Yugeng LIU

Email: yugengliu@jhu.edu Website: https://www.liuyugeng.com Tel: +1-4439415137
Malone Hall 360, 3400 N Charles St Johns Hopkins University, Baltimore, MD 21218

EDUCATION

Shanghai Jiao Tong University (SJTU), Shanghai, China *Sep 2014 - July 2018*

Bachelor of Engineering in Computer Science and Technology

Major GPA: 3.44/4.0

Core Courses: Computer Network, Artificial Intelligence, Electronic Business, Computer Security and Cryptography, Computer Graphics, Compiler Principles, Software Engineering, Data Structure, Thinking and Approach of Programming

PUBLICATION

- Zhushou Tang, Minhui Xue, Guozhu Meng, Chengguo Ying, **Yugeng Liu**, Jianan He, Haojin Zhu, Yang Liu: "**Securing Android Applications via Edge Assistant Third-Party Library Detection**." Accepted by *Computers & Security, 2019, 257-272*
- Wei Zhang*, Yan Meng*, **Yugeng Liu**, Xiaokuan Zhang, Yinqian Zhang, Haojin Zhu: "**HoMonit: Monitoring SmartHome Apps from Encrypted Traffic."** Accepted by *ACM SIGSAC Conference on Computer and Communications Security (CCS), 2018, 1074-1088*

RESEARCH EXPERIENCE

Third-party library (TPL) and Its Privacy Leakage Detection in Android | Research Assistant (RA) *Mar 2018 - June 2018*

Advisor: Prof. ***Haojin Zhu,*** Network Security and Privacy Protection (**NSEC**) Lab, SJTU

- Designed and implemented a system to set up TPLs' standard data sets of 164 TPLs with 2,066 versions for 4,658 Android apps and developed the detection of a given app for its TPLs' integrity checking and privacy leakage
- Established a *meet-in-the-middle* tool of the RSA encrypted traffic for Android system through the opensource code in PrivacyGuard to detect the traffic from the App to TPL without leaking data to any other App or any other TPL
- Defined the concept of privacy leakage based on EU General Data Protection Regulation (GDPR), systematizing and standardizing various definitions of privacy leakage and authorizing the detection result
- Recapitulated total types of privacy data leaked to TPLs on each App and contacted app development companies to prevent numerous potential leakage

Leverage Side-Channel Capabilities to Monitor SmartApps from Encrypted Traffic | RA *Sep 2016 - Sep 2017*

Advisor: Prof. ***Haojin Zhu,*** Network Security and Privacy Protection (**NSEC**) Lab, SJTU

- Designed and implemented a system to detect security flaws which allows malicious smart home apps (or SmartApps) to possess more privileges and eavesdrop or spoof events in the IoT (or SmartThings) platform
- Extracted text and symbol inference of a given SmartApp based on Natural Language Processing (NLP) from the user interface of the SmartThings mobile app to build control logic and harnessed the result to determine whether the SmartApp was malicious
- Developed *over-privileged and event-spoofing* versions of the original benign opensource SmartApps to prove the correctness of the system and published paper in *ACM CCS 2018*

WORK EXPERIENCE

Shanghai Benzhong Information Technology Co., Ltd., China | *Intern Android Security Researcher* *Nov. 2017 - Jan 2018*

- Designed and implement a standard corpus containing 800 TPLs with 9,623 versions from 9,049,323 apps to detect TPLs of a given app handled (*shrunk, optimized or obfuscated*) by ProGuard, enhancing the accuracy of detection through big data
- Developed string hash algorithm to probe the qualified name, named *"Package Stem (PS)" probing*, to identify other versions of the TPL and related hash value, successfully creating a one-to-one mapping between a specific TPL version and a hash value
- Decoupled a given app through the *"PS" probing* and then used the stable feature generated by the specific Android SDK APIs, without being affected by the usage of ProGuard, to identify TPLs of the app in detection
- Visualized detection results by using Visio, NetworkX, and Python for the paper and published the paper in *Computers & Security 2019*

AWARDS AND HONORS

- Honorable Award of American Undergraduate Mathematical Contest in Modeling *Feb 2017*
- Academic Excellence Scholarship of Shanghai Jiao Tong University *Sep 2014 - June 2015*
- Second Award of Ericsson Hackathon *Apr 2015*

SKILLS AND OTHERS

Programming Language: Python, C, C++, Java, Smali, MATLAB, Swift, Objective-C, JavaScript

Security Skills: Ollydbg, IDA, PWN, Misc, macOS and iOS Reverse Engineering

Interests: Basketball (player and assistant coach), Electronic Keyboard (Amateur Level 10)