Le Guan

CONTACT INFORMATION

Cyber Security Laboratory
College of Information Science and Technology
Pennsylvania State University, PA, US

814-883-0450
guanle.ustc@gmail.com
http://guanle.org

RESEARCH INTERESTS

My research interests cover a wide range of systems security, including mobile security and IoT systems security. I am especially interested in leveraging COTS hardware components/features to design and build systems that are more reliable and secure than solutions based on software alone.

EDUCATION

Institute of Information Engineering, Chinese academy of Sciences, China

- PhD. / Computer Science
- Advisors: Jiwu Jing/Jingqiang Lin *Sept. 2009 - Jan. 2015*

University of Science and Technology of China, China

- B.Eng. / Computer Science and Engineering *Sept. 2005 - May 2009*

EXPERIENCE AND PROJECTS

Pennsylvania State University *April 2015 - Present*

- Postdoctoral Researcher
- Advisors: Peng Liu
- Projects
  - IoT Security *2017 - Present*
    - Security mechanisms in the low-end ARM microcontroller, which powers considerable number of IoT devices, are surprisingly weak. This on-going research aims to analyze vulnerabilities residing on these low-end devices, and seek lightweight design to enhance the security of these devices.
  - TrustZone-based System Security *2015 - 2017*
    - TrustZone is a security extension to ARM devices. We novelly utilize it to achieve many security functions that go beyond its conventional usage. We used it to protect legacy programs, to encrypt memory, and to deploy bare-metal malware analysis platforms.
    - This research has led to two paper publications in *MobiSys* and *ACSAC*, as well as three papers under review.

Chinese Academy of Sciences *Sept. 2010 - Jan. 2015*

- Research Assistant
- Projects
  - Defeating Cold Boot Attacks with Cache *2013 - 2015*
    - We creatively leveraged processor cache to temporarily hold keys during a cryptographic computation. The solution eliminates the occurrences of keys in the vulnerable DRAM chip, thus defeating cold boot attacks.
    - This project has led to three paper publications in *Oakland*, *NDSS* and *TDSC*.
  - Ultra-high Speed Crypto Machine *2013 - 2014*
    - We developed a hardware security module capable of processing more than 500,000 times ECDSA signatures per second, owing to the highly optimized GPU implementation.

- This project won the first prize of Ministerial Award for Science and Technology Progress of Cryptography in China.

- PKI Inter-operation *2012 - 2012*
  - We developed a system that measures the inter-operation ability of both PKI server and client. I wrote an OCSP server and a LDAP crawler that dumps all certificates given a url.

PUBLICATIONS

[C10] **Le Guan**, Shijie Jia, Bo Chen, Fengwei Zhang, Bo Luo, Jingqiang Lin, Peng Liu, Xinyu Xing and Luning Xia, "Supporting Transparent Snapshot for Bare-metal Malware Analysis on Mobile Devices", *Proceedings of the 33rd Annual Conference on Computer Security Applications (ACSAC), 2017. Acceptance rate: 48/224=19.7%.*

[C9] **Le Guan**, Peng Liu, Xinyu Xing, Xinyang Ge, Shengzhi Zhang, Meng Yu, and Trent Jaeger, "TrustShadow: Secure Execution of Unmodified Applications with ARM TrustZone", *Proceedings the 15th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys), 2017. Acceptance rate: 34/188=18.1%.*

[C8] **Le Guan**, Sadegh Farhang, Yu Pu, Pinyao Guo, Jens Grossklags, and Peng Liu, "VaultIME: Regaining User Control For Password Managers through Auto-correction", *in Security and Privacy in Communication Networks: 13th International Conference (SecureComm), 2017* (short).

[C7] Pinyao Guo, Hunmin Kim, **Le Guan**, Minghui Zhu and Peng Liu, "VCIDS: Collaborative Intrusion Detection of Sensor and Actuator Attacks on Connected Vehicles", *in Security and Privacy in Communication Networks: 13th International Conference (SecureComm), 2017.*

[C6] **Le Guan**, Jun Xu, Shuai Wang, Xinyu Xing, Lin Lin, Heqing Huang, Peng Liu and Wenke Lee, "From Physical to Cyber: Escalating Protection for Personalized Auto Insurance", *in Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems (SenSys), 2016. Acceptance rate: 21/119=17.6%.*

[C5] **Le Guan**, Jingqiang Lin, Bo Luo, Jiwu Jing and Jing Wang, "Protecting private keys against memory disclosure attacks using hardware transactional memory", *in 2015 IEEE Symposium on Security and Privacy (Oakland), 2015. Acceptance rate: 55/407=13.5%.*

[C4] **Le Guan**, Jingqiang Lin, Bo Luo and Jiwu Jing, "Copker: Computing with Private Keys without RAM", *in 21st Annual Network and Distributed System Security Symposium (NDSS), 2014. Acceptance rate: 55/295=18.6%.*

[C3] **Le Guan**, Fengjun Li, Jiwu Jing, Jing Wang and Ziqiang Ma, "virtio-ct: A Secure Cryptographic Token Service in Hypervisors", *International Workshop on Data Protection in Mobile and Pervasive Computing (DAPRO) in conjunction with the 13th Security and Privacy in Communication Networks (SecureComm), 2014.*

[C2] Jing Wang, **Le Guan**, Limin Liu and Daren Zha, "Implementing a Covert Timing Channel Based on Mimic Function", *in Information Security Practice and Experience: 10th International Conference (ISPEC), 2014.*

[C1] Jing Wang, Peng Liu, Limin Liu, **Le Guan**, and Jiwu Jing, "Fingerprint Embedding: A Proactive Strategy of Detecting Timing Channels", *in Information and Communications Security: 15th International Conference (ICICS), 2013.*

[J2] Jingqiang Lin, **Le Guan**, Ziqiang Ma, Bo Luo, Luning Xia, and Jiwu Jing, "Copker: A Cryptographic Engine against Cold-Boot Attacks", *IEEE Transactions on Dependable and Secure Computing, vol. PP, no. 99, pp. 1-1, 2016*

[J1] Jingqiang Lin, Bo Luo, **Le Guan**, and Jiwu Jing, "Secure Computing Using Registers and Caches: The Problem, Challenges, and Solutions", *IEEE Security & Privacy, vol. 14, no. 6, pp. 63-70, Nov.-Dec. 2016*

Preprints and Papers in Submissions

Le Guan, Chen Cao, Sencun Zhu, Jingqiang Lin, Peng Liu, Yubin Xia, and Bo Luo, "Minimizing Sensitive Data Exposure on Mobile Devices with Targeted Encryption".

Le Guan, Chen Cao, Peng Liu, Xinyu Xing, Xinyang Ge, Shengzhi Zhang, Meng Yu and Trent Jaeger, "Building a Trustworthy Execution Environment to Defeat Exploits from both Cyber Space and Physical Space for ARM".

Chen Cao, **Le Guan**, Ning Zhang, Jingqiang Lin, Bo Luo, Neng Gao, Peng Liu, Ji Xiang and Wenjing Lou, "CryptMe: Data Leakage Prevention for Unmodified Programs on ARM Devices".

Chen Cao, **Le Guan**, Peng Liu, Neng Gao, Jingqiang Lin, and Ji Xiang, "Hey, you, keep away from my device: remotely implanting a virus expeller to defeat Mirai on IoT devices".

Patents and Other Publications

Jingqiang Lin, Jiwu Jing, **Le Guan**, Bingyu Li, Jing Wang, Wuqiong Pan, and Yuewu Wang, "Method and system for protecting root CA certificate in a virtualization environment", *U.S. Patent Application 20170295024, Published on October 12, 2017.*

Jingqiang Lin, **Le Guan**, Qiongxiao Wang, Jing Wang, Jiwu Jing, "Key protecting method and apparatus". *U.S. Patent Application 20160359621, Published on December 8, 2016.*

Jingqiang Lin, **Le Guan**, Jing Wang, Qiongxiao Wang, Jiwu Jing and Bingyu Li, "Multi-Core Processor Based Key Protection Method And System". *U.S. Patent Application 20150310231, Published on October 29, 2015.*

Jingqiang Lin, Jiwu Jing, **Le Guan**, Jing Wang, Bingyu Li, Yuewu Wang and Wuqiong Pan, "Method and system for providing password service in virtualized environment", *Chinese Patent CN104461678, 2015.* (in Chinese)

Wuqiong Pan, Jiwu Jing, **Le Guan**, Ji Xiang, Jingqiang Lin, and Xingjie Yu, "Method and apparatus for implementing SM2 cryptographic algorithm based on GPU", *Chinese Patent CN103532710, 2014.* (in Chinese)

Xueyan Lin, Jingqiang Lin, **Le Guan**, Lei Wang, "Deploying Chinese Commercial Cryptography in Virtual Desktop Infrastructure". *Journal of University of Chinese Academy of Sciences, 2015, 32(5):701-707.* (in Chinese).

Jing Wang, Neng Gao, Jingqiang Lin, and **Le Guan**, "A Survey of Network-based Covert Timing Channels", *Netinfo Security 8 (2012): 053.* (in Chinese).

"Research on the Protection of Cryptographic Keys in Commodity Platform", *PdH Thesis, University of Chinese Academy of Sciences, 2015.* (in Chinese).

"Deploying Public Key Infrastructure In Mobile Devices", *Bachelor Thesis, University of Science and Technology of China, 2009.* (in Chinese).

Conference Presentations

ACM MobiSys, Niagara Falls, NY. *Jun. 22, 2017*

- TrustShadow: Secure Execution of Unmodified Applications with ARM TrustZone

ACM SenSys, Stanford, CA. *Nov. 14, 2016*

- From Physical to Cyber: Escalating Protection for Personalized Auto Insurance

IEEE S&P, San Jose, CA. *May 18, 2015*

- Protecting Private Keys against Memory Disclosure Attacks using Hardware Transactional Memory

Talks

Zhejiang University, Hangzhou, China. *Sept. 2017*

- Building Hardware-assisted Secure Systems
- Host: Dr. Kui Ren

Institute of Information Engineering, CAS, Beijing, China. *Sept. 2017*

- System Security Built on the Integration of Hardware and Software
- Host: Dr. Jingqiang Lin

Institute of Software, CAS, Beijing, China. *Sept. 2017*

- Building Secure Systems with ARM TrustZone
- Host: Dr. Yu Qin

Teaching Experience

Teaching Assistant, University of Chinese Academy of Sciences, Beijing, China

- Graduate course: Introduction to Public Key Infrastructure *Sept. 2013 - Jan. 2014*

Guest Lecturer, Pennsylvania State University

- Undergraduate course: Overview of Information Security (SRA-221) *Aug. 2016 - Dec. 2014*

Mentoring Experience

PhD Candidate, University of Chinese Academy of Sciences, Beijing, China

- Wei Zhou *July 2017 - Present*
- Wei is a junior Ph.D student. We hold Skype meetings twice a week to find real-world security issues related to the emerging IoT techniques. I guide him to read relevant literatures, find tangible problems that matter, and help him address technique challenges.

PhD Candidate, University of Chinese Academy of Sciences, Beijing, China

- Congwu Li *Sept. 2016 - Present*
- Congwu is a senior Ph.D student. We are working on developing an OS-agnostic security mechanism that is resilient to memory attacks. I give him instructions on the overall system design and help him deal with programming difficulties.

PhD Candidate, Pennsylvania State University, PA

- Wenhui Zhang *Aug. 2017 - Present*
- We have weekly meeting to discuss IoT virtualization. I help her split the problem into pieces, and teach her hand-on practices to solve the problems one by one.

Academic Service

PC Member

- IEEE Conference on Communications and Network Security (CNS) 2018
- EAI International Conference on Security and Privacy in Communication Networks (SecureComm) 2017

Shadow PC Member

- ACM SIGOPS/EuroSys European Conference on Computer Systems (EuroSys) 2018

Reviewer

- IEEE Transactions on Dependable and Secure Computing (TDSC)
- European Symposium on Research in Computer Security (ESORICS) 2016, 2017
- Financial Cryptography (FC) 2016
- IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom) 2016
- International Conference on Security and Cryptography (SECRYPT) 2015

Honors and Awards

National Scholarship (top 0.2% nationwide) *2013*

Institute Director Award of Institute of Information Engineering *2013*

Merit Student of University of Chinese Academy of Sciences *2012*

Outstanding Undergraduate Thesis Award of University of Science and Technology of China (top 5%) *2009*

Outstanding Graduate of University of Science and Technology of China (top 15%) *2009*

National Endeavor Scholarship of University of Science and Technology of China *2008*

Outstanding Student Scholarship of University of Science and Technology of China *2007*

Outstanding Freshman Scholarship of University of Science and Technology of China *2005*

References

Available upon request.

Last updated: November 12, 2017