Kevin Liao

kevinliao@asu.edu ◇ kevinliao.me

EDUCATION

B.S. Computer Science *(expected) May 2017*
Arizona State University Tempe, AZ
Thesis: Next Generation Black-Box Vulnerability Analysis Framework (in progress)
Committee: Adam Doupé (Chair), Gail-Joon Ahn, Ziming Zhao
GPA: 4.00/4.00

RESEARCH INTERESTS

- Computer & web security
- Applied cryptography
- Programming languages
- Cryptographic currencies

PUBLICATIONS

Peer-Reviewed Conference Proceedings

[C1] **Kevin Liao**, Ziming Zhao, Adam Doupé, and Gail-Joon Ahn. "Behind Closed Doors: Measurement and Analysis of CryptoLocker Ransoms in Bitcoin". In: *Proceedings of the Symposium on Electronic Crime Research (eCrime)*. June 2016.

Works In Submission

[S1] **Kevin Liao**, Tejas Khairnar, and Adam Doupé. *Toward Inductive Reverse Engineering of Web Applications. (In Submission)*.

Tech Reports

[TR1] **Kevin Liao** and Jonathan Katz. *Incentivizing Double Spend Collusion in Bitcoin. Tech report.*

Book Chapters

[BC1] **Kevin Liao**, Ziming Zhao, Adam Doupé, and Gail-Joon Ahn. "Ransomware and Cryptocurrency: Partners in Crime". In: *Cybercrime Through an Interdisciplinary Lens*. Ed. by Thomas J. Holt. Advances in Intelligent Systems and Computing. Routledge, 2016.

Posters

[P1] **Kevin Liao**, Tejas Khairnar, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn. *Next Generation Black-Box Vulnerability Analysis Framework. Workshop on Information Assurance Research and Education, ASU*. October 2016.

[P2] Anupam Panwar, Ajay Modi, Jangwon Yie, **Kevin Liao**, Sajid Anwar, Wonkyu Han, Daniel Martin, Kyungyong Han, Ziming Zhao, Adam Doupé, and Gail-Joon Ahn. *Threat Intelligence Analytics (TIA): Assembling the Jigsaw Puzzles of Cybercrimes. Workshop on Information Assurance Research and Education, ASU*. November 2015.

RESEARCH EXPERIENCE

Undergraduate Research Assistant *Jun 2016 – Present*
Maryland Cybersecurity Center, University of Maryland College Park, MD
Advisor: Jonathan Katz

- Project:
  - We propose and formalize the *whale attack*, in which a minority attacker increases her chances of double-spending by incentivizing miners to subvert the consensus protocol and to collude via *whale transactions*, or transactions carrying anomalously large fees. We analyze the expected cost to carry out the attack, and simulate the attack under realistic system parameters. Our results show that double-spend attacks, conventionally thought to be impractical for minority attackers, can actually be financially feasible and worthwhile under the whale attack.
    Publications: [TR1]
- Sponsors
  - National Science Foundation

Undergraduate Research Assistant *Mar 2015 – Present*
Security Engineering for Future Computing Lab, Arizona State University Tempe, AZ
Advisors: Gail-Joon Ahn, Adam Doupé

- Projects:
  - We introduce a novel application of inductive programming, which we call *inductive reverse engineering (IRE)*. The goal of IRE is to automatically reverse engineer an abstraction of the web application's code in a completely black-box manner. We build this approach using recent advances in inductive programming, and we solve several technical challenges in order to scale the inductive programming techniques to realistic-sized web applications. We target the initial version of our IRE tool to a subset of web applications: those that do not store state and those that do not have loops. We introduce an evaluation methodology for web application cloning techniques and evaluate our approach on several real-world web applications.
    Publications: [S1] [P1]
  - We perform a measurement analysis of CryptoLocker, a family of ransomware that encrypts a victim's files until a ransom is paid, within the Bitcoin ecosystem from September 5, 2013 through January 31, 2014. Using information collected from online fora, such as reddit and BitcoinTalk, as an initial starting point, we generate a cluster of 968 Bitcoin addresses belonging to CryptoLocker. We provide a lower bound for CryptoLocker's economy in Bitcoin and identify 795 ransom payments totalling 1,128.40 BTC ($310,472.38), but show that the proceeds could have been worth upwards of $1.1 million at peak valuation. By analyzing ransom payment timestamps both longitudinally across CryptoLocker's operating period and transversely across times of day, we detect changes in distributions and form conjectures on CryptoLocker that corroborate information from previous efforts.
    Publications: [C1] [BC1] [P2]
- Sponsors
  - Fulton Undergraduate Research Initiative

TEACHING EXPERIENCE

Mentor, Course Designer *Jul 2016 – Present*
First Gen Scientists Tempe, AZ

- Developing curriculum and mentoring for introductory computer science course: Fall 2016.

Undergraduate Teaching Assistant *Aug 2014 – Present*
Arizona State University Tempe, AZ

- CSE 240 Introduction to Programming Languages with Dr. Yinong Chen: Fall 2016.
- CSE 110 Introduction to Programming with Dr. Yoshi Kobayashi: Fall 2014.