Saket Upadhyay

Contact Information	E-mail:	saketupadhyay@protonmail.com; saketupadhya@gmail.com
	Web:	`https://saket-upadhyay.github.io/`
	LinkedIn:	`https://www.linkedin.com/in/saketupadhyay/`
	GitHub:	`https://github.com/Saket-Upadhyay`

Key words Malware Analysis, Reverse Engineering, Threat Intelligence and Analysis, Adaptive Defense Systems, Network Security and Resiliency.
open to all ideas near these topics

About me A final-year undergraduate student with experience in academic and industrial cyber security research. Looking for opportunities for a doctoral degree after my graduation, and I aim to continue my career in academia after that.

Research Interest My research interest is in the area of adaptive and resilient network and computer security. With the exponential rise in consumer-level computational power comes the need for more sturdy cyber systems and new standards to ensure secure and reliable future computer systems. I want to explore how can we achieve more robust and resilient computer/network structures by tweaking existing solutions or creating new strategies. I like thinking along the lines of 'self-healing', 'situation-aware / state aware', and 'active defense' mechanisms. Also, I love exploring new malware attack tactics and understanding more about the developments of the attack vectors over time to check what kind of changes we need in our defense strategies.

Education

Vellore Institute of Technology, VIT Bhopal University, India
Division of Cybersecurity and Digital Forensics
BTech: Computer Science and Engineering with specialization in Cybersecurity and Digital Forensics. (May, 2022); CGPA: 8.55/10 *(till Winter 2020)*

Patents

1. "A scanning device, a system and a method for characterization of external devices." 2021-06-16, regno.: 369424 (IND)
2. "Nature-inspired adaptive defence system forearly intrusion detection"; 2021-11-10, regno.: 0211006268. (AUS)

Copyrights

1. "NICS Hardware Security Module Driver."; 25100/2021-CO/SW; 15.10.2021
2. "Firefly-inspired Early Alert Mechanism for Intrusion Detection System."; 23581/2021-CO/SW; 29.09.2021
3. "NICS-based Network Testbed for Adaptive Defense Analysis"; 23470/2021-CO/SW; 28.09.2021.
4. "PAMC: Platform for Android Malware Classification."; SW-14439/2021; 2021.

Publications

1. "AI-assisted Computer Network Operations testbed for Nature-Inspired Cyber Security based adaptive defense simulation and analysis"; Shishir Kumar Shandilya, Saket Upadhyay, Ajit Kumar, Atulya K. Nagar; Future Generation Computer Systems,Volume 127, 2022; `https://doi.org/10.1016/j.future.2021.09.018`.

2. "PACER: Platform for Android Malware Classification, Performance Evaluation and Threat Reporting.";
   Kumar A, Agarwal V, Kumar Shandilya S, Shalaginov A, Upadhyay S, Yadav B.; Future Internet. 2020; https://doi.org/10.3390/fi12040066
3. "PACE: Platform for Android Malware Classification and Performance Evaluation";
   A. Kumar, V. Agarwal, S. K. Shandilya, A. Shalaginov, S. Upadhyay and B. Yadav; 2019 IEEE International Conference on Big Data (Big Data), 2019, pp. 4280-4288, https://doi.org/10.1109/BigData47090.2019.9006557

Publications in queue

1. "Nature-inspired malware anomaly detection in android-based systems";
   invited chapter for 'Advances in Nature-inspired Cyber Security and Resilience', Springer; (accepted, pre-publication stage)
2. "Modified Firefly Optimization Algorithm-based IDS for Nature-Inspired Cybersecurity",
   IEEE Access (under review)

Professional Experience

Uptycs, Banglore, India (uptycs.com)

Security Research Intern **July, 2021 - to date**

As a security research intern, my job here is to do (help in) malware analysis, security compliance, and researching optimization techniques for malware detection for enterprise endpoints. I help in classifying malware families and design optimization strategies specific to the malware family's attack signature, along with analyzing different attack vectors registered in the global threat intelligence database.

Madhya Pradesh Police Department, Bhopal, India

Project Intern **May, 2020**

Development of an SOS application for Android-based smartphones capable of serving niche needs of the group, facilitating rewards points for reporting crimes to volunteers.

Azure Skynet Solutions, India

Trainee Intern **July, 2019**

As a cyber security trainee, I learned about penetration testing and conducted tests, and generated reports for the same for 5 different systems.

Honors and Awards

1. Best Paper Award, IEEE International Conference on Big Data 2019 [Certificate]
2. 1st Rank, DEFCON 28 Secure Code Tournament
3. Winner TrendMicro Cloud Security CTF (DevSecCon)
4. 1st Rank in Development Security Conference 24 (2020) Coding Tournament
5. Winner HackCoVIT'20 (National Level Hack-a-thon) [Certificate]
6. 1st Runner-up, HackDSC Hackathon [Certificate]
7. 1st Rank in DerpCon 2020 SCW Tournament

Talks & Presentations

1. **Automating malware process scanning with Python3** [Web]
   PyCode2021 Conference

2. **Firefly Inspired IDS Optimisation (NICS)** [Youtube]
   CyVIT 2021: International Cybersecurity Conclave

3. **Malware Hunting with Machine Learning** [Youtube]
   Penn State World Campus Tech Club, Penn State, Pennsylvania

4. **Multi-Model Malware Detection and Classification.**
   "Hybrid Intelligent Systems (HIS 2019)" Conference

Projects

1. **WiSDOM: WriterScript based Data Obfuscation Module** [GitHub]
   Created during HackDSC'21 (Google DSC's national level Hack-a-thon) under Open Innovation in Data Privacy and Security domain. Secured second position.

2. **WriterScript** [GitHub]
   Word Count dependent Esoteric Programming Language, Interpreter made in Python3

3. **xSFOS** [GitHub]
   A simple 64bit Linux Kernel from scratch. I am making this project a teaching tool. The aim is to create well-structured documentation and proper releases on Git so that anyone can trace the steps and learn the same concepts.

4. **NS3 Cybersecurity Simulations** [GitHub]
   Collection of cybersecurity simulations in NS3 and C++

5. **SAMPARK : Website Security Scanning Framework** [GitHub]
   National Hack-a-thon project (Won 1st Rank in Information Security Domain)

6. **Android Permission Extraction and Dataset Creation with Python** [GitHub]
   Project module for PACE and PACER (our research papers).

7. **Movement Tracing in Android using Polygraph lines.** [GitHub]
   Project in association with Madhya Pradesh Police Department (India) under CSDF Department, VIT Bhopal.

Languages

1. Hindi (Native)
2. English (Professional/Academic Proficiency)
3. Russian (Elementary, Learning)

Test Scores

IELTS Academic **Overall: 8.0/9** ; Listening: 9/9, Reading: 9/9, Speaking: 7.5/9, Writing: 7/9

References

Available upon request.