Joey **Allen**

Ph.D. Student · Computer Science · Information security

(+865) 771-5936 | jallen309@gatech.edu | jallen89.github.io | github.com/jallen89

About Me

Ph.D. candidate at Georgia Tech's Institute for Information Security & Privacy (IISP). I have eight years of experience in security research that spans web security, systems security, and Android security. My research has recently been focused on security aspects related to the browser, but I am also passionate about many aspects or software engineering and security.

Experience

Google — *Remote*

Software Engineer, Intern — *May 2022 - Present*

- Platform-level HEVC/H.265 decoding testing for Chromium & ChromeOS.
- Updated the ChromeOS testing & verification stack to support testing for hardware-supported HEVC decoding.
- During this time I found 10 previously unknown bugs in Chrome's H.265 decoder.

Georgia Tech - Institute for Information Security & Privacy (IISP) — *Atlanta, GA*

Graduate Research Assistant — *August 2016 - Present*

- Advisor: Wenke Lee
- System Security Research
- Web Security Research

Facebook — *Remote*

Security Engineer, Intern — *June 2021 - September 2021*

- Investigated threat actors that were orchestrating large-scale financial scams using Facebook products.
- Developed novel techniques for attributing on-platform assets to malicious actors.

University of Tennessee — *Knoxville, TN*

Graduate Research Assistant — *May 2014 - May 2016*

- Android Malware
- Mobile Security Research

Projects

JSCapsule: A Forensic-Based Record & Replay System for Chromium — *Atlanta, GA*

Georgia Tech — *July. 2020 - Present*

- Developed JSCapsule, a forensic-based record & replay system for Chromium.
- JSCapsule provides a forensic analyst with the capability to complete deterministic record & replay on web-based attacks.
- Over 2 years of experience with customizing Blink, V8, Chromium, and DevTools framework.
- This work is under submission to CCS'22

TRIDENT: Towards Detecting and Mitigating Web-based Social Engineering Attacks — *Atlanta, GA*

Georgia Tech — *July. 2021 - Present*

- We developed Trident, a novel defense systems that detects web-based social-engineering ads with an accuracy of 92.63%.
- Trident is developed on top of the Chromium Devtools framework.
- This work is under submission to Usenix'23.

XGuard: Understanding and Preventing Remote Code Execution on Cross-platform Desktop Apps — *Atlanta, GA*

Georgia Tech — *April 2021 - May 2022*

- Developed a novel technique for detecting cross-site scripting-based remote code execution (XRCE) in Electron Apps.
- XGuard is a monitoring framework embedded into V8 & Blink that helps maintain the the integrity of sensitive API calls in Electron apps.
- This work was accepted into CCS'22.

Mnemosyne: A Postmortem Watering Hole Attack Investigation System — *Atlanta, GA*

Georgia Tech — *Aug. 2019 - May 2020*

- Developed Mnemosyne, a postmortem forensic investigation system for investigating watering hole attacks against enterprise networks.
- Developed an auditing system for the Chromium browser that tracks attack provenance for web-based attacks.
- Mnemosyne reduces the audit logs required to inspect by 98.17% on average.
- This work was accepted into CCS'20.

DARPA Transparent Computing Program

Atlanta, GA

Georgia Tech

Dec. 2016 - May 2019

- A DARPA and AFRL-funded project that researches how data is tracked between computers, internet hosts, and browsers to improve security.
- Developed Theia, a forensic analysis system that relies on whole-system record & replay for investigating sophisticated APT-style attacks.
- Developed RTAG, an efficient data flow and tracking mechanism that enables cross-host attack investigations.
- This work included publications in CCS'17 & Usenix'18.

PikaDroid: Android Malware Analysis & Detection

Atlanta, GA

Georgia Tech

August 2017 - May 2017

- A ONR-funded project relies on a lightweight and efficient method for Android malware detection.
- A state-of-the-art Android malware detection system that first uses a set of static analysis techniques implemented to extract sensitive behaviors used by an Android app and then constructs a frequency model for classification detection.
- PikaDroid detected Android malware samples with an f-score of 97.41% and maintained a false-positive rate of 0.96%.
- This work was accepted into ACSAC'18.

pDroid (privateDroid): Detecting Suspicious Information Leaks in Android Applications

Knoxville, TN

University of Tennessee

May 2014 - August 2016

- A market-independent static analysis framework that identifies sensitive information leaks in Android applications.
- pDroid correctly classified 91.4% of Android malware with a false-positive rate of 4.9%.
- This work was used as a Master's thesis.

APPE - Finding the Hidden Scenes Behind Android Applications

Knoxville, TN

CURENT: Center for Ultra-Wide-Area Resilient Electric Energy Transmission Networks

May 2014 - January 2015

- Developed APPE, a framework to detect Android applications that made permission requests inconsistent with the app's alleged behavior. APPE verified legitimate versus illegitimate permission requests

Education

Georgia Institute of Technology

Atlanta, GA

Ph.D. in Computer Science

August 2016 - Present

- Advisor: Dr. Wenke Lee

University of Tennessee

Knoxville, TN

M.S. in Computer Engineering

August 2014 - May 2016

- GPA: 4.0/4.0
- Advisor: Dr. Jinyuan Sun
- Thesis: pDroid - Comparing Dataflows to Textual Descriptions in Android Applications

University of Tennessee

Knoxville, TN

B.S. in Computer Engineering

Mar. 2010 - Aug. 2014

- magna cum laude
- GPA: 3.78/4.0

Skills

Programming	C, C++, Python, Java, Javascript
Chromium Development	Blink, V8, DevTools Framework, Graphics Stack
Binary Exploitation	Familiar with Linux binary exploitation techniques and defenses.
Web Security	Familiar with web attack techniques and defenses.
Machine Learning	pandas, Scikit-learn, SciPy, MALLET

Honors & Awards

- Nankivell Engineering Scholarship
- Fred M. Roddy Merit Scholarship
- Member of Tau Beta Pi Engineering Honors Society (top 7% in undergraduate engineering class)
- Georgia Tech Presidential Fellowship

Selected Publications

Understanding and Mitigating Remote Code Execution Vulnerabilities in Cross-Platform Ecosystem

CCS'22

Feng Xiao, Zheng Yang, **Joey Allen**, Guangliang Yang, Grant Williams, Wenke Lee

- Conducted a systematic study on XRCE attacks and their diverse attack behaviors.
- Design and implemented a novel XRCE defense system, XGuard.

Mnemosyne: An Effective and Efficient Postmortem Watering Hole Attack Investigation System

CCS'20

Joey Allen, Zheng Yang, Matthew Landen, Raghav Bhat, Harsh Grover, Andrew Chang, Yang Ji, Roberto Perdisci, Wenke Lee

- Proposed Mnemosyne a forensic analysis system for investigating watering hole attacks.
- Mnemosyne was able to detect the victims of a watering hole attack, while also reducing the analysis by 98.17% on average.

Improving Accuracy of Android Malware Detection with Lightweight Contextual Awareness

ACSAC'18

Joey Allen, Matthew Landen, Sanya Chaba, Yang Ji, Simon Chung, Wenke Lee

- Proposed PikaDroid, a state-of-the-art Android malware detection system.
- PikaDroid detected Android malware samples with an f-score of 97.41% and a false-positive rate of 0.96%.
- PikaDroid required less than one minute on average to determine if an application is benign or malicious.
- ACM Artifact Evaluated Badge

Enabling Refinable Cross-Host Attack Investigation with Efficient Data Flow Tagging and Tracking

Usenix Security'18

Yang Ji, Sangho Lee, Mattia Fazzini, **Joey Allen**, Evan Downing, Alessandro Orso, Taesoo Kim, and Wenke Lee

- Proposed RTAG, an efficient data flow tagging and tracking mechanism that enables practical cross-host attack investigations.
- RTAG reduced the memory consumption of DIFT-based analysis by up to 90% and decreases the overall analysis time by 60% – 90% compared with prior approaches.