Vaibhav Hemant Dixit

480-410-0993

Tempe, Arizona | vaibhav.hemant@gmail.com | www.vaibhavdixit.com | www.linkedin.com/in/vaibhavhd

OBJECTIVE

Graduate student with industry experience, seeking full-time positions in software development and cybersecurity domains

EDUCATION

Arizona State University, Tempe, AZ Master of Science, Computer Science ***May 2018, GPA 3.67***

Courses - Software Security, Automated Binary Analysis, Foundation of Algorithms, Embedded Operating System Internals

Vellore Institute of Technology, Tamil Nadu, India Bachelor of Technology, Information Technology ***May 2013, GPA 3.6***

SKILLS

Languages - *Proficient* - C, Java; *Familiar* - Python, JavaScript, Shell, Yang. **Tools:** Gdb, Wireshark, Objdump, IDA, Scapy.

Others - Pentesting, SDN, Openflow, Openstack, TCP/IP, WLAN, ELK, Android, Git, Docker, Jenkins, Eclipse, Linux, Windows.

PROFESSIONAL EXPERIENCE

Graduate Research Assistant, *Center for Cybersecurity and Digital Forensics, ASU* ***Dec 2016 to present***

Designed a **novel** SDN-based **adaptive security** mechanism on ASU's Science-DMZ network. Continuous behavioral analysis of the attacker by propagating the attack to a quarantined research zone.

- **Devising countermeasure** generation algorithm on Elastic Search Cluster using attack graph with CVSS scores of compromised services. Results of **research proved useful** in blacklisting IPs and for hardening campus network servers.

Software Engineer, *Samsung Electronics, India* ***Jul 2013 to Jun 2016***

- **Built advanced features** like 802.11w, secret SSID and multiband support by making control path handlers at kernel space and patching Google Android supplicant at user space. Contributions made way to Samsung phones and market.
- **Implemented and improved** WEP, WPA, WPA2 secured connection procedures for Wi-Fi softAP driver. Quickly identified critical kernel bugs like memory leaks and race conditions in the driver and **for features not directly owned**.
- **Automated entire process** of build, sanity and stress testing by working **beyond assigned duties.** Created scripts linked with git server to catch development bugs like regressions, kernel crashes before reaching the test team. This greatly **reduced overall bug fixing time** and had a direct impact in winning agile deadlines by a minimum profit of 3-6 days.

RECENT PROJECTS

- **Evolutionary mutational fuzzer**: Developed a Python based automatic binary fuzzer to find the vulnerabilities in the executable programs. Used Gdb and Valgrind to trace the basic blocks inside the assembly version of the binary. Mutating the input seed using bit manipulation techniques to cover infinite branches of the code and make it crash.
- **Fingerprinting and attacking SDN controllers**: Threat modelled controller using a security framework in Python. Discovered vulnerabilities: dictionary attack using REST (**CVE-2017-1000406**) and a DoS attack (**CVE-2017-1000411**).
- **Advanced software firewall for SDN:** Single handedly designed a centralized Java application for policy conflict detection and dynamic resolution which pulled topology information using OpenFlow APIs and generated a **complex logical graph of flow rules** to validated **security compliance**. Research findings are published in ACM security workshop.
- **Framework for exploit detection and patching in Capture the Flag competition**: Participated in a project based CTF game. Developed a Python based network attack reflector using Scapy. Contributed to defense framework to reverse engineer the binaries, patch the application/web vulnerabilities in real time. Team won the iCTF competition.
- **Embedded programming in Intel Quark based Galileo board**: Team project aimed to provide an understanding of internals of Linux and RTOS kernel architecture by implementing device drivers. Investigated Linux kernel source code including memory management, kernel synchronization, device driver design and trace, debug support. Programmed **ioctls**, **syscall** interface, **static and dynamic probes, MISC drivers**, etc.
- **Android application for distributed image reconstruction**: Team made a volunteer computing service where a master phone distributes the work to slaves based on attributes like processing power, battery, signal strength, etc.
- **Full-fledged compiler in C**: Performed lexical and semantic analysis and developed a parser, type checker and compiler.

PUBLICATIONS († First author) (‡ Co-author)

† **Challenges and Preparedness of SDN-based Firewalls** at ACM CODASPY SDNNFV Workshop 2018, Tempe, Arizona.

‡ Science DMZ: **Software Defined Networking based Secured Cloud Testbed** at IEEE NFV-SDN 2017, Berlin.

‡ HONEYPROXY: **Design and Implementation of Next-Generation Honeynet via SDN** at IEEE CNS 2017, Vegas.