Lele MA

Last Updated on Feb 13, 2018

ADDRESS: 101A, McGlothlin-Street Hall,
The College of William and Mary

PHONE: +1 757 332 6046
EMAIL: lma03@email.wm.edu

RESEARCH INTERESTS & SPECIALTIES

General Interests: **Cloud/Edge Computing; Virtualization, Linux Containers; Operating System, System Security, Binary Analysis.**

Specialties:
- Virtual Machine Introspection, Xen Virtualization Security
- Intrusion Detection, Memory Integrity Checking
- Docker Container Migration
- Programming Languages: Professional in C/C++, Java; Familiar with Go, Python, Bash Shell, Haskell, Prolog.

EDUCATION

08/2015 – PRESENT
Ph.D. Candidate in COMPUTER SCIENCE
College of William & Mary, Williamsburg, VA, USA
Advisor: Prof. Qun LI

09/2012 – 07/2015
Master Degree in COMPUTER SCIENCE
Institute of Software, Chinese Academy of Sciences, Beijing, China
Advisor: Prof. Qiusong YANG

09/2008 – 06/2012
Bachelor Degree in COMPUTER SCIENCE
Shandong University, Jinan, Shandong Province, China

WORK EXPERIENCE

08/2015 – PRESENT
Teaching Assistant
Classes:
- CSCI 312: Principles of Programming Languages — Fall 2016, Spring 2017, Spring 2018
- CSCI 420-2: Computer Animation — Fall 2017
- CSCI 141: Computational Problem Solving — Spring 2016
- CSCI 420: Data and Code Security — Fall 2015

Skills: compilation, rainbow tables; **languages**: Python, Haskell, C, C++

01/2017 – 04/2017
Project: Service Handoff across Edge Servers via Docker Container Migration
Description: Enable seamless service handoff across edge servers by fast migrating the Docker container while mobile clients moving from one edge server towards another edge server. By leveraging layered file system on Docker's AUFS storage driver, we reduce service handoff time by $\%56 \sim 80\%$ compared to the VM-based solution.
Skills: union mount file system; user space process migration; **language skills**: Python, Go.

05/2014 – 06/2015
Project: CPU and OS Integrated Security Research
Prject Tasks: Integrated protection for the system, mainly utilizing 4 kinds of techniques: CPU micro-codes enhanced protection, trusted booting, dynamic integrity measurments, and virtual machine introspection.

My Task: Kernel Integrity Checking via Virtual Machine Introspection Based on Mini-OS—the tiny operating system in Xen source tree.
Design and implement the integrity checking agent based on a Mini-OS domain on Xen platform. The agent is well isolated through the Mandatory Access Control by XSM; it's lightweight with much less performance overhead; it's clean-state with little expansion of the TCB of the system. It can detect malicious behaviors that attempt to tamper with the critical codes or data of the runtime kernel, like the IDT table, keyboard handler, etc.
Skills: runtime integrity measurements, virtual machine introspection, para-virtualization, Xen and Mini-OS; **language**: C.

07/2013 – 05/2014

Project: Design of Hardware & Software Integrated Security Attack Scenarios
Prject Tasks: Reproduce the hardware bugs and evaluate their hazards to operating systems under certain scenarios. Mainly contain 4 bugs to design the attack scenarios: CPU micro-codes updating bugs, CPU cache vulnerability, System Management Mode attacks, and Hardware Virtual Machine attacks.
My Task: Research on CPU cache vulnerability & Hardware Virtual Machine Attacks.
Mainly doing experiments on two scenarios: experiment that exploits the vulnerability of CPU cache to attack SMM codes stored in SMRAM; experiment that reproduces attacks on the HVM platform via NewBluePill (from Invisible Things Lab)
Skills: System Management Mode, CPU cache control via MTRR, Hardware Virtual Machine; **language**: IA32 assembly, C.

09/2012 – 06/2013

Project: Static Program Analysis and Driver Verification Based on Symbolic Execution
Prject Tasks: Driver verification based on symbolic analysis of their c source codes. Mainly use the predator as the back-end tool to operate the checking. Front-end is developed based on Linux Driver Verification.
My Tasks: Develop the front-end based on the open source project Linux Driver Verification Project.
Skills: Programming in combination of Perl, Ruby, Shell, and C codes, and programs management via Makefiles.

11/2011 – 06/2012

Project: Personalized Privacy Policy Definition and Verification
Prject Tasks: Explore the mechanisms of how the privacy policies can be personally defined by users, and how to check and resolve the conflicts among the personalized policies.
My Tasks:(Thesis work) Design and Implementation of Privacy Policy Management Middleware System.
The system allows users to define personalized privacy policies on their online private resources. The system uses tuProlog logic engine to model privacy policies and check the potential conflicts among the personalized policies. Conflicts can be detected via the logic engine and can be resolved by users' choice.
Skills: RBAC, ABAC; First-order logic programming; **language**: Prolog, Java (>20KLOC).

Publications

[1] Lele Ma, Shanhe Yi, and Qun Li. Efficient service handoff across edge servers via docker container migration. In *IEEE/ACM Symposium on Edge Computing (SEC)*. IEEE, 2017.

[2] Lele Ma, Xiaomeng Yue, Yuqing Wang, and Qiusong Yang. Virtual machine introspection and memory security monitoring based on light-weight operating system. *Journal of Computer Applications (in Chinese)*, 2015.

[3] Yuan Wang, Yuqing Sun, and Lele Ma. Specification and enforcement of personalized privacy policy for social network. *Journal of China Institute of Communications (in Chinese)*, 33, 2012.