# 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](http://@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.* <br> Computer Security, advised by Prof. Giovanni Vigna & Prof. Christopher Kruegel |
| 2013–2015 | **M.Tech.**, *Indian Institute of Technology*, Madras, *GPA – 8.81/10.0.* <br> Computer Science & Engineering, advised by Prof. PanduRangan Chandrasekaran |
| 2006–2010 | **B.Tech.**, *Institute of Engineering & Management*, Kolkata, *GPA – 8.92/10.0.* <br> 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. <br> ○ 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. <br> ○ Automatic patching of closed-source programs |
| 2017–2017 | **Interim Engineering Intern**, *Qualcomm Technologies, Inc*, San Diego. <br> ○ Developing a memory safe API in Rust to be used by *Qualcomm* drivers <br> ○ Developing an off-device fuzzing platform for a WLAN driver |
| 2020–2020 | **Research Intern**, *Univesrsity of Minnesota (Prof. Kangjie Lu)*, Minneapolis. <br> ○ Kernel fuzzing technique to trigger order-inconsistency bugs |

## Publications

[8] P. Bose, **D. Das**, Y. Chen, Y. Feng, C. Kruegel, and G. Vigna, "Sailfish: Vetting smart contract state-inconsistency bugs in seconds," in *IEEE Symposium on Security and Privacy (IEEE S&P)*, 2022.

[7] **D. Das**, P. Bose, N. Ruaro, C. Kruegel, and G. Vigna, "Understanding security issues in the nft ecosystem," in *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 *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 *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 *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 *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 *USENIX Security Symposium (Usenix)*, 2017.

[1]  P. Bose, **D. Das**, and C. P. Rangan, "Constant size ring signature without random oracle," in *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 $29^{th}$ in $X^{th}$ standard and $16^{th}$ in $XII^{th}$ state board examinations.

○ Awarded by *Viren J. Shah*, ex-governor of West Bengal, for $10^{th}$ rank in Kolkata zone in $X^{th}$ standard board examination.

○ Received *National Merit Scholarship* twice from *Ministry of Human Resource and Development* (MHRD), Government of India for securing $29^{th}$ position in $X^{th}$ standard and $16^{th}$ position in $XII^{th}$ 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

| | | |
|---|---|---|
| Shadow PC | IEEE Symposium on Security and Privacy (IEEE S&P) | *2021* |
| | ACM SIGOPS in Europe (EuroSys) | *2021* |
| Program Committee | Usenix Security Symposium (Usenix) Artifact Evaluation | *2022* |
| | Workshop on Binary Analysis Research (BAR) | *2022* |
| External Reviewer | The Network and Distributed System Security Symposium (NDSS) | *2022* |

| | | |
|---|---|---|
| | Usenix Security Symposium (Usenix) | *2022* |
| Journal Reviewer | ACM Computing Surveys (CSUR) | *2021* |

## Media Coverage

NFT Study [7] **Axetue**, *OpenSea hack verified 3 security concerns. Here's what you need to know*, (Feb 2022).

**Hong Kong Security Response Team Coordinate Centre (HKCERT)**, *What You Know about the Cyber Security of NFT*, (Mar 2022).

**Medium**, *NFT Security 101*, (Mar 2022).

**Sensors Tech Forum**, *NFT Security and Risks: How Secure Are Your Digital Assets?*, (Feb 2022).

**Merehead**, *How to make NFTs secure?*, (Dec 2021).

**CoinYuppie**, *Do you know how to audit safe and reliable NFT projects?*, (Feb 2022).

Sailfish [8] **TheHackerNews**, *SAILFISH System to Find State-Inconsistency Bugs in Smart Contracts*, (Jan 2022).

**IEMLabs**, *SAILFISH System to Find State-Inconsistency Bugs in Smart Contracts*, (Jan 2022).

**CyberFishNews**, *SAILFISH System to Find State-Inconsistency Bugs in Smart Contracts*, (Jan 2022).

**CyberSecurity.News**, *SAILFISH System to Find State-Inconsistency Bugs in Smart Contracts*, (Jan 2022).

BootStomp [2] **ZDNet**, *Android security: Multiple bootloader bugs found in major chipset vendors' code*, (Sep 2017).

**The Register**, *Boffins hijack bootloaders for fun and games on Android*, (Sep 2017).

**The Hacker News**, *Mobile Bootloaders From Top Manufacturers Found Vulnerable to Persistent Threats*, (Sep 2017).

**NowSecure**, *Android bootloader security and BootStomp: A Primer*, (Sep 2017).

**Washington Center for CyberSecurity**, *BootStomp: Useful Tool in Researching Bootloaders*, (Sep 2017).

**PenTestIT**, *BootStomp: Find Mobile Device Bootloader Vulnerabilities*, (Aug 2017).

**ProgrammerSought**, *BootStomp: About the bootloader security of mobile devices - 6 BootStomp*, (Sep 2017).

**SecurityWeek**, *Multiple Vulnerabilities Found in Mobile Bootloaders*, (Sep 2017).

**Pentest Tools**, *BootStomp - A Bootloader Vulnerability Finder*, (Dec 2017).

**NowSecure**, *Android bootloader security and BootStomp: A Primer*, (Sep 2017).

**HebergementWebs**, *Experts discovered zero day flaws in Android bootloaders*, (Sep 2017).

**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).