

Ethan Zhichuang Sun

RESEARCH INTERN · EXPERTISE IN SYSTEM SECURITY

27 Madeley, Stony Brook, NY, U.S.A. 11790

☎ (+1) 631-946-9937 | ✉ zhisun@cs.stonybrook.edu | 📱 sunzc | 📠 sun-zc-0942657b

“Be like a duck. Calm on the surface, but always paddling like the dickens underneath. —Michael Caine”

Education

Stony Brook University

SECOND YEAR PH.D. IN SYSTEM SECURITY, CS DEPT.

- Special CS Department Chair Fellowship

Stony Brook, NY, U.S.A.

Aug 2015 - present

Peking University

M.S. IN COMPUTER SCIENCE

- The Okamatsu Scholarship, 2014

Beijing, China

Sep 2012 - Jul 2015

Huazhong University of Science and Technology(HUST)

B.S. IN COMPUTER SCIENCE

- National Scholarship, 2010

Wuhan, China

Sep 2008 - Jul 2012

Paper

Shreds : Fine-grained Execution Units with Private Memory

YAOHUI CHEN, SEBASSUJEEN REYMONDJOHNSON, ZHICHUANG SUN, LONG LU

S&P/Oakland'16)

(acceptance rate 13.3% = 55/413)

Experience

Graduate Research, Research in Software and System Security Lab(Prof. Long Lu)

Stony Brook University, NY, U.S.A.

REMOTE ATTESTATION FOR EMBEDDED DEVICES (PROJECT LEADER, ON-GOING PROJECT)

Aug 2016 - now

- **Motivation:** the state-of-art remote attestation focus mostly on code integrity, which is not enough considering control-flow hijacking attacks, C-FLAT move it forward by introducing control flow verification, but the overhead is quite high, and it has limited cover on data-oriented attack. While the real world attacks targeting at IoT devices are becoming more and more complex, like Stuxnet, Mirai malware. This work aims at improving the state-of-art remote attestation by covering both control-flow and critical data-flow verification with high efficiency.
- **Key Idea:** First, improving the efficiency of control-flow verification by reducing world-switch frequency and offering better design of hash-mechanism. Second, introducing critical data-flow verification using compiler-based instrumentation.
- This is still an on-going project, while the current evaluation shows that it is a quite promising work, so far, for control-flow verification, it brings tens of times improvement on overhead and a more wide range of adoption.

Graduate Research, Research in Software and System Security Lab(Prof. Long Lu)

Stony Brook University, NY, U.S.A.

RESEARCHER FOR <SHREDS: FINE-GRAINED EXECUTION UNITS WITH PRIVATE MEMORY>

Aug 2015 - Dec 2015

- **Motivation:** current memory isolation/protection provided by the OS are at process level, which means once attacker hijacks the control flow of program, the whole memory of the process is exposed to the attacker. It's bad. Shreds project tries to provide the programmer a set of hardware-backed OS primitives that help programmer protect its secrets even when the process is compromised. Shreds make an innovative use of ARM domain memory management mechanism and the basic idea is that the secrets is only open to access when the programmer needs it, otherwise it is kept in locking state.
- **Contribution:** Shreds has two key components, a S-compiler which helps make sure code inside shred won't leak secrets and is security-augmented, a S-driver that functions as a kernel module and handles the secure memory allocation and management. My contribution in this project is offering an optimized design and implementation of the S-driver, which is a modularized thread-safe secure memory management driver.
- Besides, I also implement the memory domain fault handler which cooperates with the S-driver. and provide a user interface as well as a run-time helper library.

Graduate Course Project(OS): Implement an OS from Scratch for x64 architecture(Finished Alone)

Stony Brook University, NY, U.S.A.

PLUM OS: PEOPLE LIKE U AND ME CAN WRITE OS

Aug 2015 - Dec 2015

- Implement the PLUM OS totally from scratch, which is a preemptive OS that support virtual memory, process management, terminal, simple tarfs file system and so on.
- Support demand-paging and copy-on-write, process tracking(ps, kill -9, background running), short-cut for process and screen management(Ctrl-C, Ctrl-L), as well as executing shell scripts.
- Implement the corresponding simple libc library and a user shell, including some simple user command like ls, cd, cat, ps, kill and so on.

Graduate Course Project(Compiler Design): Implement a Compiler for a Event Processing Language E--(Team Work)

Stony Brook University, NY, U.S.A.

COMPILER DESIGN

Aug 2016 - Dec 2016

- Implement the Compiler for language E-- in C++, which is an event processing language that support basic data types, functions, events, and rules.
- Use lex and bison to do lexical and grammar analysis, generating AST, implementing type-checker, and finally we need to output the IR(an assembly style language) , which will be translated into native binary code with the tool provided by professor.
- This course offers a great chance to build our own compiler from scratch and a good chance to practice programming with C++.

Graduate Research, OS Group, Micro-Processor Research&Development Center(Prof. Xuetao Guan)

Peking University, Beijing, China

IMPLEMENTING LINUX BASED OS FOR UNICORE64 ARCHITECTURE

Sep 2012 - Aug 2013

- UniCore-III processor(based on UniCore64 architecture) is designed by Micro-Processor Research&Development Center of Peking University, which is a 64-bit, multi-core and superscalar micro-processor.
- Implement the low-level virtual memory and process management interface for Linux on UniCore64 Architecture. And gain rich Linux kernel development and debugging experiences
- Design and implement a tool named FuncTrace to assist kernel-debugging, which is a QEMU trace plugin with a analysis tool written in python. It helps locate low level kernel bugs. This tool was widely used within our lab.

Graduate Research, OS Group, Micro-Processor Research&Development Center(Prof. Xuetao Guan)

Peking University, Beijing, China

EXTENDING QEMU FOR UNICORE64 ARCHITECTURE

Sep 2012 - Aug 2013

- Adding support for UniCore64 architecture in QEMU, which is a generic and open source machine emulator and virtualizer.
- Emulating PCI-host-bridge for PKUnity SoC, supporting PCI IDE&Network devices in QEMU for UniCore64 architecture.
- Adding PCI-host-bridge driver in Linux kernel for UniCore64 architecture.

Toy Project Using Python GUI(Just for fun)

Peking University, Beijing, China

JAPANESE DICTIONARY FROM SCRATCH

Aug 2013

- **Motivation:** current on-line Japanese dictionaries recommend long and difficult sentences which are possibly crawled from news website. Those sentences are generally too hard for beginners. Which motivate me to build my own Japanese dictionary that can recommend rich and easy sample sentences for beginners.
- Build my own Japanese dictionary in python, which is a combination of web crawler, NLP and Japanese languages skills.
- Implement a new sentences recommending strategy incorporating the idea of ranking the sentences by the 'complexity' , which is calculated on the length and the word frequency of the sentences.

Bachelor Thesis Project

HUST, Wuhan, China

A SEARCH ENGINE PROTOTYPE FROM SCRATCH

Feb 2012 - May 2012

- Build a search engine from scratch and delve into the inner details of a search engine, like building a web page crawler, setting up reverse index for docs, designing page-rank strategies, preparing page digest as well as showing the results via web interface.
- Support alternate page-ranking strategies, including TF/IDF, PageRank, LSA, etc

Skills

Programming C/C++, Python, JAVA, Bash, Javascript

Web Node.js, Spring with Java, Mysql, HTML

Others Linux Kernel Hacking, ARM Binary Rewriting, Android App Dev., Git, Latex, Trusted Application Dev.