: Towards Precise Pointer and Taint Analysis,” in *Proceedings of the Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA)*, 2022.
- [7] **D. Das**, P. Bose, N. Ruaro, C. Kruegel, and G. Vigna, “Understanding Security Issues in the NFT Ecosystem,” in *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2022.

- [6] N. Redini, A. Continella, **D. Das**, G. D. Pasquale, A. Machiry, A. Bianchi, C. Kruegel, and G. Vigna, "Diane: Identifying Fuzzing Triggers in Apps to Generate Under-constrained Inputs for IoT Devices," in *Proceedings of the IEEE Symposium on Security and Privacy (IEEE S&P)*, 2021.
- [5] D. Song, F. Hetzelt, **D. Das**, C. Spensky, Y. Na, S. Volckaert, G. Vigna, C. Kruegel, J. P. Seifert, and M. Franz, "PeriScope: An Effective Probing and Fuzzing Framework for the Hardware-OS Boundary," in *Proceedings of the BlackHat USA*, 2019.
- [4] D. Song, F. Hetzelt, **D. Das**, C. Spensky, Y. Na, S. Volckaert, G. Vigna, C. Kruegel, J. P. Seifert, and M. Franz, "PeriScope: An Effective Probing and Fuzzing Framework for the Hardware-OS Boundary," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, This work was presented in Qualcomm Product Security Summit (QPSS), San Diego, CA, May 2019. **Was among the top 10 finalists in Applied Research Competition, CSAW, November 2019**, 2019.
- [3] N. Redini, A. Machiry, **D. Das**, Y. Fratantonio, A. Bianchi, E. Gustafson, Y. Shoshitaishvili, G. Vigna, and C. Kruegel, "BootStomp: On the Security of Bootloaders in Mobile Devices," in *Proceedings of the Chaos Communication Congress (CCC)*, 2017.
- [2] N. Redini, A. Machiry, **D. Das**, Y. Fratantonio, A. Bianchi, E. Gustafson, Y. Shoshitaishvili, G. Vigna, and C. Kruegel, "BootStomp: On the Security of Bootloaders in Mobile Devices," in *Proceedings of the USENIX Security Symposium (Usenix)*, 2017.
- [1] P. Bose, **D. Das**, and C. P. Rangan, "Constant Size Ring Signature Without Random Oracle," in *Proceedings of the Australasian Conference on Information Security and Privacy (ACISP)*, 2015.

---

## Professional Activities

- Reported five high-impact security vulnerabilities with financial consequences in OpenSea, Sorare, and Rarible NFT marketplaces (2021).
- Reported vulnerabilities CVE-2018-14745, CVE-2018-14852, CVE-2018-14853, CVE-2018-14854, CVE-2018-14855, CVE-2018-14856 to Samsung and CVE-2018-11947, CVE-2018-11902 to Qualcomm.
- Appears in [CodeAurora Hall-of-Fame](#) (2018) and [Samsung Android Security Updates](#) (August 2018).
- Invited to [Qualcomm Vulnerability Rewards Program](#) at [HackerOne](#) (September 2018).
- Member of [Shellphish](#) Capture-The-Flag (CTF) team. Participated in DEFCON CTF Finals in the year 2017, 2018 and 2019.
- Member of the organizing team of UCSB iCTF security competition in the year 2017 and 2018.

---

## Scholastic Achievements

- Stood 29<sup>th</sup> in X<sup>th</sup> standard and 16<sup>th</sup> in XII<sup>th</sup> state board examinations.
- Awarded by *Viren J. Shah*, ex-governor of West Bengal, for 10<sup>th</sup> rank in Kolkata zone in X<sup>th</sup> standard board examination.
- Received *National Merit Scholarship* twice from *Ministry of Human Resource and Development* (MHRD), Government of India for securing 29<sup>th</sup> position in X<sup>th</sup> standard and 16<sup>th</sup> position in XII<sup>th</sup> state board examinations.
- Secured all India rank 11 and 20 among 12,227 and 10,737 candidates in Indian Space Research Organization (ISRO) entrance examination 2011 and 2014 respectively.
- Secured all India rank 106 among 2,24,160 candidates in GATE 2013.
- Received *Presidential Graduate Fellowship* at *National University of Singapore* (NUS).

---

## Academic Services

Program Committee	Usenix Security Symposium (Usenix) Artifact Evaluation	2022
	Workshop on Binary Analysis Research (NDSS BAR)	2022

	Workshop on Decentralized Finance and Security (ACM CCS DeFi)	2022
	Conference on Emerging Security Information, Systems and Technologies (Securware)	2022
	Blockchain and Cryptocurrency Congress (B2C)	2022
Journal Reviewer	ACM Computing Surveys (CSUR)	2021
External Reviewer	The Network and Distributed System Security Symposium (NDSS)	2022
	Usenix Security Symposium (Usenix)	2022
Shadow PC	IEEE Symposium on Security and Privacy (IEEE S&P)	2021
	ACM SIGOPS in Europe (EuroSys)	2021

## Media Coverage

NFT Study [7]	<p><b>Axetue</b>, <a href="#">OpenSea hack verified 3 security concerns. Here's what you need to know</a>, (Feb 2022).</p> <p><b>Hong Kong Security Response Team Coordinate Centre (HKCERT)</b>, <a href="#">What You Know about the Cyber Security of NFT</a>, (Mar 2022).</p> <p><b>Medium</b>, <a href="#">NFT Security 101</a>, (Mar 2022).</p> <p><b>Sensors Tech Forum</b>, <a href="#">NFT Security and Risks: How Secure Are Your Digital Assets?</a>, (Feb 2022).</p> <p><b>Merehead</b>, <a href="#">How to make NFTs secure?</a>, (Dec 2021).</p> <p><b>CoinYuppie</b>, <a href="#">Do you know how to audit safe and reliable NFT projects?</a>, (Feb 2022).</p> <p><b>DevNews Podcast</b>, <a href="#">Elon Musk's Twitter Takeover, Security Vulnerabilities in Web3, and Experimenting With the TikTok Algorithm</a>, (Apr 2022).</p> <p><b>The Atlantic</b>, <a href="#">Please Ignore My Last 577 Tweets</a>, (May 2022).</p> <p><b>TruthDAO Podcast</b>, <a href="#">NFT Academic Roundtable</a>, (May 2022).</p> <p><b>TruthDAO</b>, <a href="#">Fraudulent "Wash Sales" Roil Booming NFT Market</a>, (May 2022).</p> <p><b>TruthDAO</b>, <a href="#">Fake Trading, Stablecoin Troubles, and the Threat of Crypto Regulation: Our Crypto DeFined NFT Roundtable Takeaways</a>, (May 2022).</p>
Sailfish [9]	<p><b>TheHackerNews</b>, <a href="#">SAILFISH System to Find State-Inconsistency Bugs in Smart Contracts</a>, (Jan 2022).</p> <p><b>IEMLabs</b>, <a href="#">SAILFISH System to Find State-Inconsistency Bugs in Smart Contracts</a>, (Jan 2022).</p> <p><b>CyberFishNews</b>, <a href="#">SAILFISH System to Find State-Inconsistency Bugs in Smart Contracts</a>, (Jan 2022).</p> <p><b>CyberSecurity.News</b>, <a href="#">SAILFISH System to Find State-Inconsistency Bugs in Smart Contracts</a>, (Jan 2022).</p>
BootStomp [2]	<p><b>ZDNet</b>, <a href="#">Android security: Multiple bootloader bugs found in major chipset vendors' code</a>, (Sep 2017).</p> <p><b>The Register</b>, <a href="#">Boffins hijack bootloaders for fun and games on Android</a>, (Sep 2017).</p> <p><b>The Hacker News</b>, <a href="#">Mobile Bootloaders From Top Manufacturers Found Vulnerable to Persistent Threats</a>, (Sep 2017).</p> <p><b>NowSecure</b>, <a href="#">Android bootloader security and BootStomp: A Primer</a>, (Sep 2017).</p> <p><b>Washington Center for CyberSecurity</b>, <a href="#">BootStomp: Useful Tool in Researching Bootloaders</a>, (Sep 2017).</p> <p><b>PenTestIT</b>, <a href="#">BootStomp: Find Mobile Device Bootloader Vulnerabilities</a>, (Aug 2017).</p> <p><b>ProgrammerSought</b>, <a href="#">BootStomp: About the bootloader security of mobile devices - 6 BootStomp</a>, (Sep 2017).</p> <p><b>SecurityWeek</b>, <a href="#">Multiple Vulnerabilities Found in Mobile Bootloaders</a>, (Sep 2017).</p> <p><b>Pentest Tools</b>, <a href="#">BootStomp - A Bootloader Vulnerability Finder</a>, (Dec 2017).</p> <p><b>NowSecure</b>, <a href="#">Android bootloader security and BootStomp: A Primer</a>, (Sep 2017).</p> <p><b>HebergementWebs</b>, <a href="#">Experts discovered zero day flaws in Android bootloaders</a>, (Sep 2017).</p>

**Security Affairs**, <https://securityaffairs.co/wordpress/62762/mobile-2/bootstomp-bootloaders-flaws.html>, (Sep 2017).

**Hackers Online Club**, *BootStomp: An Android boot-loader Bug Finder*, (Sep 2017).

**Quantus**, *BootStomp – Find Android Bootloader Vulnerabilities*, (Feb 2018).