Le Guan

CONTACT INFORMATION

805 Boyd Graduate Studies Research Center — 814-883-0450
School of Computing — leguan@uga.edu
The University of Georgia, GA, US — https://cobweb.cs.uga.edu/~leguan/

RESEARCH INTERESTS

My research interests cover a wide range of systems security and software security. My prior work leverages COTS hardware components/features to design and build systems that are more reliable and secure than solutions based on software alone. Recently, I am actively involved in research focused on advancing the state of the art in firmware analysis.

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

The University of Georgia — *November 2018 - Present*

- Assistant Professor

Pennsylvania State University — *April 2015 - October 2018*

- Postdoctoral Researcher — Advisors: Peng Liu

PUBLICATIONS

Conference Publications

[C31] Xi Tan, Zheyuan Ma, Sandro Pinto, **Le Guan**, Ning Zhang, Jun Xu, Zhiqiang Lin, Hongxin Hu, Ziming Zhao, "SoK: Where's the "up"?! A Comprehensive (bottom-up) Study on the Security of Arm Cortex-M Systems", *USENIX WOOT Conference on Offensive Technologies (WOOT '24).*

[C30] Jiameng Shi, Wenqiang Li, Wenwen Wang, **Le Guan**, "Facilitating Non-Intrusive In-Vivo Firmware Testing with Stateless Instrumentation", *Annual Network and Distributed System Security Symposium (NDSS '24).*

[C29] Shariful Alam, **Le Guan**, Zeyu Chen, Haining Wang, Jidong Xiao, "CAUSEC: Cache-based Secure Key Computation with (Mostly) Deprivileged Execution", *43rd IEEE International Conference on Distributed Computing Systems (ICDCS '23)*

[C28] Kai Cheng, Yaowen Zheng, Tao Liu, **Le Guan**, Peng Liu, Hong Li, Hongsong Zhu, Kejiang Ye, Limin Sun, "Detecting Vulnerabilities in Linux-based Embedded Firmware with SSE-based On-demand Alias Analysis", *2023 ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA '23)*

[C27] Wei Zhou, Zhouqi Jiang, **Le Guan**, "Understanding MPU Usage in Microcontroller-based Systems in the Wild", *2023 Workshop on Binary Analysis Research (BAR '23).*

[C26] Wei Zhou, Zhouqi Jiang, **Le Guan**, "Good Motive but Bad Design: Pitfalls in MPU Usage in Embedded Systems in the Wild", *Black Hat Europe 2022.*

[C25] Wei Zhou, Lan Zhang, **Le Guan**, Peng Liu, Yuqing Zhang, "What Your Firmware

Tells You Is Not How You Should Emulate It: A Specification-Guided Approach for Firmware Emulation", *2022 ACM Conference on Computer and Communications Security (CCS '22)*.

[C24] Jiameng Shi, **Le Guan**, Wenqiang Li, Dayou Zhang, Ping Chen, Ning Zhang, "HARM: Hardware-assisted Continuous Re-randomization for Microcontrollers", *2022 IEEE European Symposium on Security and Privacy (EuroS&P '22)*.

[C23] Wenqiang Li, Jiameng Shi, Fengjun Li, Jingqiang Lin, Wei Wang, **Le Guan**, "μAFL: Non-intrusive Feedback-driven Fuzzing for Microcontroller Firmware", *44th International Conference on Software Engineering (ICSE '22)*.

[C22] Dongliang Fang, Zhanwei Song, **Le Guan**, Puzhuo Liu, Anni Peng, Kai Cheng, Yaowen Zheng, Peng Liu, Hongsong Zhu, Limin Sun, "ICS3Fuzzer: A Framework for Discovering Protocol Implementation Bugs in ICS Supervisory Software by Fuzzing", *Proceedings of the 37th Annual Conference on Computer Security Applications (ACSAC '21)*.

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

[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)*.

[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 36th 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-Companion), 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 '18.*

[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 '18.*

[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 '18.*

[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

[J10] Dongliang Fang, Anni Peng, **Le Guan**, Erik van der Kouwe, Klaus von Gleissenthall, Wenwen Wang, Yuqing Zhang, Limin Sun, "InvisiGuard: Data Integrity for Microcontroller-Based Devices via Hardware-Triggered Write Monitoring", *IEEE Transactions on Dependable and Secure Computing, 2024.*

[J9] Lingyun Situ, Chi Zhang, **Le Guan**, Zhiqiang Zuo, Linzhang Wang, Xuandong Li, Peng Liu, Jin Shi, "Physical Devices-Agnostic Hybrid Fuzzing of IoT Firmware", *IEEE Internet of Things Journal, 2023.*

[J8] Lingyun Situ, Zhiqiang Zuo, **Le Guan**, Linzhang Wang, Xuandong Li, Jin Shi, and Peng Liu. "Vulnerable Region-Aware Greybox Fuzzing", *Journal of Computer Science and Technology, 2021.*

[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 environ-

ment", *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

ICDCS, Hong Kong, China. *July 21, 2023*

- CAUSEC: Cache-based Secure Key Computation with (Mostly) Deprivileged Execution

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

Northwestern University, U.S. *April 2022*

- Research on Microcontroller Security
- Host: Dr. Xinyu Xing

NIO California, U.S. *Jan. 2022*

- Emulation-based Fuzzing for Microcontroller Firmware
- Host: Dr. Yueqiang Cheng

Institute of Information Engineering, Chinese Academy of Sciences, China. *Dec. 2021*

- Fuzzing Microcontroller Firmware
- Host: Dr. Kai Chen

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

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

Institute of Information Engineering, Chinese Academy of Sciences, 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

- ACM Conference on Computer and Communications Security (CCS), 2023 (2nd review cycle), 2024
- USENIX Security, 2022
- International Conference on Dependable Systems and Networks (DSN), 2022, 2024
- Annual Conference on Computer Security Applications (ACSAC), 2022, 2023, 2024
- Military Communications Conference (MILCOM), 2023
- International Conference on Computer Communictions and Networks (ICCCN), 2023
- International Conference on Information and Communications Security (ICICS) 2019, 2020, 2022
- EAI International Conference on Security and Privacy in Communication Networks (SecureComm) 2017, 2018, 2019, 2020
- IEEE Conference on Communications and Network Security (CNS) 2018
- Joint Workshop on the Internet of Things Security and Privacy (IoT S&P), in conjunction with CCS 2019
- Joint Workshop on CPS & IoT Security and Privacy (CPSIOTSEC), in conjunction with CCS 2020 - 2024
- Workshop on Secure Cryptographic Implementation, in conjunction with ACNS 2020

Workshops Chair

- EAI International Conference on Applied Cryptography in Computer and Communications (AC3), 2021

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 - 2023
- IEEE Transactions on Dependable and Secure Computing (TDSC) 2016 - 2022
- ACM Transactions on Privacy and Security 2021
- IEEE Transactions on Mobile Computing (TMC) 2018 - 2021
- IEEE TransactionsTransactions on Services Computing (TSC), 2021
- Frontiers of Computer Science 2019
- IEEE Access 2019
- Sensors 2020
- Springer Cybersecurity 2018
- ACM CCS 2018, 2019
- ICDCS 2021
- 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

Faculty Research Excellence Award, School of Computing, UGA *2023*

NSF CAREER Award *2023*

Greatly contribute to the career development of UGA graduates *2020, 2022*

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*