VIJAY PRAKASH

🌐 https://viz-prakash.github.io/ ◇ in ◇
✉ vijay.prakash@nyu.edu

EDUCATION

New York University *Sep 2021 - now*
PhD in ECE

University of Florida *Aug 2016 - May 2018*
MS in Computer Science
Graduate Certificate in Information Security *May 2018*

University of Pune, Pune *Jul 2010 - Jun 2014*
Bachelor of Engineering in Information Technology

SKILLS

Programming Languages and Software Engineering

- Proficient in Python, Java, C, C++, and Bash; beginner with MATLAB

Vulnerability Research

- Static analysis/debugging: CodeQL, GDB, IDA, Ghidra, OllyDbg
- Fuzzing: familiar with fuzzers like AFL++
- Audited IoT related protocol implementations with CodeQL, for e.g., Android Bluetooth and ARM MbedOS Bluetooth stack, XMPP, and MQTT
- CVEs: critical **CVE-2021-0968** in Google's Android Bluetooth stack and **CVE-2020-1999** in PAN-OS through internal security review
- Cryptography, binary exploitation, and reverse engineering experience from CTFs and academic projects

Network Security

- Proficient with various layer 2, layer 3, DNS, and application layer protocols
- Networking utilities: Wireshark, tcpdump, Nmap, traceroute, and iptables
- Can deploy and manage commercial intrusion protection systems (IPS), like Palo Alto Networks Next-gen firewall
- Proficient in analyzing zero day vulnerabilities and writing IPS signatures that can work on industrial scale

RESEARCH

Security, Privacy, and Supply Chain Issues in IoT Ecosystem Sep 2021 - now
New York University mLab

- Assessing impact of IoT devices on users' (individual and enterprises) security and privacy in local network with IoT Inspector
- Assessing the update practices in IoT ecosystem using data collected with IoT Inspector
- Analyzing Over-the-Top TV streaming devices to understand profiling and behavioral targeting for advertisements on these devices

Fingerprinting JavaScript (JS) Obfuscation Using Machine Learning Nov 2019 - June 2020
Palo Alto Networks

- Developed a prototype to fingerprint a specific type of JS obfuscation using deep neural network (DNN) model with accuracy of 93% and 0.1 % false positive (FP) rate
- Built a open source tool called **TCPsession** to extract obfuscated JS in HTTP traffic from PCAPs

Examining DES-based Cipher Suite Support within the TLS Ecosystem Jan 2018 - Apr 2018
University of Florida

- Researched about 36 possible DES based ciphers as targets for scanning
- Designed and implemented a multi-threaded scanner in Java to scan the large IP address list
- Scanner was capable of performing TLS handshakes using Zgrab2 for selected 36 ciphers
- Used NoSQL database to store the handshake results to be analysed by Apache Spark server
- Tool was used to scan 31 million IP address and perform TLS handshakes over time of five months

Malware Classification Aug 2017 - Nov 2017
Lastline Inc. (now VMware)

- Performed feature engineering to classify PE malware files by just using static features, for e.g., strings, and treating PE as an image compressed with Haar transformation
- Built a fast extractor, capable of running along with an inline Intrusion Protection System (IPS), to extract those static features from malware executables

- Used a model that classified samples by similarity of their features using MinHash and local sensitivity hashing (LSH). Model detected malwares with accuracy of 35% and false positive rate of 0.047%.
- Classifier could reduce the computation burden of automated malware analysis sandbox engine by 35%

Mallodroid Aug 2016 - Dec 2016
University of Florida

- Researched about improving accuracy of the static code analysis tool Mallodroid, which is used to detect TLS/SSL misconfiguration in Android applications
- Improved it's detection rate by 21% and reduced its false positives (FP) rate by 1.7%

INDUSTRY EXPERIENCE

Palo Alto Networks *May 2018 - Aug 2021*
Senior Security Researcher *3000 Tannery Way, Santa Clara, CA, 95054, US*
Security Research

- Vulnerability research on softwares widely using in IoT products, for e.g. Android and ARM Mbed BLE stacks
- Built a system using ML to fingerprint specific type of obfuscated JavaScript in HTTP traffic
- Built a library in Python to extract TCP session data from a PCAP that is faster than ∼50 times using Wireshark
- Contributed to development of a system to de-obfuscate JavaScript before running inline IPS signature against it
- Contributed to development and improvement of next-generation firewall technology
- Found a high severity **CVE-2021-0968** in Google's Android Bluetooth stack, and **CVE-2020-1999** in Palo Alto Networks IPS OS
- Analyzed numerous publicly disclosed vulnerabilities, including many Zero-Days, to develop IPS signatures

Lastline Inc. *Aug 2017 - Nov 2017*
Software Engineer Intern *6950 Hollister Ave, Suite 100, Goleta, CA, 93117, US*
Anti Malware Group

- Built a classifier to detect PE (Windows executable) malwares using ML

Amazon *May 2017 - Jul 2017*
SDE Intern *440 Terry Ave N., Seattle, WA, 98109, US*
AWS Perimeter Protection

- Built a integration testing framework in Python for AWS Anti-DDoS/WAF product

GS Lab *Jul 2014 - Jul 2016*
Software Engineer *Pune, MH, India*
Ensuring Confidentiality and Integrity of VMs Deployed in Cloud Data Centers

- Rewrote the integrity checking module in C++ for Linux and Windows to improve stability and add concurrency; resulted in performance improvement of 10% for each thread
- Lead two-member team to write a Windows OS kernel-space boot driver for doing the integrity checks of windows OS
- Contributed to development of Docker plugin that triggered the integrity check
- Automated the creation of initrd (inital ramdisk) images for various flavor of Linux OSs for integrity check
- Improved shell scripts to mount different formats of VM and Docker images that resulted in a performance improvement of 300% in some integrity checking control flows

PUBLICATIONS

Examining DES-based Cipher Suite Support within the TLS Ecosystem Jan 2018 - May 2018
Vanessa Frost, Dave (Jing) Tian, Christie Ruales, **Vijay Prakash**, Patrick Traynor, and Kevin R. B. Butler. In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security (Asia CCS '19)

ACHIEVEMENTS

2nd place at South Eastern Collegiate Cyber Defense Competition (SECCDC) representing UF	*Apr 2018*
3rd place at South Eastern Collegiate Cyber Defense Competition (SECCDC) representing UF	*Apr 2017*
Favorite hack award at SwampHacks hackathon chosen by The Agency(UF) and Gainesville Dev Academy	*Jan 2017*
2nd runner-up in an organization wide 24 hours hackathon held at GS Lab	*Feb 2016*
2nd best performing engineer of the year among new graduates at GS Lab	*2014-2015*
Senior year project was selected in as a five best projects in the entire engineering school	*May 2014*

OTHER PROJECTS

P2P File Sharing project Jan 2018 - May 2018
Final course project for Computer Networks *University of Florida*

- Built a program in Java which allows file sharing using P2P protocol, very similar to BitTorrent

SwampCTF March 2018 - now
UF Student Info-Sec capture the flag competition *University of Florida*

- Problem creator and organizer at yearly hosted UF Student Info-Sec's (UFSIT) CTF, which has 1000+ participating teams from all over the world

DNS Security *Sep 2016 - Oct 2016*
Course project for Computer & Network Security *University of Florida*

- Developed a C program that successfully exploit DNS cache poisoning vulnerability on DNS servers

Shoulder-surfing Resistant Authentication Mechanism *Aug 2013 - Mar 2014*
Final year project *University of Pune*

- Developed a shoulder-surfing resistant Android application to overcome the deficiency of pattern locks in Android OS