Amin Kharraz | Curriculum Vitae
458 Coordinated Science Laboratory
1308 W Main Street, Urbana, IL 61801-2307
(339) 224 3351 • kharraz@illinois.edu • kharraz.org

Research Interests

My research focuses on building systems to facilitate a data-driven approach to security. The primary goal of my program is to apply this methodology to rigorously analyze the behavior of online attacks and facilitate developing platforms to discover and mitigate these attacks in a scalable and reliable manner. The problems that I tackle often involve the intersection of society, technology, and security. My research seeks to create solutions to evaluate the security and privacy implications of emerging technologies, identify associated threats, and improve the agility of defenders in responding to those threats in a timely fashion. My work has helped to develop techniques to protect users from important security problems, including ransomware and online scams, and guide the design of new defense systems.

Education

Northeastern University **Boston, MA**
Ph.D. in Information Assurance – Systems Security *2012–2017*
Dissertation: Techniques and Solutions for Addressing Ransomware Attacks
Advisor: Prof. Engin Kirda

Sharif University of Technology **Tehran, Iran**
Master of Science – Telecommunications *2008–2010*
Thesis: Quality of Service Multicast Routing in Wireless Mesh Networks
Advisor: Prof. Hamid Sarbazi-azad

Shiraz University **Shiraz, Iran**
Bachelor of Science – Computer Engineering, *2001–2006*

Experience Highlights

University of Illinois at Urbana–Champaign **Urbana, IL**
Post-Doc Research Associate *2018–Present*
– Propose and lead research projects toward building tools and techniques to systematically analyze emerging web threats and evaluate the security and privacy of web technologies.

– Performed a systematic study on in-browser cryptojacking attacks by developing a machine learning tool, called Outguard, to automatically detect the incident at scale.

Northeastern University **Boston, MA**
Research Associate *2012–2017*
– Developed Unveil, a dynamic analysis platform to automatically detect and cluster more than 250 K ransomware samples in 28 families by analyzing 2 Millions unlabeled binaries.

– Performed an analysis of web-based social engineering attacks by designing Surveylance, an automated approach to analyze the underlying ecosystem of today's online scams. Surveylance relies on an instrumented version of Chromium to collect web content and a machine learning model (i.e., Random Forest) to detect pages that led victims to malware, Potentially Unwanted Programs (PUPs), scams, and affiliated programs.
– Developed a module for Java bytecode space/time analysis to identify potentially vulnerable program paths. The module includes a black-box mutational fuzzer and a model constructor to characterize the Java method execution and identify potentially costly-but-benign paths which can be trigged by an attacker.
– Designed and implemented USBeSafe, an anomaly detection module, to protect users from rogue transient

devices.
– Modified Chromium code base (C++) and built an instrumented browser for automatic detection of web malware and malicious browser extensions.
– Designed a large-scale and distributed crawling infrastructure to collect and identify malicious QR codes on the web.

iDefense – Verisign Labs **Reston, VA**
Graduate Research Intern *Summer 2015*
– Designed and implemented an early warning system, called RegTracker, using classification techniques to automatically detect newly-registered malware domains.

Infoamn Consulting Company **Tehran, Iran**
Senior Engineer *2009 – 2011*
– Directed a team of 6 information security specialists on multiple projects with authority to perform threat analysis, vulnerability detection, incident response, IT audit, and security compliance.

Conferences

Amin Kharraz, Zane Ma, Paul Murley, Charles Lever, Joshua Mason, Andrew Miller, Nikita Borisov, Manos Antonakakis and Michael Bailey, Outguard: Detecting In-Browser Covert Cryptocurrency Mining in the Wild, The Web Conference (WWW), May 2019. 1,247 submissions, accepted 225 (18.0%)
Best Paper Award
Amin Kharraz, Brandon L. Daley, Graham Z. Baker, William Robertson, Engin Kirda, USBeSafe: An End-Point Solution to Protect Against USB-Based Attacks, The 22nd International Symposium on Research on Attacks, Intrusions and Defenses (RAID'19). Beijing, China, September 2019. 166 submissions, accepted 37 (22.3%)
Amin Kharraz, William Robertson, Engin Kirda, Surveylance: Automatically Detecting Online Survey Scams, 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, California, May 2018. 549 submissions, accepted 63 (11.5%)
Amin Kharraz, Engin Kirda, Redemption: Real-time Protection Against Ransomware at End-Hosts, The 20th International Symposium on Research on Attacks, Intrusions and Defenses (RAID 2017). Atlanta, Georgia, September 2017. 105 submissions, accepted 21 (20.0%)
Amin Kharraz, Sajjad Arshad, Collin Muliner, William Robertson, Engin Kirda, UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware, USENIX 2016. Austin, Texas, August 2016. 463 submissions, accepted 72 (15.5%)
Sajjad Arshad, **Amin Kharraz**, William Robertson, Identifying Extension-based Ad Injection via Fine-grained Web Content Provenance, The 19th International Symposium on Research on Attacks, Intrusions and Defenses (RAID 2016). Paris, France, September 2016. 85 submissions, accepted 21 (24.7%)
Sajjad Arshad, **Amin Kharraz**, William Robertson, Include Me Out: In-Browser Detection of Malicious Third-Party Content Inclusions, The 20th International Conference on Financial Cryptography and Data Security (FC). Barbados, 2016. 139 submissions, accepted 36 (25.9%)
Amin Kharraz, William Robertson, Davide Balzarotti, Leyla Bilge, Engin Kirda, Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks, The 12th International Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA). Milan, Italy, July 2015. 75 submissions, accepted 17 (22.7%)
Amin Kharraz, Engin Kirda, William Robertson, Davide Balzarotti, Aurelien Francillon, Optical Delusions: A Study of Malicious QR Codes in the Wild, Proceedings of 43th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Atlanta, GA USA, June 2014. 139 submissions, accepted 36 (31.0%)

Journals and Book Chapters

Amin Kharraz, William Robertson, Engin Kirda, Protecting Against Ransomware: A New Line of Research or Restating Classic Ideas?, IEEE Security and Privacy Magazine, June 2018.

Amin Kharraz, Engin Kirda, Root Cause Analysis for Cybersecurity, Big Data Analytics in Cybersecurity, Taylor & Francis, 2016.
Amin Kharraz, Hamid Sarbazi-Azad, Albert Zomaya, On-Demand Multicast Routing Protocol with Efficient Route Discovery, Elsevier Journal of Network and Computer Application, 2012.

Awards

The Web Conference 2019: The best paper award

IEEE Symposium on Security and Privacy 2018: Student PC Award

RSA Conference 2017: RSA Conference Security Scholars 2017

Scientific Community Service

Registration Chair: WiSec 2019, Miami, Florida

Program Committee: AsiaCCS 2020, Taipe, Taiwan

Program Committee: AsiaCCS 2019, Aukland, New Zealand

Program Committee: RAID 2018, Crete, Greece

Shadow Program Committee: IEEE Security and Privacy 2018, San Francisco, CA

Shadow Program Committee: IEEE Security and Privacy 2017, San Jose, CA

External Reviewer: USENIX'18, NDSS'18, NDSS'17, DSN'16, USENIX'16, NDSS'16, USENIX'15

Teaching Services

Guest Lecturer at Boston University: Vulnerability, Malware, and Defensive Systems (EC700)

Co-Teach at Northeastern University: Introduction to Software Security (ECE-5641)

Co-Teach at Northeastern University: Software Vulnerabilities and Security (CS-5770)

Invited Talks

Northeastern University, September 2019, Boston, MA
MidWest Security Workshop, April 2019, Chicago, IL
RSA Conference, February 2017, San Francisco, CA
Federal Trade Commission (FTC), January 2017, Washington D.C.
Verisign Inc, August 2015, Reston, VA
Open Web Application Security Project (OWASP) 2015, Boston, MA
Conference talks are not included.

Research on Media

BankInfo Security: Better Ransomware Detection: Follow the Shouting, August 2016

MIT Tech Review: Two Ways to Stop Ransomware in Its Tracks, July 2016

The Conversations: It's easier to defend against ransomware than you might think, May 2016

Associate Press: It's easier to defend against ransomware than you might think, May 2016 (Republished)

ComputerWorldUK: Ransom malware could be beaten with simple file-system security, study concludes, July 2015

Collaborators

Michael Bailey (UIUC), Nikita Borisov (UIUC), Andrew Miller (UIUC), Engin Kirda (Northeastern University), William Robertson (Northeastern University), Sajjad Arshad (Google), Leila Bilge (Symantec), Davide Balzarotti (Eurecom), Hamid Sarbazi-azad (Sharif University), Albert Zomaya (University of Sydney), Zane Ma (UIUC), Paul Murley (UIUC), Collin Muliner (Northeastern University), Manos Antonakakis (Georgia Tech), Charles Lever (Georgia Tech), Aurelien Francillon (Eurecom), Brandon Daley (MIT Lincoln Lab), Graham Z. Baker (MIT Lincoln Lab)

References

Engin Kirda, Ph.D.
Professor
Northeastern University
618 Khoury College of Computer Science
360 Huntington Ave Boston
Boston, MA 02115
Email: ek@ccs.neu.edu
Phone: +1 (857) 244-0999

Michael Donald Bailey, Ph.D.
Associate Professor
University of Illinois at Urbana-Champaign
Dep. of Electrical and Computer Engineering
458 Coordinated Science Laboratory
1308 W Main Street
Urbana, IL 61801
E-mail: mdbailey@illinois.edu
Phone: +1 (217) 244-8830

William Robertson, Ph.D.
Associate Professor
Northeastern University
617 Khoury College of Computer Science
360 Huntington Ave
Boston, MA 02115
Email: wkr@ccs.neu.edu
Phone: +1 (510) 423-0673

Davide Balzarotti, Ph.D.
Professor
EURECOM
Campus SophiaTech
450 Route des Chappes
06410 Biot FRANCE
Email: davide.balzarotti@eurecom.fr
Phone: +33 4 9300 8156

Manuel Egele, Ph.D.
Assistant Professor
Boston University
337 Photonics Building
8 St. Mary's Street
Boston, MA 02215
Email: megele@bu.edu
Phone: +1 (617) 353-7338