Fengguo (Hugo) Wei

Contact Information	225 ENB University of South Florida Tampa, FL, USA 33613	Email: fwei@mail.usf.edu http://www.fengguow.com/

Research Interests

My research focuses on developing program analysis technologies to address security related issues, particularly in the areas of mobile systems. My recent research efforts can be categorized as follows:

- **Applying static methods for Android security analyzing:** The focus is on detecting security issues on Android application. A large portion of those issues can be resolved by addressing one core problem – capturing semantic behaviors of the app such as object points-to and control-/data-flow information. Thus, we designed an approach to conducting static analysis for vetting Android apps, and built a generic framework, called Amandroid, which does inter-component, flow-/context-sensitive data flow analysis. Based on Amandroid, we applied certain security applications on popular Android apps, and the results shows that the tool is capable of finding real security issues and efficient enough in terms of analysis time.

  Amandroid is currently merged into a new open-source project – Argus-SAF (Argus static analysis framework),

  Website: http://pag.arguslab.org/argus-saf

- **Android malware categorization and landscape study:** By utilizing the tool chains I built during last couple years, I perform a large-scale landscape study to revealing the new threats and evolving trends of Android malware. This work presents a detailed picture of current malware behaviors and their evolving trend, which provides the Android malware research community a better ground truth dataset for evaluating their approach.

  Website: http://amd.arguslab.org/

Research Impact

The Amandroid project provides a comprehensive static analysis framework for vetting Android applications as well as finding framework vulnerabilities. Amandroid is implemented from scratch and being carefully designed to fit into the analysis for modern smartphone architecture. This work advanced state of the art in providing a more precise environment model for Android components and tracking data flow across different components.

- The Amandroid is open-sourced at https://github.com/arguslab/Argus-SAF. Researchers from different institutes and research labs have provided valuable plugins into the code base.
- The Amandroid tool has been downloaded over five thousand times as of December 2016 and become foundation of many research projects (cited over 160 times as of January 2017).

The AMD is a well-labeled and well-studied Android malware dataset containing 24,650 samples, categorized in 135 varieties among 71 families ranging from 2010 to 2016. For each variety of this dataset we conduct a comprehensive study to profile their behaviors and evolution trends. We details document the process of creating this dataset to enable other researchers to replicate the process.

- The AMD information is available at `http://amd.arguslab.org/`, and shared with community upon request. It have been shared with 33 research institute world-wide.

Education

University of South Florida, Tampa, FL, USA

Ph.D., Computer Science, August 2015 – Present

- Advisor: Dr. Xinming (Simon) Ou

Kansas State University, Manhattan, KS, USA

Ph.D., Computer Science, August 2012 – August 2015

- Advisor: Dr. Xinming (Simon) Ou

Chinese People's Public Security University, Beijing, China

B.S., Computer Science, September 2008 – June 2012

- *Summa Cum Laude*

Academic Experience

University of South Florida, Tampa, FL, USA

Graduate Research Assistant, August 2015 – May 2017

- Conducted Ph.D. research in the area of malware analysis, smartphone security and program analysis.

Kansas State University, Manhattan, KS, USA

Graduate Research Assistant, August 2012 – August 2015

- Conducted Ph.D. research in the area of smartphone security and program analysis.

Work Experience

Coverity R&D Team, Synopsys Inc, San Francisco, CA, USA

Research & Development Intern, May 2017 – August 2017
Supervisor: Aaron Hurst, Manager: Timothy Alper

I am working in the Software Integrity Group (SIG) R&D team to design WEB&Android&IOS security checkers for Coverity static analysis tool.

B2B Lab, Samsung Research America, Mountain View, CA, USA

Research & Development Intern, January 2015 – July 2015
Supervisor: Wu Zhou, Manager: Michael Grace

Our team is responsible of providing security solutions for Samsung's internal products. My work includes:

- Perform static analysis and manual analysis for Samsung KNOX Trust-zone applications, and Samsung Pay backend framework codes.
- Designed an integrated android application reverse engineering and code analysis tool called Argus-CIT (Argus Code Inspect Tool), and implemented as a plugin for IntelliJ.

China Academy of Launch Vehicle Technology, Beijing, China

Research Intern, June 2011 – August 2011
Supervisor: Shuliang Ren

Central Control with MES System Integration Development.

- Participated in the control system interface development of external system which including the enterprise service bus (ESB), Web service and XML.

Open-source Products

I strongly believe in the philosophy that freedom is power.

- **Argus-SAF:** Argus-SAF is a static analysis framework for Android applications and libraries. It integrated Jawa and Amandroid, and have the capability to perform comprehensive, efficient and highly precise Inter-component Data Flow Analysis.

  Website: https://github.com/arguslab/Argus-SAF

- **Jawa-Compiler:** Jawa is an intemediate representation (IR) language for Java-like bytecode (e.g., Java bytecode, Dalvik bytecode). Jawa compiler provides compilation support for Jawa language. It provides lexer and parser to parse jawa code, and code generator to generate java bytecode from jawa code. This gives Jawa language the ability to work with java program and perform cross compilation.

  Website: https://github.com/arguslab/jawa-compiler

- **Jawa2Java:** Jawa2Java provides user the ability to translate Jawa code to Java code, which helps reverse engineering Android application much easier. Jawa2Java addressed the challenges of recovering control logics and exception handling, and we plan to further optimize the translation to make it even more readable.

  Website: https://github.com/arguslab/jawa2java

- **Argus-CIT-Intellij:** Argus Code Inspection Tool is an Intellij plugin, which provides an IDE for editing Jawa language. It also helps user to perform analysis and reverse engineering for Android applications.

  Website: https://github.com/arguslab/argus-cit-intellij

Publications

Papers

1. **Fengguo Wei**, Yuping Li, Sankardas Roy, Xinming Ou, and Wu Zhou. Deep Ground Truth Analysis of Current Android Malware. In the 14th Conference on Detection of Intrusions and Malware & Vulnerability Assessment. (DIMVA 2017)
2. **Fengguo Wei**, Sankardas Roy, Xinming Ou, Robby. Amandroid: A Precise and General Inter-component Data Flow Analysis Framework for Security Vetting of Android Apps. Technical report 2017-4, University of South Florida, Computer Science and Engineering Department. May, 2017. (A significantly enhanced version of our Amandroid CCS 2014.)
3. **Fengguo Wei**, Yuping Li, Sankardas Roy, Xinming Ou, and Wu Zhou. Deep Ground Truth Analysis of Current Android Malware. Technical report 2017-2, Argus Cybersecurity Lab, University of South Florida, Computer Science and Engineering Department. February, 2017.
4. **Fengguo Wei**, Sankardas Roy, Xinming Ou, Robby. Amandroid: A Precise and General Inter-component Data Flow Analysis Framework for Security Vetting of Android Apps. In the 21st ACM Conference on Computer and Communications Security. (CCS 2014)

Posters

1. **Fengguo Wei**, Sankardas Roy, Xinming Ou, Robby. A Precise and General Inter-component Data Flow Analysis Framework for Security Vetting of Android Apps. In the 35th IEEE Symposium on Security and Privacy. 2014. (S&P 2014)

Professional Activities

Reviewer:

- 33rd Annual Computer Security Applications Conference (ACSAC 2017)
- 6th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM 2016)
- 32nd Annual Computer Security Applications Conference (ACSAC 2016)
- 23rd ACM Conference on Computer and Communications Security (CCS 2016)
- 11th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2016)
- 6th ACM Conference on Data and Application Security and Privacy (CODASPY 2016)
- 24th USENIX Security Symposium (USENIX 2015)
- 10th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2015)
- The 9th International Conference on Network and System Security (NSS 2015)
- 30th Annual Computer Security Applications Conference (ACSAC 2014)
- 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2014)
- 12th International Conference on Privacy, Security and Trust (PST 2014)
- 9th International Conference on Risks and Security of Internet and Systems (CRiSIS 2014)
- 10th International Conference on Security and Privacy in Communication Networks (SecureComm 2014)

Technical Skills

Programming:	Scala, Java, C/C++, Python, ML, DataLog, LaTeX
Programming IDE:	Eclipse, Intellij
Operating Systems:	Mac, Android, Linux, Unix
Version Control Tools:	Git, SVN

Awards

- PhD Fellowship, Kansas State University, 2012 - 2014. ($8000 per year)
- National grants, China, 2011.

Professional Affiliations

- The Honor Society of Phi Kappa Phi