# Dipanjan Das

*Security Researcher*
*SecLab, UCSB*

✉ *dipanjan@cs.ucsb.edu*
*dipanjan.in*
*sherl0ck*
*sher10ckk*
*dipanjan*

## Research Interests

My research extends in two distinct directions. I develop automated program analysis techniques to uncover vulnerabilities in low-level systems, such as, operating system kernel, bootloader, and Internet of Things (IoT) devices. In addition, I took a deep dive in the areas related to vulnerability analysis of smart contracts, and various aspects of cryptoeconomics, specifically the design flaws, and the market manipulation strategies employed in the decentralized finance (DeFi) ecosystem.

## 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

2020–2020 **Research Intern**, *University of Minnesota (Prof. Kangjie Lu)*, Minneapolis.

2017–2017 **Interim Engineering Intern**, *Qualcomm Technologies, Inc*, San Diego.

2015–2016 **Post-Graduate Research Intern**, *National University of Singapore*, Singapore.

2015–2015 **Software Developer**, *BrowserStack*, Mumbai, India.

2013–2015 **Teaching Assistant**, *Indian Institute of Technology (IIT)*, Madras, India.

2012–2013 **Scientist Engineer - SC, Gazetted Officer, Class 'A'**, *Indian Space Research Organization (ISRO), Vikram Sarabhai Research Centre (VSSC)*, Trivandrum, India.

2010–2012 **Assistant Systems Engineer**, *Tata Consultancy Services (TCS)*, Kolkata, India.

## Publications

[11] P. Bose, **D. Das**, S. Vasan, I. Grishchenko, A. Continella, A. Bianchi, C. Kruegel, and G. Vigna, "Columbus: Android App Testing Through Systematic Callback Exploration," in *Proceedings of the International Conference on Software Engineering (ICSE)*, 2023.

[10] **D. Das**, M. Fleischer, P. Bose, W. Bai, C. Kruegel, G. Vigna, and K. Lu, "Actor: Action-aware Kernel Fuzzing," in *Under submission*, 2023.

[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.

## Books

[1] **D. Das** and P. Bose, *An Identity Based Encryption Scheme Resilient to RAM Scraper Like Malware Attacks: Glassbox Secure IBE*. Eliva Press, 2022, ISBN-13: 978-9994980918, ISBN-10: 9994980912.

## 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, and organized UCSB iCTF security competition in the year 2017 and 2018.

## Scholastic Achievements

- Stood $29^{th}$ in $\mathrm{X}^{\mathrm{th}}$ standard and $16^{th}$ in $\mathrm{XII}^{\mathrm{th}}$ state board examinations.
- Awarded by *Viren J. Shah*, ex-governor of West Bengal, for $10^{th}$ rank in Kolkata zone in $\mathrm{X}^{\mathrm{th}}$ 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 $\mathrm{X}^{\mathrm{th}}$ standard and $16^{th}$ position in $\mathrm{XII}^{\mathrm{th}}$ 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

| | | |
|---|---|---|
| Program Committee | Usenix Security Symposium (Usenix) Artifact Evaluation | *2022* |
| | Workshop on Binary Analysis Research (NDSS BAR) | *2022, 2023* |
| | Workshop on Decentralized Finance and Security (ACM CCS DeFi) | *2022* |
| | Conference on Emerging Security Information, Systems and Technologies (Securware) | *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]

**The Verge**, *The black market for blue checks*, (Oct 2022).

**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).

**DevNews Podcast**, *Elon Musk's Twitter Takeover, Security Vulnerabilities in Web3, and Experimenting With the TikTok Algorithm*, (Apr 2022).

**The Atlantic**, *Please Ignore My Last 577 Tweets*, (May 2022).

**TruthDAO Podcast**, *NFT Academic Roundtable*, (May 2022).

**TruthDAO**, *Fraudulent "Wash Sales" Roil Booming NFT Market*, (May 2022).

**TruthDAO**, *Fake Trading, Stablecoin Troubles, and the Threat of Crypto Regulation: Our Crypto DeFined NFT Roundtable Takeaways*, (May 2022).

Sailfish [9]

**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).