# XIAOYONG ZHOU

2637 E Windermere Woods Dr., Bloomington, IN, 47401
Tel: (812) 272-0568 E-mail: zhou@indiana.edu
Homepage: http://www.cs.indiana.edu/~zhou/


## OBJECTIVE

A highly motivated and creative PhD candidate interested in security and privacy related research positions. In-depth knowledge and research experience of mobile security and privacy, program analysis, malware analysis, and operating system. Some research experiences on Cloud Computing. Fast in creating solutions and algorithms with C/C++, Python, Matlab and Java. A team leader and also a team player.

## EDUCATION

School of Informatics and Computing (SOIC), Indiana University, Bloomington, IN — Sept 2008-July 2014
*PhD Candidate, expect on May 2014*, Majored in Information Security

School of Computing, National University of Defense Technology, Changsha, China — Sept 2004-May 2007
*Master of Engineering, Computer Science*, Majored in Computer Networks

Software College, Hunan University, Changsha, China — May 2004
*Bachelor of Engineering, Computer Science*, Majored in Software Engineering

## PUBLICATIONS

- The Peril of Fragmentation: Security Hazards in Android Device Driver Customizations. Xiaoyong Zhou, Yeonjoon Lee, Nan Zhang, Muhammad Naveed, XiaoFeng Wang. To appear on IEEE Symposium on Security and Privacy, 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 *CCS '2013*, Berlin, Germany.
- Inside Job: Understanding and Mitigating the Threat of External Device Misbinding on Android Muhammad Naveed, Xiaoyong Zhou, Soteris Demetriou, XiaoFeng Wang, Carl Gunter. Accepted by *NDSS* 2014.
- Screenmilker: How to Milk Your Android Screen for Secrets. Chia-Chi Lin, Hongyang Li, Xiaoyong Zhou and XiaoFeng Wang. Accepted by *NDSS* 2014.
- To Release Or Not To Release: Evaluating Information Leaks in Aggregate Human-Genome Data. Xiaoyong Zhou, Peng Bo, XiaoFeng Wang and Haixu Tang. In *ESORICS*, Leuven, Belgium, Sept, 2011
- Sedic: Privacy-Aware Data Intensive Computing on Hybrid Clouds. Kehuan Zhang, Xiaoyong Zhou, Yangyi Chen, XiaoFeng Wang, Yaoping Ruan. The 18th ACM Conference on Computer and Communications Security (*CCS'11*), Chicago, IL.
- Soundminer: A Stealthy and Context-Aware Sound Trojan for Smartphones. Roman Schlegel, Kehuan Zhang, Xiaoyong Zhou, Mehool Intwala, Apu Kapadia, and XiaoFeng Wang. To appear in *the 18th Annual Network & Distributed System Security Symposium (NDSS '11)*, San Diego, CA, February 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 09)*, Chicago, IL, Nov. 2009. **PETs award 2011.**

- L. Jean Camp, Rui Wang, and Xiaoyong Zhou. Global Regulation of IPv4 Address Exhaustion. ISGIG 2009, Prague, Czech Republic.
- Xiaoyong Zhou, Ning Hu, Zhenghu Gong. Data Stream based Real Time Network Traffic Data Analysis System Design. *Journal of Application Research of Computers*, September, 2007

## EXPERIENCE

**SOIC, Indiana University, Bloomington, IN** Now

*Research Assistant*

- **Project on security hazards of Android fragmentation.** Vendors usually add new device drivers to Android to support their own hardware. We found 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. This paper has been accepted by IEEE Symposium on Security and Privacy (S&P 14), 2014. Project website: https://sites.google.com/site/linuxdroid0/. We have reported those vulnerabilities to Google and Samsung. As a token of appreciation, Samsung send us latest devices for our future research. Following this work, I am doing research on automatically configuring SE Linux policies to make the security protection on Linux and framework layer consistent.
- **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 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 Security Team and Android Security Team, Mountain View, CA 2012

- Research on how to prevent click fraud on Android apps.
- Developed an information flow analysis tool to check if a malicious app tries to inject clicks to the embedded ads or generates non-organic ads requests. This tool is integrated into Google Bouncer and scans thousands apps each day.

**Microsoft** Summer Intern at Online Service, Redmond, WA 2011

- Built a reporting system to track the software testing progress of AdCenter testing platform and automatically generate test plans for failed test cases.
- Learned how Microsoft ad network operate and it's team process.

SOIC, Indiana University, Bloomington, IN Feb 2011

*Research Assistant*

- **Project on privacy preserving hybrid cloud computing.** The idea is to combine private cloud with public cloud. For many computations, only part of the data is sensitive, we can 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 source to source code transformation tool using Soot to automatically transform simple Java Map-Reduce code to split the computation. The transformation tool performs static code analysis and information flow analysis to detect the `fold` operations in map reduce program (Java code) and

automatically split this problem to shift as much computation to public cloud as possible. This paper was accepted by ACM CCS'11.

SOIC, Indiana University, Bloomington, IN From May 2010
*Research Assistant*

- **Android malware project.** This project discovered novel colluding attacks in which two applications collude with each other to hide malicious behaviors. Paper published on NDSS 2011.
- Extended AudioFlinger to prevent sensitive audio data leaks to malicious app. Extended the Android static permission checking mechanism to an context sensitive permission checking system to protect critical data at different context. (Java, C++)
- In-depth analysis of Android OS kernel, particularly the audio subsystem. (Android OS)

SOIC, Indiana University, Bloomington, IN Jan 2009 - Sept 2009
*Research Assistant*

- **GWAS data release project.** The project tries to find a risk measurement scale system to evaluate 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.
- Designed novel genome data reversing attack using integer program, machien learning and Markov Chain.(C++, Python, Matlab)

SOIC, Indiana University, Bloomington, IN May 2008 - Sept 2008
*Research Assistant*

- Participated in the 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.
- Developed a Windows kernel driver to log all the system calls and generate system call dependence graph as a malware signature. (C/C++, Python)
- Gained some experiences on Windows system level programming, malware analysis and program analysis.

## TECHNICAL SKILLS

Languages: Experienced in C/C++, Python, Java and Matlab, familiar with Ruby, R.
Platform: Experienced in programming on both Linux, Windows and Android OS.
Dev Tools: Eclipse, Emacs, Visual Studio, Matlab, R

## SELECTED COURSE PROJECTS

- Optimization MPI Collective Communication Operation (for CSCI B629) Developed an compiler module for GCC 4.2 using LLVM pass to automatically analyze the data flow and data dependence in C++ source code, automatically transform synchronized MPI call to asynchronized MPI call to parallize computation and communication. (C++, LLVM)
- Simple Speaker Recognition System based on MFCC and VQ (for INFO 547).Build a simple speaker recognition system. The front end is build on matlab voicebox to extract MFCC as features. The backend is a Vector Quantization to classify the data. The simple system can recognize a speaker from a pool of more than 10 people. (R, C++)
- Cloud-based on-line bidding system (for CSCI B534). Developed an bidding system running on Amazon EC2 and S3. (Java Axis2)

**PROFESSIONAL ACTIVITIES**

PET Award 2011 (The highest reward in privacy research)
External reviewer of CCS'2010,2011, 2013; WWW 2009; NDSS 2014; Oakland 2011,2012, 2013, 2014
Journal Reviewer: Computer & Security