Joey **Allen**

Ph.D. Student · Computer Science · Information security

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

Research Interests

PhD student at Georgia Tech's Institute for Information Security & Privacy (IISP). Seven years of experience in security research spanning web security, system security, and mobile security research. My current research interests are related to web security, vulnerability analysis, and forensic investigations.

Experience

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 — *Virtual*

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*

- Developing 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 1.5+ years of experience with customizing Blink, V8 and Chromium.

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

Georgia Tech — *April 2021 - Present*

- Developed a novel technique for detecting cross-site scripting-based remote code execution (XRCE) in Electron Apps.
- Implemented a monitoring framework in Electron, V8, and Blink to monitor the invocation of sensitive JS APIs and to complete call stack inspection during runtime.
- This work is under submission at Usenix'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 amount of audit logs required to manually 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 that 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, 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 relies on static taint tracking to identify sensitive information leaks in Android applications. Next, it relies on state-of-the-art NLP techniques to identify when a information leak is inconsistent with the app's intent, specified in it's textual description.
- pDroid correctly classified 91.4% of Android malware with a false false-positive rate of 4.9%.
- This work was used as a Master's thesis.

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
Static Analysis Frameworks	WALA, Soot, LLVM
Dynamic Analysis and Instrusion Monitoring	Linux Audit System (LAS), Pin (DBI), Neo4j, Record & Replay
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
  - Requirement: Top 7% in undergraduate engineering class.
- Georgia Tech Presidential Fellowship

Selected Publications

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.