Cheng TAN

New York University
ct1607@nyu.edu

EDUCATION

Phd Student, Courant Institute of Mathematical Sciences Sep.2014∼Present
New York University, USA

Master of Science, Software School Sep.2011∼Jun.2014
Fudan University, China

Bachelor of Engineering, Software Institute Sep.2007∼Jun.2011
Nanjing University, China
Rank: Top 10%

RESEARCH EXPERIENCE

System Group, New York University, U.S.A
Research Assistant, July. 2015 ∼ Sept. 2015
Advisor: Prof. Micheal Walfish
Concentration: Web Verification

Institute of Parallel And Distributed System (IPADS),Shanghai Jiao Tong University, China
Visiting Student, Oct. 2012 ∼ Jun. 2014
Advisor: Prof. Haibo CHEN
Concentration: Mobile System

Parallel Processing Institute (PPI), Fudan University, China
Research Assistant, Dec. 2010 ∼ Sep. 2012
Advisor: Prof. Haibo CHEN and Prof. Binyu ZANG
Concentration: Virtualization, Computer System

PUBLICATIONS

Yubin Xia, Yutao Liu, **Cheng Tan**, Mingyang Ma, Haibing Guan, Binyu Zang, Haibo Chen. TinMan: Eliminating Confidential Mobile Data Excposure with Security-oriented Offloading. (**Eurosys 2015**)

Cheng Tan, Haibo Li, Yubin Xia, Binyu Zang, Cheng-Kang Chu, Tieyan Li, Feng Bao. PreCrime to the Rescue: Defeating Mobile Malware One Step Ahead. (**Apsys 2014**)

Cheng Tan, Yubin Xia and Haibo Chen, Binyu Zang. TinyChecker: Transparent Protection Of VMs Against Hypervisor Failures With Nested Virtualization. The Second International Workshop on Dependability of Clouds, Data Centers and Virtual Machine Technology (**DCDV 2012**)

HONORS AND AWARDS

- Outstanding Graduates Student of Software School, 2014
- Outstanding Contribution Award at IPADS, SJTU, 2013
- Silver medal award in Nvidia CUDA Parallel Program Competition, 2011
- Third-place award in National Morgan Stanley CodeStorm, 2011
- First Grade Scholarship for Excellent Freshman, 2011
- Outstanding Graduates Awards of Nanjing University, 2011

- Outstanding Student of Nanjing University, 2008

RESEARCH PROJECTS

Nested Virtualization

Along with the rapid development of virtualization technology, lots of new features are added to the hypervisor which inflates its code size and brings bugs and vulnerabilities. Nested virtualization systems are built beneath virtualization layer to mitigate these threats.

TinyChecker: Transparent Protection Of VMs Against Hypervisor Failures With Nested Virtualization
Dec. 2011 ∼ May. 2012

With the expansion of the code size, hypervisors are more likely to crash. To survive the guest VMs from a crashed hypervisor, we design TinyChecker, a very small software layer designated for transparent failure detection and recovery. By recording the entire communication context between VM and hypervisor, TinyChecker can protect the critical VM data, detect and recover the hypervisor among failures. [DCDV 2012 (collocated with **DSN 12**)]

CloudVisor: Retrofitting Protection of Virtual Machines in Multi-tenant Cloud with Nested Virtualization
Dec. 2010 ∼ Nov. 2011

With overstaffed software stack, clouds are vulnerable from adversaries including the cloud operators, which may lead to leakage of sensitive data. CloudVisor is a tiny monitor underneath the commodity VMM using nested virtualization and provides protection to the hosted VMs. I helped in building the final version of CloudVisor and implemented the automatic PCI-device detector and secure live migration module with emulated NIC. [SOSP 2011]

Mobile Enhancement Systems

Mobile platforms like smartphones have unique features like scarce computing, storage and power resources, high possible to physical attacks and lost. These usually render traditional measures for desktop and servers not directly applicable. The following projects aim at hardening mobile systems using various approaches.

PreCrime to the Rescue: Defeating Mobile Malware One Step Ahead
Aug. 2013 ∼ May. 2014

Since suspicious apps are constantly evolving to bypass present detecting techniques, it becomes harder for nowadays measures to prevent abnormal behavior from happening. We propose a speculative execution framework called PreCrime, which is deployed on cloud to explore the possible paths one step ahead of the smartphone. [Apsys 2011]

TinMan: Eliminating Confidential Mobile Data Excposure with Security-oriented Offloading
Feb. 2013 ∼ Jun. 2014

The wide adoption of smart devices has stimulated a fast shift of security-critical data from desktop to mobile devices. However, recurrent device theft and loss expose mobile devices to various security threats and even physical attacks. This paper presents TinMan, a system that protects confidential data, such as web site password and credit card number, from being leaked or abused even under device theft. TinMan separates accesses of these confidential data from the rest of the functionalities of an app, by introducing a trusted node to store confidential data and offloading any code from a mobile device to the trusted node to access such data. I designed and implemented the **asymmetric** taint tracking part of RoseCloud. [Eurosys 2015]

Redroid: Automated Auditing and Recovery on Smartphones
Feb. 2012 ∼ Oct. 2013

Market release model and repackaged applications make the suspicious apps easy to spread and hard to spot. Since malware is hard to eliminate, how to do post-mortem auditing and recovery of the damage caused becomes a key research challenge. We design and implement ReDroid, an event-centric record and replay framework, to track the applications' operations with little overhead. By replaying a malware-free version of the application, ReDroid can analyze the different behavior between record and replay and repair the data generated from benign operations.

TEACH ASSISTANT

NYU	CSCI-UA.0202: Operating System	Spring 2015
SJTU	X037514: Computer System Design and Implementation	Spring 2013
Fudan	SOFT130031.01: Operating System II	Spring 2012

SKILLS

Programming: C, JAVA, OCaml, Lua
Platform: Linux, Android, Xen