Ilhan Mohammed Raja

26519 Ridgestone Park Lane, Cypress, TX 77433
832-571-5823 ilhan.raja@icloud.com

Texas A&M - Engineering Honors (Computer Science) 2021
Stanford University - Center of Professional Development - Adv Computer Security Certificate

Software Projects
http://github.com/YungRaj/
http://yungraj.com

Objective

- Aspires to become a kernel engineer, firmware developer, CPU architect engineer, software security engineer for OS vulnerability research or general software engineer for iOS/macOS/etc

Skills

- Research on the BIOS and UEFI specification as well as projects dedicated to them (CoreBoot, Tianocore, Clover, Chameleon, and GRUB)
- Research on kernel engineering (XNU, IOKit, BSD, and Linux) as well kernel reverse engineering for security purposes (iOS and macOS) - checkra1n, taking apart an iPhone in the virtual world
- Knows approximately 9 programming languages, namely lower level machine dependent languages such as Objective C(++), and x86/ARM Assembly

Programming Languages

Proficient in C, C++, Objective C, x86, Java
Moderate in Swift, ARM Assembly, Python, SQL, JavaScript, Bash scripting and ACPI Machine Language

Experience

Apple Internship - Firmware Security Engineering
August 2017 - June 2018

- Use the new hash verification tool named eficheck to check customer binaries for malware in the wild using Python and C and create a production framework in Python to detect malicious payloads coming from customers
- Fix Coverity, the static analysis tool to parse EFI code and detect real buffer overflows, information leaks, etc in shipping code
- Fuzz NVRAM variables stored on the flash chip using an IOKit and userland interface
- Develop malware for EFI by fuzzing low level implementations of DHCP, HFS+, APFS (unsuccessful), PCI, SPI, etc
- Triage and fix existing bugs found from fuzzing low level implementations
- Exploit vulnerabilities found in EFI file system implementations to bypass firmware passwords on MacEFI machines
- Inject x86 payloads into existing MacEFIFirmware to detect DMA buffer vulnerabilities and other security issues in hardware/firmware implementation
- Create full fuzzing infrastructure using the simics x86 emulator for NVRAM variables
- EFI security team worked on T2 Security

Developing for BIOS and UEFI - Software Development
May 2014 - October 2017

- Use x86/ARM assembly and C to write lower level startup machine code for modern machines
- Conform to the specification of the firmware interfaces and study development of projects such as Clover and Chameleon
- Read research papers on System Management Mode, TPM, ARM TrustZone, SGX, Intel Microcode, Cache Evictions, MDS, etc
- Review open source UEFI firmware through existing reference implementations such as CoreBoot + Tianocore (ACPI and EDK2 development kit)

iOS Reverse Engineering and Jailbreaking
September 2015 - October 2020

- Reverse engineering iOS kernel, binaries and firmware dumps using IDA Pro, Hopper, radare2, class-dump, cycript, etc through dynamic and static analysis of assembly level instructions for x86/ARM, interface definitions and API/ABI's
- Read research papers on the *OS kernel heap, WebKit heap, JavaScript implementations, pointer authentication codes, APRR, KTRR. PPL, KPP, attack vectors in *OS, etc
- Inject into system processes and applications using the Mobile Substrate library using the Theos development tools and reverse engineering exploration (http://github.com/DHowett/theos)
- Implemented a Mobile Substrate tweak for the Snapchat application that notifies the user if a Snapchat streak is going to be over and provides hooks into the Application now on Cydia http://cydia.saurik.com/package/com.yungraj.streaknotify

NOTE: StreakNotify is planned into the Phantom Lite project (@CokePokes on Twitter)

OSX86
October 2013 - May 2014

- Participated in a hobby project dedicated to installing OS X on a non-Apple Intel and AMD machines called OSX86
- Worked with lower level subsystems and API's in OS X and iOS such as Mach, IOKit, dyld, Mach-O, launchd, macf, sandbox, kauth, BSD, libkern, osmfk, libSystem, SpringBoard, Mach vm, hfs+, GCD, UIKit/Foundation, and Core Foundation to support the ecosystem
- Vastly skilled in Unix-based environments (bash/shell scripting)
- Supported the community by providing advanced technical support in an IRC chat
- Shared full set instructions to install OS X with binary patches, setup instructions and shared ACPI patches and tables such as the DSDT, SSDT and others on github (http://github.com/ilhanraja/XPS-13-9350-OS-X)
- Wrote a MachO binary parser before interning at Apple, it analyzes Objective C metadata, load commands, symbol tables, code signatures (verifies), etc

Application Development (iOS and Android)
May 2013 - January 2015

- Use Xcode and Android Studio to write applications in Java and Objective C(++)
- Utilize the frameworks such as UIKit, OpenGL, SpriteKit, SceneKit, Foundation, CoreFoundation, AppSupport, BulletinBoard, Security, GLKit, SpringBoardServices , CoreGraphics, CoreAnimation and many more to build complete products
- Developed This is the End for the iPhone (github)

Extracurriculars
TAMU CyberSecurity Club
November 2016 - February 2017

- Collectively learn reverse engineering, software security through the static and dynamic analysis tools such as OllyDbg, IDA Pro, radare2, Hopper, and the command line utility class-dump
- Participate in code hacks such as the NSA codebreaker and Microsoft coding competition

Service
The Citizen's Foundation
30 hours: Feb 2012 - March 2014

- Actively participated as a member of the local chapter of a national Non Government Organization to provide funds for schools in the underprivileged parts of Pakistan
- Volunteered for the local charity and enticed donations to those interested in the organization

Education
Cypress Ranch High School
Class of 2016

- Summa Cum Laude

Texas A&M University
Class of 2021

- Computer Science and Engineering
- Honors

Stanford University

- Center of Professional Development - Advanced Computer Security Certificate (online @ scpd.stanford.edu)
- Cryptography, Network Security, Mobile Security, SQL Injection/Buffer Overflows, XSS attacks, etc

Publications read

- MacOS and iOS Internals, Volume I: Kernel Mode
- MacOS and iOS Internals, Volume II : User Mode
- MacOS and iOS Internals, Volume III: Security & Insecurity
- MacOS and iOS Internals (2012)
- The A64 instruction set
- The EFI specification