Sanket Goutam

Ph.D. Candidate · Stony Brook University

Department of Computer Science, Stony Brook University, Stony Brook, NY

+1 919-946-6070 | sanketgoutam@gmail.com | sgoutam.github.io

Research Experience

Samsung Research America — *Mountain View, CA*

Mentors: Dr. Michael Grace, Dr. Hayawardh Vijayakumar — *May 2023 - Present*

- Security Researcher – Intern
- My research focuses on designing a privacy framework for the Android API subsystem

Ethos Lab, Stony Brook University — *Stony Brook, NY*

Advisor: Dr. Amir Rahmati — *Aug. 2021 - Present*

- Research Assistant
- My (anticipated) Ph.D. thesis : "Privacy-centric Infrastructures for Pervasive Computing Ecosystems"

WSPR Lab, North Carolina State University — *Raleigh, NC*

Co-Advisors: Dr. William Enck, Dr. Brad Reaves — *2017 - '19*

- Graduate Student Researcher
- Master Thesis: "Simple Least Privilege Network Policies for Smart Homes"

Education

Stony Brook University — *Stony Brook, New York*

Ph.D., Computer Science — *2021 - present*

GPA: 3.93/4.0

North Carolina State University — *Raleigh, NC*

M.S., Computer Science — *2019*

GPA: 3.875/4.0

VIT University — *Tamil Nadu, India*

B.Tech, Computer Science & Engineering — *2017*

GPA: 8.84/10.0

Industry Experience

2023-now	**Samsung Research America**, Research Intern, KNOX Security	*California*
2019-2021	**HPE Aruba Networking**, Software Engineer-II, OS Infrastructure	*California*
2018	**HPE Aruba Networking**, Software Engineering Intern, OS Infrastructure	*California*
2017	**GE Digital**, Software Engineering Intern, AppOps	*Bangalore*

Selected Publications

** = Equal Contribution*

Peer-Reviewed Conference Publications

C3 **Sanket Goutam** and Amir Rahmati, "Identity Management Framework for IoT Ecosystems"(Anonymized Title), in *Under Submission*, 2023.

C2 **Sanket Goutam***, Yoonsang Kim*, Amir Rahmati, and Arie Kaufman, "Erebus: Access Control for Augmented Reality Systems", *In Proceedings of the USENIX Security Symposium* **(USENIX Security'23)**, August 2023.

C1 **Sanket Goutam**, William Enck, and Bradley Reaves, "Hestia — Simple Least Privilege Network Policies for Smart Homes", *in Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks* **(WiSec'19)**, May 2019. (Short Paper).

Book Chapters

B1 Kiruthika Devi B.S., **Sanket Goutam**, Anisha Jain, and Sai Pranav R, "Enhancing Web Security using Learning Algorithms for Anomaly Detection", in the *Handbook of Cloud Security Parameters: Real-Time Measurements*, Shanlax Publications, 2016.

Presentations

P4 "Privacy-preserving API Frameworks for Samsung Knox SDK", *Samsung Research America*, California, 2023.
P3 "Erebus: Access Control for Augmented Reality Systems", *32nd USENIX Security Symposium (USENIX Security'23)*, Anaheim, California, 2023.
P2 "Designing an Access Control Framework for AR/VR systems", *Graduate Research Day (GRD)*, Stony Brook University, New York, 2022.
P1 "Hestia: Simple Least Privilege Network Policies for Smart Homes", *12th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'19)*, Miami, Florida, 2019.

Patents

Pa1 Enforcing Least Privilege Network Policies for Smart Homes, *NCSU Invention #19262*, 2019

Fellowships & Awards

Fellowships

2021 -'24 **Excellence Fellowship**, Stony Brook University
2022 -'24 **Inclusive Computing Fellowship**, Dept. of Computer Science, Stony Brook University

Conference Grants

2024 **Student Support Grant**, NDSS Symposium
2023 **Student Grant**, USENIX Security Symposium
2023 **Student Travel Grant**, IEEE Security & Privacy Symposium (S&P)
2021 **NSF Student Conference Award**, ACM CCS
2019 **Student Travel Grant**, ACM WiSec

Honors

2020, '21 **Recognition Awards for contributions to high-impact projects**, HPE Aruba Networking
2015 **Regional Qualifiers**, ACM International Collegiate Programming Contest (ACM ICPC)

Professional Activities

Artifact Evaluation Committee

2024 **ISOC Network and Distributed Systems Symposium (NDSS)**, Reviewer
2023-24 **USENIX Security Symposium (USENIX Security)**, Reviewer
2023 **ACM Conference on Computer and Communications Security (ACM CCS)**, Reviewer

Peer Reviews

2023 **IEEE Transactions on Dependable and Secure Computing (TDSC)**, Sub-Reviewer
2022 **USENIX Security Symposium (USENIX Security)**, Sub-Reviewer
2018 **ISOC Network and Distributed Systems Symposium (NDSS)**, Sub-Reviewer

Service and Outreach

2023 **IEEE Security & Privacy Symposium**, Student Volunteer *California*
2022-24 **Pedagogy and Inclusivity Training for Computer Science TAs**, CIC Fellow *SBU*
2022-24 **WAC Lighting Foundation Invitational Science Fair**, Judge *New York*
2022 **CSIRE (Computer Science and Informatics Summer Research Experience Program)**, Reviewer *SBU*

Invited Talks

2018 **Silicon Valley Outreach Program for K-12 Students**, Speaker *California*
2018 **Students in Programming, Robotics and Computer Science (SPARCS)**, Mentor *NCSU*

Teaching Experience

2022	**CSE508-Network Security**, Teaching Assistant	*SBU*
2021	**CSE331-Computer Security Fundamentals**, Teaching Assistant	*SBU*
2019	**CSC591-Privacy**, Teaching Assistant	*NCSU*
2019	**CSC591-Cellular Network Security**, Teaching Assistant	*NCSU*
2018	**CSC415-Software Security**, Teaching Assistant	*NCSU*

Selected Projects

Access Control Mechanism for Augmented Reality Devices : This is a research project where I developed a Domain-specific Language (DSL) to enforce access control policies for AR devices. It uses a NLP engine (using spaCy), a language transpiler (using ANTLR in C#), and policy enforcement in the Android subsystem.

Public Key Infrastructure(PKI) for IoT Devices : An ongoing research project where I am developing a PKI for IoT devices. The goal is to develop a framework for certificate enrollment specifically for resource-constrained off-the-shelf embedded devices.

DiemBFT State Machine Replication : I implemented parts of the DiemBFT consensus algorithm to develop a distributed log replication system in Python. This was undertaken as a course project.

Distributed Data Store and Shared Memory Infrastructure for ArubaOS : One of the core projects I was involved in at Aruba Networks, where I helped redesign a distributed data sharing service to support a 10x scale increase for the Aruba 9240 controller. I developed some of the core infrastructure services, Linux IPC services, and memory allocation to solve the scalability challenges of a large distributed network.

Message streaming service for Aruba controllers using gRPC : For my internship project, I developed a device-to-cloud message streaming application using gRPC in C++ with cross-compilation support to run it on the C-based ArubaOS.

Relevant Skills

Programming : Python, C/C++, C#, R, Matlab
Utilities : Docker, certbot, ANTLR, spaCy, ptrace, gdb, Git, LaTeX, OpenFlow, Ryu, Wireshark, protobuf, gRPC
Systems : Linux, OpenWRT, Raspberry Pi, Windows