

# Yaohui Chen

---

College of Computer and Information Science  
Northeastern University  
Boston, MA, 02115

**Mobile:** (631)681-8706  
**E-mail:** yaohway@ccs.neu.edu

---

## Education

- 2017 - 2019 **Ph.D.**, *College of Computer and Information Science*, Northeastern University, Boston, MA, Advisor: Prof. Long Lu.
- 2014 - 2017 **Ph.D.**, *Department of Computer Science*, Stony Brook University (transferred to Northeastern University), Stony Brook, NY, Advisor: Prof. Long Lu.  
GPA:3.90/4.00
- 2013 - 2013 **Exchange Student**, Polytechnic University of Catalonia, Barcelona, Spain.
- 2010 - 2014 **B.Sc.**, *Department of Computer Science*, Tongji University, Shanghai, China.

---

## Research Interests

My research interests mainly include **Bug Finding Automation, Program Analysis, Binary Exploit Mitigations, Virtualization, Operating System and Mobile Security**.

---

## Publications

**SAVIOR: Towards Bug-Driven Hybrid Testing**, Yaohui Chen, Peng Li, Jun Xu, Shengjian Guo, Rundong Zhou, Yulong Zhang, Taowei, Long Lu, In the proceeding of the 41th IEEE Symposium on Security and Privacy (Oakland'20).

**FUDGE: Fuzz Driver Generation at Scale**, Domagoj Babic, Stefan Bucur, Yaohui Chen, Franjo Ivancic, Tim King, Markus Kusano, Caroline Lemieux, Laszlo Szekeres and Wei Wang, In the proceeding of The ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE'19), (*Best Paper Award*).

**Pttrix: Efficient Hardware-Assisted Fuzzing for COTS Binary**, Yaohui Chen, Dongliang Mu, Zhichuang Sun, Jun Xu, Wenguo Shen, Xinyu Xing, Long Lu, Bing Mao, In Proceedings of the 14th ACM on Asia Conference on Computer and Communications Security (AsiaCCS'19).

**Compiler-assisted Code Randomization**, Hyungjoon Koo, Yaohui Chen, Long Lu, Vasileios P. Kemerlis, Michalis Polychronakis, In the proceeding of the 39th IEEE Symposium on Security and Privacy (Oakland'18), (*Final list, CSAW 2018*).

**InstaGuard: Instantly Deployable Hot-patches for Vulnerable System Programs on Android**, Yaohui Chen, Yuping Li, Long Lu, Yueh-Hsun Lin, Hayawardh Vijayakumar, Zhi Wang, Xinming Ou, In Proceedings of the 2018 Network and Distributed System Security Symposium (NDSS'18).

**Norax: Enabling Execute-Only Memory for COTS Binaries on AArch64**, **Yaohui Chen**, Dongli Zhang, Ruowen Wang, Rui Qiao, Ahmed Azab, Long Lu, Haywardh Vijayakumar, Wenbo Shen, In the proceeding of the 38th IEEE Symposium on Security and Privacy (Oakland'17), (*Third Place of Best Paper Award in Applied Cyber Security Research, CSAW 2017*).

**Secure Integration of Web Content and Applications on Commodity Mobile Operating Systems**, Drew Davidson, **Yaohui Chen**, Franklin George, Long Lu, Somesh Jha, In Proceedings of the 12th ACM on Asia Conference on Computer and Communications Security (AsiaCCS'17).

**Shreds: Fine-grained Execution Units with Private Memory**, **Yaohui Chen**, Sebassujeen Reymondjohnson, Zhichuang Sun, Long Lu, In the proceeding of the 37th IEEE Symposium on Security and Privacy (Oakland'16).

---

## Experiences

- Dec. 2019 - present - **Research Scientist**, *Infrastructure Security Team*, Facebook.
- May. 2017 - Oct. 2019 - **Research Assistant**, *RiS3 Lab*, Northeastern University.
- Sep. 2018 - Dec. 2018 - **Research Intern**, *Software Analysis Team*, Google.
- June. 2018 - Aug. 2018 - **Research Intern**, *System Security and Privacy Research*, Microsoft Research.
- Feb. 2018 - May. 2018 - **Research Intern**, *X-Lab*, Baidu USA.
- May. 2017 - Sep. 2017 - **Research Intern**, *B2B Lab*, Samsung Research America.
- May. 2016 - Sep. 2016 - **Research Intern**, *B2B Lab*, Samsung Research America.
- Aug. 2014 - May. 2017 - **Research Assistant**, *RiS3 Lab*, Stony Brook University.

---

## Research Projects

- Sep. 2018 - Dec. 2018 - **Automatic fuzz testing harness generation.**
- Jointly designed harness generation based on unit-test dynamic tracing and AST slicing.
  - Studied and compared different internal tracing services.
  - Worked in a multi-team collaboration to extend a company-wide tracing service.
  - Integrated the dynamic trace generation component into harness generation pipeline.
- June. 2018 - Aug. 2018 - **Hyper-V hypervisor coverage feedback-guided fuzz testing.**

- Studied the existing automatic testing solutions for Hyper-V hypervisor.
- Designed and implemented code coverage guided fuzzer for Hyper-V hypervisor.
- The end-to-end solution involved Intel-PT virtualization support for hardware tracing.
- Discovered 3 real bugs in the newest Hyper-V hypervisor and they have been fixed.
- The solution has been adopted into Hyper-V hypervisor testing process before release.

Feb. 2018 - **Bug-driven hybrid fuzz testing.**  
present

- Studied the inefficiency of current code coverage guided hybrid fuzzing solutions.
- Designed and implemented bug-coverage based hybrid fuzzing based on LLVM domination analysis and sanitizer instrumentation.
- Added C++ support for KLEE with GNU libstd-C++.
- Found over 2,000 unique sanitizer violations in 14 real-world open-source programs.
- Scaled the system up using Kubernetes and found numerous security bugs in Baidu's Apollo Auto-driving platform.

May. 2017 - **Harnessing Efficiency of Fuzzing and Soundness of Symbolic Execution.**  
present

- Studied the inefficiency of symbolic execution and unsoundness of fuzzing.
- Modified KLEE to support on-demand symbolic execution.
- Developed light-weight static analysis to guide symbolic execution.
- Developed infrastructure to coordinate KLEE, AFL and static analysis components.
- Evaluated the framework on real-world programs including ARM TrustZone TAs, commonly fuzzed applications and showed it out-performed the state-of-the-art.

May. 2017 - **Enabling Whole-process COTS Binary Fuzzing with Near-native Speed.**  
April. 2019

- Identified limitations of the state-of-the-art grey-box fuzzing solution when fuzzing binary-only programs.
- Designed practical framework to integrate Intel Processor Trace into AFL.
- Modified Glibc loader to support fork-server mode.
- Developed customized Intel PT kernel module driver for efficient online target tracing.
- Integrated the framework to AFL, dubbed PT mode.
- Evaluated on real-world benchmark programs and found dozens of new bugs.

May. 2016 - **Scalable Fine-grained Randomization Solution for ELF Binaries on x86-64.**  
Jan. 2018

- Systematically studied the adoption resistance facing all existing fine-grained randomization solutions and identified reliability and scalability are the key factors.
- Jointly devised the design consist of full toolchain including compiler and static linker as well as an offline randomizer.
- Extensively modified GNU Gold linker to aggregate the minimum per-object binary layout information.
- Performed rigorous evaluation on randomizing all SPEC2006 binaries and several large real-world applications including NGINX, Putty and OpenSSH.

May. 2016 - **Practical Policy-Driven Patching Solution for Android Mobile System.**

May. 2017

- Investigated the reasons behind the status quo of the always belated Android system security patches.
- Designed and implemented a full-package patching solution, which provides the quick direct patching ability for the phone vendors.
- The solution includes a front-end policy configuration compiler as well as a policy-driven backend features OS-backed security primitives such as hardware breakpoint and watchpoint and process runtime acts as assertion verification engine.

Jun. 2016 - **Enabling Execute-Only Memory for COTS Binaries on AArch64.**

Dec. 2016

- Explored and showcased the feasibility of enforcing Execute-only memory permission in AArch64 Based System.
- Developed binary analysis and binary rewriting engine based on AArch64-Objdump to rewrite 64-bit Android system COTS binaries to be execute-only friendly.
- Developed corresponding kernel module and modified Bionic dynamic linker to support the rewritten binaries to run in execute-only mode
- Performed large-scale evaluation on system binaries extracted from commodity Android phone Nexus5X, including proprietary Qualcomm drivers, common system libraries such as libm, libc, etc

May 2015 - **Fine-grained Memory Access Control for Sub-process Execution Units.**

May 2016

- Surveyed the needs of fine grained memory access control for preventing In-process memory abuse and related works.
- Retrofitted ARM memory domain-based protection into Linux kernel, in particular, the task scheduler, meta-data bookkeeper and memory manager.
- Created new user-space programing primitives.
- Extended Clang-LLVM by adding the compilation passes for analyzing and instrumenting programs that use the new primitives, enforcing both control flow and data flow properties.

Aug. 2014 - **Secure WebView on Android.**

Mar. 2015

- Conducted a comprehensive security analysis on the design of WebView, the fundamental mechanism for embedding Web content into Android apps.
- Studied the root cause of its security design flaw and co-implemented the POC attacks
- Built prototype system to address the problem of mutually untrusted relationship between Web and App

---

## Honors and Awards

2019 **Best Paper Award**, ACM ESEC/FSE.

2019 **Google Fellowship Nomination**, Northeastern University.

2018 **RSA Scholarship**, *RSA Conference 2018*, U.S.A.

2017 **Best Paper Award**, CSAW, U.S.A.

2014 **Chair Fellowship**, *Department of Computer Science*, Stony Brook University.

2013 **Exchange Student Scholarship**, *Department of Computer Science*, Tongji University.

☎ (631)681-8706 • ✉ [yaohway@ccs.neu.edu](mailto:yaohway@ccs.neu.edu)

🌐 [www.ccs.neu.edu/home/yaohway/](http://www.ccs.neu.edu/home/yaohway/)

2012 **Second-Class Scholarship**, *Department of Computer Science*, Tongji University.

## Professional Skills

OS **Linux, Android, Windows.**  
Programming **C, C++, Java, Python, System-verilog, ARM/x86/Sparc/MIPS assembly.**  
Compiler **Clang, LLVM.**  
Misc **Kubernetes, Reverse Engineering, Program Analysis, ELF Binary Linking  
Loading Toolchain.**