Jake **Corina**

SECURITY RESEARCHER

San Francisco / Bay Area

☎ (+1) 206-484-4667 | ✉ j@hijack.rip

Summary

Security researcher with 7+ years of experience in vulnerability research, static and dynamic analysis, binary exploitation, and reverse engineering. Prior work on web browsers (primarily Chrome via V8), Android kernel, and baseband. Interested in both furthering the state of security research and helping to build secure products. I enjoy learning new technologies and environments with recent work/interest in vehicular security and virtualization.

Work Experience

Seaside Security — *Berkeley, California*

CO-FOUNDER & SECURITY RESEARCHER — *Jan. 2018 - Present*

- Conducted vulnerability (0day) research on web browsers and Android phones.
- Applied research techniques to assist in the discovery of vulnerabilities.
- Developed many exploits for found vulnerabilities.

UCSB SecLab — *Santa Barbara, California*

RESEARCHER — *Jun. 2014 - Jun. 2017*

- Thesis on automated discovery of Android kernel driver bugs via static and dynamic (fuzzing) analysis.
- Research across various domains pertaining to reverse engineering & binary exploitation.
  Including: Android/Linux kernel, baseband, TrustZone.
- Early member of the angr symbolic execution team

FLARE Team (FireEye) — *San Francisco, California*

REVERSE ENGINEER & RESEARCHER — *Jun. 2015 - Sep. 2015*

- Internship focused on malware analysis.
- Designed novel malware detection and fingerprinting capabilities utilizing taint tracking.

Presentations

Black Hat Europe — *London, England*

DIFUZZING ANDROID KERNEL DRIVERS — *Dec. 2017*

- Presented work of Master's Thesis on fuzzing Android kernel drivers.
- Explained difficulty of fuzzing ioctl handlers from the ground up and showed how our automated system overcame these difficulties.

GeekPwn — *Shanghai, China*

ONE BYTE TO ROOT — *Oct. 2016*

- Demonstrated a 0day against an Android kernel driver.
- Leveraged a single byte write to kernel memory at a non-arbitrary address to escalate privileges and exfiltrate a photo from the target device.

Publications

Token-Level Fuzzing — *30th Usenix Security Symposium*

CHRISTOPHER SALLS, CHANI JINDAL, **JAKE CORINA**, CHRISTOPHER KRUEGEL, AND GIOVANNI VIGNA — *2021*

- Introduces the concept of fuzzing on a token level for language interpreters rather than adhering to a strict grammar as is commonly the approach. Modifies AFL to operate on tokens rather than a bit/byte level and used to fuzz Javascript interpreters.

DIFUZE: Interface Aware Fuzzing for Kernel Drivers — *24th ACM CCS*

JAKE CORINA, ARAVIND MACHIRY, CHRISTOPHER SALLS, YAN SHOSHITAISHVILI, SHUANG HAO, CHRISTOPHER KRUEGEL, AND GIOVANNI VIGNA — *2017*

- An automated system that uses static analysis to recover interface information for Android kernel drivers and feeds it into fuzzing systems to identify vulnerabilties.

DR. CHECKER: A Soundy Analysis for Linux Kernel Drivers — *26th USENIX Security Symposium*

ARAVIND MACHIRY, CHAD SPENSKY, **JAKE CORINA**, NICK STEPHENS, CHRISTOPHER KRUEGEL, AND GIOVANNI VIGNA — *2017*

- A static analysis tool for discovering vulnerabilities in Linux/Android kernel drivers.

Education

University of California, Santa Barbara

Santa Barbara, CA

M.S. in Computer Science

Sep. 2016 - Jun. 2017

- GPA: 3.92
- Graduate researcher at UCSB SecLab.
- Accelerated M.S. program. Graduate courses are taken starting as an undergraduate.

University of California, Santa Barbara

Santa Barbara, CA

B.S. in Computer Science

Sep. 2012 - Jun. 2016

- GPA: 3.84
- Undergraduate researcher at UCSB SecLab.
- Recruited to the prestigious College of Creative Studies.

Workshops

Introduction to Kernel Exploitation

San Francisco, CA

Creator, Presenter, Trainer

May 2018

- Gave an introductory talk on Linux kernel exploitation to the NCC San Francisco office.
- Created a custom kernel challenge which was used to walk students through the concepts and techniques of kernel exploitation.

Extracurricular Activity

Order Of the Overflow (Organizers of DEF CON CTF)

Member

- Helped organize the worlds most prestigious hacking competition.
- Inspired, conceptualized, and drove the implementation of an in-depth exploitation series based around modern virtualization technology.

Shellphish (CTF Team)

Member

- Participated in numerous hacking (CTF) competitions with several high places.
- Was also a member of the Shellphish Grill Team which was responsible for conducting vulnerability research on various targets.

CVEs

- CVE-2020-6468 (Google Chrome), CVE-2018-3560 (Android Kernel), CVE-2017-15307 (Android Kernel, Huawei), CVE-2017-0802 (Android Kernel, Mediatek), CVE-2017-0636 (Android Kernel, Mediatek)

Honors & Awards

2021	**Organizer**, DEF CON CTF Hacking Competition World Final	*Las Vegas, U.S.A*
2014-2020	**Finalist**, DEF CON CTF Hacking Competition World Final	*Las Vegas, U.S.A*
2018	**Finalist**, Real World CTF	*Zhengzhou, China*
2017	**3rd Place**, WCTF	*Beijing, China*
2016	**Finalist**, Insomni'hack CTF	*Geneva, Switzerland*
2013-2015	**Finalist**, CSAW CTF	*New York City, U.S.A*