Le Guan

CONTACT INFORMATION

805 Boyd Graduate Studies Research Center
Department of Computer Science
The University of Georgia, GA, US

814-883-0450
leguan@uga.edu
https://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

The University of Georgia *November 2018 - Present*

- Assistant Professor

Pennsylvania State University *April 2015 - October 2018*

- 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 Cryptographic 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

Conference Publications

[C21] Wei Zhou, **Le Guan**, Peng Liu, Yuqing Zhang, "Automatic Firmware Emulation through Invalidity-guided Knowledge Inference", *30th USENIX Security Symposium (Security'21)* (accepted).

[C20] Wenqiang Li, **Le Guan**, Jingqiang Lin, Jiameng Shi, Fengjun Li, "From Library Portability to Para-rehosting: Natively Executing Microcontroller Software on Commodity Hardware", *Annual Network and Distributed System Security Symposium (NDSS'21)* (accepted).

[C19] Chen Cao, **Le Guan**, Jiang Ming, Peng Liu, "Device-agnostic Firmware Execution is Possible: A Concolic Execution Approach for Peripheral Emulation", *Proceedings of the 36rd Annual Conference on Computer Security Applications (ACSAC'20)*.

[C18] Fangjie Jiang, Quanwei Cai, Jingqiang Lin, Fengjun Li, Bo Luo, **Le Guan**, Ziqiang Ma, "TF-BIV: Transparent and Fine-grained Binary Integrity Verification in the Cloud", *Proceedings of the 35th Annual Conference on Computer Security Applications (ACSAC'19)*.

[C17] Dawei Chu, Kaijie Zhu, Quanwei Cai, Jingqiang Lin, Fengjun Li, **Le Guan**, Lingchen Zhang, "Secure Cryptography Infrastructures in the Clouds", *IEEE Global Communications Conference (GLOBECOM'19)*.

[C16] Wei Zhou, Yan Jia, Yao Yao, Lipeng Zhu, **Le Guan**, Yuhang Mao, Peng Liu, Yuqing Zhang, "Discovering and Understanding the Security Hazards in the Interactions between IoT Devices, Mobile Apps, and Clouds on Smart Home Platforms", *28th USENIX Security Symposium (Security'19)*.

[C15] **Le Guan**, Chen Cao, Sencun Zhu, Jingqiang Lin, Peng Liu, Yubin Xia, Bo Luo, "Protecting Mobile Devices from Physical Memory Attacks with Targeted Encryption", *12th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec'19*.

[C14] Lingyun Situ, Linzhang Wang, Xuandong Li, **Le Guan**, Wenhui Zhang and Peng Liu, "Poster: Energy Distribution Matters in Greybox Fuzzing", *41st ACM/IEEE International Conference on Software Engineering (ICSE), 2019*.

[C13] 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", *21st International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2018*.

[C12] Fangjie Jiang, Quanwei Cai, **Le Guan** and Jingqiang Lin, "Enforcing Access Control

for Cryptographic Cloud Service Invocation based on Virtual Machine Introspection", *21st Information Security Conference (ISC), 2018.*

[C11] 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", *1st International Workshop on Security and Privacy for the Internet-of-Things (IoTSec), 2018.*

[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: 48/244=19.7%* (**Best Paper Award**).

[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.*

Journal Publications

[J7] Wei Zhou, Chen Cao, Dongdong Huo, Kai Cheng, Lan Zhang, **Le Guan**, Tao Liu, Yan Jia, Yaowen Zheng, Yuqing Zhang, Limin Sun, Yazhe Wang and Peng Liu, "Reviewing IoT Security via Logic Bugs in IoTPlatforms and Systems", *IEEE Internet of Things Journal, 2021*

[J6] Jin Ye, Lulu Guo, Bowen Yang, Fangyu Li, Liang Du, **Le Guan**, and Wenzhan Song, "Cyber-Physical Security of Powertrain Systems in Modern Electric Vehicles: Vulnerabilities, Challenges and Future Visions", *IEEE Journal of Emerging and Selected Topics in Power Electronics, 2020.*

[J5] Lulu Guo, Bowen Yang, Jin Ye, Hong Chen, Fangyu Li, Wenzhan Song, Liang Du, and **Le Guan**, "Systematic Assessment of Cyber-physical Security of Energy Management System for Connected and Automated Electric Vehicles", *IEEE Transactions on Industrial Informatics, 2020.*

[J4] Congwu Li, **Le Guan**, Jingqiang Lin, Bo Luo, Quanwei Cai, Jiwu Jing, and Jing Wang, "Mimosa: Protecting Private Keys against Memory Disclosure Attacks using Hardware Transactional Memory", *IEEE Transactions on Dependable and Secure Computing, 2019.*

[J3] **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", *IEEE Transactions on Dependable and Secure Computing, 2018.*

[J2] **Le Guan**, Jingqiang Lin, Ziqiang Ma, Bo Luo, Luning Xia, and Jiwu Jing, "Copker: A Cryptographic Engine against Cold-Boot Attacks", *IEEE Transactions on Dependable and Secure Computing, 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*

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", *PhD 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

WiSec, Miami FL. *May 15, 2019*

- Protecting Mobile Devices from Physical Memory Attacks with Targeted Encryption

ACSAC, Orlando, FL. *Dec. 7, 2017*

- Supporting Transparent Snapshot for Bare-metal Malware Analysis on Mobile Devices

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

Academic Service

PC Member

- International Conference on Information and Communications Security (ICICS) 2019, 2020
- EAI International Conference on Security and Privacy in Communication Networks (SecureComm) 2017, 2018, 2019, 2020
- IEEE Conference on Communications and Network Security (CNS) 2018

- Workshop on the Internet of Things Security and Privacy, in conjunction with CCS 2019, 2020
- Workshop on Secure Cryptographic Implementation, in conjunction with ACNS 2020

Shadow PC Member

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

Publicity Co-chair

- Workshop on Secure Cryptographic Implementation, in conjunction with ACNS 2020

Reviewer

- IEEE Transactions on Information Forensics and Security (TIFS) 2019, 2020
- IEEE Transactions on Dependable and Secure Computing (TDSC) 2016, 2017, 2018, 2019, 2020
- IEEE Transactions on Mobile Computing (TMC) 2018, 2019, 2020
- Frontiers of Computer Science 2019
- IEEE Access 2019
- Springer Cybersecurity 2018
- ACM CCS 2018, 2019
- IET Information Security 2017
- 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

Best Paper Award of ACSAC 2017 (2 out of 244 submissions) *2017*

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*