EDWARD XUEJUN WU

Email: edwardwu@cs.washington.edu Homepage: https://www.edwardxwu.com

SUMMARY OF QUALIFICATIONS

- 5 years of academic research experience in cybersecurity, including malware reversing, application security, network security, mobile security and privacy, and applied machine learning
- Experience of devise, implement and evaluate new defense and security tools:
  - **Program analysis**: static and dynamic program analysis, fuzzing, symbolic execution, sensitive information tracking, memory access violation detection, and program instrumentation
  - **Behavioral modeling**: model application's runtime behaviors based on network traffic, information flow and API calls
  - **Automated reasoning**: automated network protocol reversing, temporal security policy enforcement and machine learning based automated malware detection
- Familiar with system and network stacks, computer architecture, and Android internals
- Proficiency with IDA Pro, QEMU, Pin, LLVM, z3, Soot, Wala, x86 ASM, ARM, Dalvik
- Programming experience in C, C++, Java, Python, OCaml, PHP, Ruby on Rails, Scheme, bash
- Involved in 7 CVE vulnerability disclosures

EDUCATION

University of Washington, Seattle Sep. 2012 - Present
PhD student in Computer Science and Engineering

University of California, Berkeley Aug. 2008 - May 2012
Bachelor of Science in Electrical Engineering and Computer Science
Certificate in Engineering Leadership from Center for Entrepreneurship & Technology

WORK EXPERIENCE

Intern, Intel Labs Jun. 2014 - Sep. 2014
Anti-Malware Intelligence, Security and Privacy Research

- Built a static instrumentation framework for Dalvik bytecode that enables arbitrary code injection and modification to existing pre-compiled Android applications
- Developed a portable and runtime environment agnostic system for recording detailed Android apps' runtime behaviors in both Dalvik and native code components
- Prototyped an automated black-box GUI exploration testbed and an enterprise data protection tool for arbitrary Android applications

Intern, Qualcomm Research Jun. 2012 - Sep. 2012
Qualcomm Product Security Initiative

- Implemented a fully working runtime memory monitoring tool for Qualcomm's proprietary Hexagon ISA and real time OS based on Address Sanitizer (LLVM)
- Enabled the capability to detect stack, heap, and global out-of-bound memory accesses and use-after-free bugs in code running on Qualcomm's basebands, with virtually no false positive or negatives

RESEARCH EXPERIENCE

Graduate Student Researcher, University of Washington

Realtime Malware Detection via Online Behavioral Classification Sep. 2014 - Present

- Explored how to build an online classifier using offline training and the resulting challenge of mislabeled data on machine learning algorithms

Fine-grained Private Information Protection, Triceratops Mar. 2013 - Present

- Built a static instrumentation based taint tracking tool that can track how sensitive information is used by an application on any Android OS with no modification.

Secure Android Application Development, SPARTA Sep. 2012 - Jan. 2014

- Investigated ways in which a developer can make verifiable security guarantees to the end user during the development process by using additional source code annotation.

Research Assistant, PI: Prof. Dawn Song, UC Berkeley

Static Android App Behavior Extraction Framework May 2011 - May 2012

- Built the points-to analysis and string resolution modules for the framework
- Evaluated the effectiveness of the framework on benign and malicious Android apps

Distributed Large-scale Android Applications Similarity Analysis Aug 2011 - Nov. 2011

- Participated in building a machine learning based tool that clusters unknown Android apps with known malicious samples, and devised new feature extraction approaches.
- Scaled existing C++ implementation to hundreds of nodes by porting and optimizing them to run on Amazon EC2

Model Guided Concolic Execution and Model Inference Platform, Mace Oct. 2010 - Feb. 2011

- Modified the dynamic symbolic execution engine to support network-interfaced applications
- Scaled up and fully automated the dynamic symbolic execution tool to a on-demand cloud analysis service on over 60 nodes, with dynamic task allocation

IDA Pro Plugin for Execution Trace Overlay Jun. 2010 - Aug. 2010

- Improved performance and memory footprint by at least 1000x using pre-computation, caching, and data structure optimizations.

Automatic Vulnerability Discovery by Binary Program Analysis, BitBlaze Sep. 2009 - June. 2010

- Performed reverse engineering and crash analysis on closed-source applications, malware samples, and Windows kernel
- Used advanced dynamic symbolic execution engine to find memory access crashes in COTS programs
- Generated a proof-of-concept 0-day exploit in Zeus trojan

Publications and Talks

Triceratops: Privacy-protecting Mobile Apps
Edward X. Wu, Sai Zhang, Ravi Bhoraskar, Rene Just, Mike Ernst. HCSS '14 (invited talk)

Contextual Policy Enforcement in Android Applications with Permission Event Graph
Kevin Zhijie Chen, Noah Johnson, Vijay DSilva, Shuaifu Dai, Kyle MacNamara, Tom Magrino, Edward XueJun Wu, Martin Rinard and Dawn Song. NDSS '13

Juxtapp: A Scalable System for Detecting Code Reuse Among Android Applications
Steve Hanna, Ling Huang, Edward Wu, Charles Chen, Saung Li, and Dawn Song. DIMVA '12

FreeMarket: Shopping for free in Android applications
Daniel Reynaud, Richard Shin, Tom Magrino, Edward Wu, and Dawn Song. NDSS '12 (short paper)

MACE: Model-inference-Assisted Concolic Exploration for Protocol and Vulnerability Discovery
Chia Yuan Cho, Domagoj Babic, Pongsin Poosankam, Kevin Zhijie Chen, Edward XueJun Wu, and Dawn Song. USENIX Security '11

Teaching Assistance Experience

Introduction to Database Systems, *Hal Perkins*	Winter 2014
Advanced Computer Architecture, *Susan Eggers*	Spring 2014
Systems Programming, *John Zahorjan*	Autumn 2014
Systems Programming, *Xi Wang*	Winter 2015