VIJAY PRAKASH

+1-352-284-3471 ◇ vijay.prakash@ufl.edu
3427 Bella Vista Ave, Santa Clara, CA, 95051
https://viz-prakash.github.io/ ◇ www.linkedin.com/in/viz-prakash/ ◇ www.github.com/viz-prakash

EDUCATION

University of Florida *Aug 2016 - May 2018*
Master of Science in Computer Science *GPA- 3.81*
Graduate Certificate in Information Security *May 2018*
- Researched under Prof. Kevin Butler and Prof. Patrick Traynor
- Worked under Prof. Joseph Wilson for various cybersecurity competitions

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

ACADEMIC 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)

RESEARCH PROJECTS

Fingerprinting JavaScript Obfuscation using ML Nov 2019 - June 2020
- Came up with an idea of fingerprinting a specific type of JS obfuscation using ML
- Built a tool to extract JS from PCAPs containing obfuscated JS in HTTP traffic
- Collaborated with ML team to pick a suitable model for the problem; used a Deep Neural Network (DNN) model
- Model was able to fingerprint the obfuscation with 93% accuracy and 0.1% false positive (FP) rate

Examining DES-based Cipher Suite Support within the TLS Ecosystem Jan 2018 - Apr 2018
- 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 using machine learning (ML) Aug 2017 - Nov 2017
- Researched about different static features of PE malware files that could be used as features for training a ML model, like - strings; treating executable as an image compressed with Haar transformation
- Built a fast extractor, capable of running along with an inline Intrusion Protection System (IPS), to extract static features from malware executables
- Trained the ML model with extracted features, improved the extractor further for better results
- Classifier detected malwares with decent accuracy of 35% and false positive rate of 0.047%, resultantly it could reduce the computation burden of automated malware analysis sandbox engine by 35%

Mallodroid Aug 2016 - Dec 2016
- 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%

PROJECTS

TCPSession Jan 2020 - June 2020
Fingerprinting JS obfuscation *Palo Alto Networks*
- Built an open sourced native Python library from scratch to extract TCP sessions from a pcap
- Compliant with latest TCP RFCs
- Performs TCP stream assembly, handles all the cases including re-transmission, out-of-order delivery, bit loss errors, and packets that test the protocol RFC
- On an average 50 times faster than using Wireshark

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

INDUSTRY EXPERIENCE

Palo Alto Networks *May 2018 - Now*
Senior Security Researcher *3000 Tannery Way, Santa Clara, CA, 95054, US*
Security Research
- Doing vulnerability research on IoT software by fuzzing them with AFL++
- 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, which 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 critical vulnerability **CVE-2020-1999** in PAN-OS in internal security review
- 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 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 *Amar Arma Genesis, Baner, Pune, 411045, MH, India*
Data Center Security Product: Providing confidentiality and integrity of VMs deployed in cloud
- Rewrote the entire ∼3000 lines of C++ written integrity checking module to make it multi-threaded and fix its stability issues for both Linux and Windows platforms
- Improved performance of integrity checking module by 10% in a single control flow
- Lead two-member team to write a Windows OS kernel-space boot driver for doing the integrity checks of windows OS
- Investigated, designed, and contributed to the development of Docker plugin that triggers the integrity check
- Wrote shell scripts to create initrd (inital ramdisk) images for various flavor of Linux OSs
- 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

SKILLS

Programming Languages
- Proficient in Python, Java, C, C++, and Shell.

Security
- Proficient with networking protocols and networking utilities, like - Wireshark, tcpdump and intermediate experience with Nmap, traceroute, and iptables
- Intermediate experience with binary analysis tool GDB, IDA, Ghidra, OllyDbg, and Metasploit
- Cryptography, binary exploitation, and reverse engineering experience from CTFs and academic projects

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 hires straight coming from college, at GS Lab	*2014-2015*
Final year project was selected in five best projects in college	*May 2014*