Saagar Jha

@saagarjha ⌂ San Jose, California

☎ (408) 707-8023 ✉ saagar@saagarjha.com

Experience

Director, Sophisticated Threats @ Corellium Aug 2023 –

Spun up a new team to research and identify mobile spyware originating from attackers with nearly unlimited resources.

Software Engineer, Android Security @ Google May 2022 – Aug 2023

Developed resilient techniques to thwart bad actors targeting Android by following them into where they operate.

Client Performance Engineer @ Twitter Aug 2021 – May 2022

Leveraged deep platform expertise to enable Twitter to navigate its hardest user-facing scalability and reliability challenges.

Contractor to the Radar team at Apple @ Advantis Oct 2020 – Feb 2021

Browser Architect @ Kagi Jun 2020 – Dec 2020

Led development and initial bringup of a new WebKit-based browser for macOS and iOS.

Safari Intern @ Apple Jun 2019 – Jul 2019

Darwin Platform Experience Consultant at Orchid @ SaurikIT Oct 2018 – Dec 2018

Provided architectural and design guidance for Orchid's development efforts on iOS, watchOS, and macOS.

HomeKit QA Tooling Intern @ Apple Jun 2018 – Sep 2018

Education

University of California, Santa Barbara Sep 2017 – Jun 2020

Bachelor of Science Computing, College of Creative Studies Santa Barbara, CA

Regents Scholar, College of Engineering and College of Creative Studies Honors

Personal Projects

unxip (Swift) GitHub

High-performance Xcode archive extraction utility. A carefully designed streaming LZMA decoder (accelerated by Swift Concurrency to effectively harness hardware parallelism) achieves decompression speeds several times faster than Apple's own tools, and transparent APFS compression using LZFSE more than halves final on-disk size.

VirtualApple (Swift) GitHub

Cocoa frontend for the Virtualization framework. Capable of creating macOS VMs, but also exposes a variety of features useful for security research and low-level analysis, including support for kernel debugging and alternative boot policies.

library_injector (C++) GitHub

macOS code injection platform built on EndpointSecurity, DYLD_INSERT_LIBRARIES, and custom AMFI patches.

TSOEnabler (C) GitHub

Kernel extension that exposes hardware total store ordering (via a sysctl) for arm64(e) threads on Apple silicon Macs.

break (Swift) App Store, GitHub

Third-party application for accessing grades, assignments, and other school-related materials from School Loop using a reverse-engineered HTTP REST/WebDAV interface. Features significant use of iOS technologies, including 3D Touch, Touch ID/Face ID, Watch Connectivity, Grand Central Dispatch, the Keychain, and custom UIKit controls.

Miscellaneous

I'm a Capture the Flag player with my team, Shellphish. We're pretty good!

I'm a core maintainer of projects like IINA, a macOS video player, and iSH, a Linux implementation for iOS.

I contribute to a lot of open source projects; here's a couple of them: WebKit, GDB, GNU nano, file, Ghidra.

I have a blog, where I sometimes write satire, publish sandbox escapes, and try to fix software distribution.

I was a WWDC Scholarship Recipient in 2017.

May 2024