XIAOYONG ZHOU

959 Stewart Dr. #1034, Sunnyvale CA 94085
Tel: (812) 272-0568 E-mail: zhou.xiaoyong@gmail.com
http://xiaoyongzhou.weebly.com/ @xzhou

OBJECTIVE

Experienced security researcher with extensive backgrounds in security and privacy, vulnerability analysis and applied cryptography, especially in **mobile security** and **mobile payment** looking for security engineer or research position.

EDUCATION

School of Informatics and Computing (SoIC), Indiana University, Bloomington, IN — Sept 2008 - May 2014
PhD, Oct 2014, majored in Security Informatics

School of Computing, National University of Defense Technology, Changsha, China — Sept 2004 - May 2007
Master of Engineering, Computer Science, majored in Networking Security

Software College, Hunan University, Changsha, China — Sept 2000 - May 2004
Bachelor of Engineering, Computer Science, majored in Computer Science

WORK EXPERIENCE

Samsung Research America, Mountain View, CA — Aug 2014 - Now
Senior Security Research Engineer

- **Samsung Knox**. Samsung Knox is a secure application container for enterprise applications. It offers multiple levels of security (hardware TrustZone, SELinux in kernel and application container) to provide an secure and isolated execution environment to protect sensitive enterprise apps and data. My routine job involves designing and reviewing security related features especially those related to Android Framework.
- **Samsung Pay**. Architected Samsung Pay security framework from scratch. The payment system support both MST and NFC payment. I designed few security critical components such as wearable payment protocol and secure communication channel between TrustZone App and Token Service Provider. Reviewed the payment framework and identified dozens of security vulnerabilities such as crypto misuses. Using static analysis tools (Fortify and Veracode) to find common vulnerabilities in payment system. **The payment system is now widely used worldwide**.
- **Security Research**. Identified Hanging Attributes vulnerabilities that allows malicious app to masquerade critical system app or content provider such as Keyguard(password bypass), Gmail Setting (password leaking) et. al. (Published at CCS 2015). Discovered few vulnerabilities in Android application installation transaction that allows malicious app to install app without user consent.
- **Vulnerability Incidence Response**. Analyzed few zero day vulnerabilities as Stagefright, Qualcomm image verification vulnerability, Keyguard bypass et al. Awarded for keeping up with the security reviews and vulnerability response.

SOIC, Indiana University, Bloomington, IN — Jan 2012 - Oct 2014
Research Assistant

- **Research on cloud messaging for mobile devices.** In this project, we identified vulnerabilities of Google Cloud Messaging, Amazon Device Messaging and Urban Airship that enable a malicious user to remotely lock, wipe a phone as well as intercept Facebook messages. Paper accepted by CCS 2014. **Google Acknowledged our contribution to Android security[link]. Facebook awarded us $2000.**
- **Project on security hazards of Android fragmentation.** Vendors usually add new device drivers to Android to support their own hardware. I discovered that those third party drivers and vendor customization could severely undermine Android Security design. In this research, we built a dynamic

analyzer to automatically detect such vulnerabilities. We identified 5 vulnerabilities that allow zero permission app to take picture, screenshots, log touchscreen events, kill any process and allocate kernel memory. We further build a static analyzer and scanned 2423 phone roms and found 1290 vulnerable phone images. Paper is accepted byIEEE Symposium on Security and Privacy (S&P 14), 2014. More information at https://sites.google.com/site/linuxdroid0/. Samsung Awarded few latest devices as a token of appreciation for those findings.

- **Project on Android public resource information leaks.** In this project, we found information leaks on mobile platform such as Android. We demonstrated that an app without any permission can get the phone user's identity, financial data and locations precisely. The problem is caused by the gap between Linux design and mobile phone usage. Paper accepted by CCS 2013. Project demo at: https://sites.google.com/site/sidedroid/home.
- **Project on Android external device protection.** More and more external medical devices connect to a mobile phone via Bluetooth or NFC. But Android does not provide enough protection for those external devices and allows malicious app to communicate with critical devices such as glucose meter, blood pressure meter. This project demonstrates a few attacks on external medical devices. I extended Android and SeLinux to provide a OS level protection for those devices so only the official app can communicate with the device. Demo at: https://sites.google.com/site/edmbdroid/. Project is open sourced at: https://github.com/DabinderAndroid/extDroid.git. The Paper is accepted by NDSS 2014.

Google Summer Intern in Ads Spam Team, Mountain View, CA May 2012 - Aug 2012

- Research on preventing Ads click fraud on Android apps using static code analysis on Bouncer. Designed and Developed a tool to migrate a SQL database to bigtable.

Microsoft Summer Intern at Online Service Division, Redmond, WA May 2011 - Aug 2011

- Built a reporting system to track the software testing progress of AdCenter testing platform and automatically generate test plans for failed test cases.

SOIC, Indiana University, Bloomington, IN Aug 2009 - Dec 2011

Research Assistant

- **Project on privacy preserving hybrid cloud computing.** The idea is to combine private cloud with public cloud and ship the computation on non-sensitive data to public cloud while keeping the computation on sensitive data in private cloud and later combine the results. Developed a static source code analyzer based on Soot to automatically transform Java code and split the computation.
- **Android malware project.** This project discovered novel colluding attacks on Android that allow two applications collude with each other to hide malicious behaviors. Paper published on NDSS 2011.
- **Human genome data privacy project.** The project measure the risk of releasing genome data. Paper accepted by ESORICS 2011. Proved the NP-completeness of genome data reversing problem and analyzed the attack space of reversing genome sequence data from aggregate data.
- **Effective Malware Detection Project.** The aim of the project was to combine system call dependence graph with instruction level data flow analysis to detect polymorphic malwares. This work was published in USENIX Security 2009.

SELECTED PUBLICATIONS

- What's in Your Dongle and Bank Account? Mandatory and Discretionary Protection of Android External Resources. Xiaoyong Zhou*, Soteris Demetriou*, Muhammad Naveed, Yeonjoon Lee, Kan Yuan, Xiaofeng Wang and Carl A. Gunter. In Network and Distributed System Security Symposium (NDSS), 2015.
- Hare Hunting in the Wild Android: A Study on the Threat of Hanging Attribute References. Yousra Aafer, Nan Zhang, Zhongwen Zhang, Xiao Zhang, Kai Chen, XiaoFeng Wang, Xiaoyong Zhou, Wen-

liang Du, Michael Grace. In ACM Conference on Computer and Communications Security (CCS), 2015

- Leave Me Alone: App-level Protection Against Runtime Information Gathering on Android. Nan Zhang, Kan Yuan, Muhammad Naveed, Xiaoyong Zhou, XiaoFeng Wang. In IEEE Symposium on Security and Privacy (Oakland), 2015.
- The Peril of Fragmentation: Security Hazards in Android Device Driver Customizations. Xiaoyong Zhou, Yeonjoon Lee, Nan Zhang, Muhammad Naveed, XiaoFeng Wang. In IEEE Symposium on Security and Privacy (Oakland), 2014.
- Mayhem in the Push Clouds: Understanding and Mitigating Security Hazards in Mobile Push-Messaging Services. Tongxing Li, Xiaoyong Zhou, Luyi Xing, Yeonjoon Lee, Muhammad Naveed, Xiaofeng Wang and Xinhui Han. In ACM Conference on Computer and Communications Security (CCS), 2014.
- Inside Job: Understanding and Mitigating the Threat of External Device Misbinding on Android Muhammad Naveed, Xiaoyong Zhou, Soteris Demetriou, XiaoFeng Wang, Carl Gunter. In Network and Distributed System Security Symposium (NDSS), 2014.
- Screenmilker: How to Milk Your Android Screen for Secrets. Chia-Chi Lin, Hongyang Li, Xiaoyong Zhou and XiaoFeng Wang. In Network and Distributed System Security Symposium (NDSS), 2014.
- Identity, Location, Disease and More: Inferring Your Secrets from Android Public Resources. Xiaoyong Zhou, Soteris Demetriou, Dongjing He, Muhammad Naveed, Xiaorui Pan, Xiaofeng Wang and Carl Gunter, Klara Nahrstedt. In ACM Conference on Computer and Communications Security (CCS), 2013.
- To Release Or Not To Release: Evaluating Information Leaks in Aggregate Human-Genome Data. Xiaoyong Zhou, Peng Bo, XiaoFeng Wang and Haixu Tang. In European Symposium on Research in Computer Security (ESORICS), 2011.
- Sedic: Privacy-Aware Data Intensive Computing on Hybrid Clouds. Kehuan Zhang, Xiaoyong Zhou, Yangyi Chen, XiaoFeng Wang, Yaoping Ruan. In The 18th ACM Conference on Computer and Communications Security (CCS), 2011.
- Soundminer: A Stealthy and Context-Aware Sound Trojan for Smartphones. Roman Schlegel, Kehuan Zhang, Xiaoyong Zhou, Mehool Intwala, Apu Kapadia, and XiaoFeng Wang. In The 18th Annual Network & Distributed System Security Symposium (NDSS), 2011.
- Effective and Efficient Malware Detection at the End Host. Clemens Kolbitsch, Paolo Milani Comparetti, Christopher Kruegel, Engin Kirda, Xiaoyong Zhou, and XiaoFeng Wang. In The 18th USENIX Security Symposium, Canada, August 2009.
- Learning Your Identity and Disease from Research Papers: Information Leaks in Genome Wide Association Study. By Rui Wang, Yong Li, XiaoFeng Wang, Haixu Tang, Xiaoyong Zhou. In The 16th ACM Conference on Computer and Communications Security (CCS), 2009. **PETs award 2011**.

HIGHLIGHTS & HONORS

- Acknowledged by Google Android security team for finding vulnerabilities in Google Cloud Messaging. https://source.android.com/devices/tech/security/acknowledgements.html
- Awarded a Galaxy Note for finding vulnerabilities in Samsung Android driver customization across hundreds phone models. https://sites.google.com/site/linuxdroid0/
- Cash award by Facebook for cloud messaging vulnerabilities in Facebook Messenger.
- CSAW Best paper award in applied cyber security research, 2014. (3/80)
- Program Committee of Usenix Security 2015, AsiaCCS 2015, 2016, ICDCS 2016, Securecomm 2015
- Media Coverage: The Register, Tom's Hardware ...