# 陈泓旭

网络安全, 软件工程

hongxu_chen@foxmail.com
HongxuChen
hongxu-chen-ntu

## 工作经历

2020.10 至今 **华为**, 主任工程师

以天才少年身份加入华为新加坡研究所，于 2021 年 7 月调回 2012 实验室-可信实验室 (深圳)。

1. 研究华为软件实现和软件设计中一致性看护能力，通过软件设计中的安全性、可维护性规约识别设计架构中接口和实现的质量腐化问题。在此期间我带领团队实现了代码和架构一致性看护平台 *TENET*，通过自研 C/C++、Java 架构逆向引擎，识别代码实现中的关键架构元素，并结合规约完成一致性检查；相关能力已落地华为终端 BG、海思、车 BU 等产业。
2. 基于前述 TENET 工作，进行代码分析的数字化服务项目研究，完成 C/C++、Java、ArkTS 的代码知识图谱的设计和实现。在技术上攻关单仓 3000w+ 的 C/C++ 源代码级精准分析能力。该项目已孵化形成①代码质量度量和架构异味识别引擎用于 Clean Code L3 检查的 IDE 端和版本级检查平台 CleanArch，落地于公司 13 个产业的 80+ 个业务；②基于代码知识图谱和 LLM 的精准代码文档生成和智能问答的 Web 端类 deepwiki 服务，已完成对公司内 410+ 存量代码仓的分析。
3. 研究软件缺陷和漏洞、缺陷代码测试集、检查工具的映射关系，建立类 CWE 的代码缺陷字典，通过对软件设计、编码、代码 review、静态检查、DT 测试等软件开发过程进行系统性分析，形成基于数据驱动的代码缺陷主动防御体系。该工作正联合华为公司数通、光、终端 BG 等主要产业进行能力共建，目前着重解决内存安全类缺陷问题。

2019.08-2020.9 **南洋理工大学**, *Research Fellow*

扩展了自研模糊测试框架 FOT, 项目主页https://sites.google.com/view/fot-the-fuzzer，①增强了其对结构化输入的支持，提升了测试用例生成的合法性；②对多线程分析场景下提供了模糊测试方案 MUZZ，提升了非顺序执行场景下的模糊测试有效性。同时进行的项目包括高性能跨 CPU 二进制模糊测试框架 BiFF，完成了在 ARM、x86 及 RISCV 下仅二进制场景下的高效 fuzz，相关工作已落地 Continental 渗透测试。

2014.05-2015.08 **南洋理工大学**, *Research Associate*

基于 LLVM 的数据流分析, 该项目主要为了精化数据流分析来指导动态测试的有效性。

2013.02-2013.11 **微软亚洲研究院**, 研究实习生

通过静态分析提高白盒测试程序补丁的有效性; 实现了对补丁程序切片静态代码分析工具, 使得被切片后的程序可以有效地用于白盒测试，相关工作成为 SRG 组内研究成果。

## 教育经历

2015.08-2019.07 **博士**, 南洋理工大学, 计算机科学与技术, 网络安全实验室, 导师: LIU Yang 教授

主要关注移动系统安全和软件的实现安全:

- 系统安全: 利用类型系统验证依赖于权限的信息流安全, 该类型系统主要对 Android 系统的 App 之间的交互进行建模, 我设计了该类型系统并完成对系统健壮性的形式化验证。
- 软件安全: 从事对 C/C++ 程序进行模糊测试的研究, 主要思路为利用程序分析的方法来提高模糊测试的有效性。

2011.09-2014.03 **硕士**, 上海交通大学, 计算机科学与技术, 高可靠软件实验室, 导师: 赵建军教授

关注基于程序分析的软件可靠性研究, 包括基于 LLVM 的 Andersen 指针分析和程序切片，基于 KLEE 的符号执行优化，基于 SOOT 框架的单元测试有效性分析等。

2007.09-2011.07 **本科**, 南京理工大学, 信息与计算科学

## 科研项目

FOT 2017.07-2020.09 主导开发并维护模糊测试框架 *FOT*, 该框架由 Rust 编写，强调使用静态分析来指导模糊测试。FOT 已经检测了 100+ 开源软件并从其中找到了 300+ 漏洞, 61 个被赋予 CVE 编号, 这包括 GNU libc, FFmpeg, ImageMagick 等知名开源项目中的 10 个严重或高危漏洞。具体漏洞详见https://github.com/fot-the-fuzzer/pocs. FOT 获 NASAC2017 原型竞赛 (命题型) 一等奖, 并被 CCF-A 类会议 ESEC/FSE 2018 接受。基于该框架的 Hawkeye 和 Cerebro 分别被 CCF-A 类会议 CCS 2018 和 ESEC/FSE 2019 接受。

BiFF 2018.11-2020.09 参与开发高性能跨 *CPU* 模糊测试框架 *BiFF*, 该框架致力于改进现有二进制模糊测试技术, 使用轻量级的 hooking 技术及对 "服务型" 程序的测试流程优化, 提高对不同 CPU 下 IoT 设备模糊测试的有效性。该框架获得 NASAC2019 原型竞赛 (自由型) 一等奖。

MUZZ 2018.07-2019.07 设计并实现了多线程场景下的模糊测试技术 *MUZZ*，结合传统静态分析技术实现了面向多线程下覆盖率的插桩、记录多线程上下文的插桩和用于干预多线程调度器的插桩，并在动态模糊测试过程中提出了针对多线程环境的种子选择策略和自适应重复执行策略，提升了模糊测试的有效性和优效性。

Hawkeye 2017.12-2018.05 设计并提出导向性模糊测试技术 Hawkeye, 指出了导向性模糊测试的 4 个属性及解决方案, 并用实验论证了有效性。该技术被 CCF-A 类会议 CCS 2018 接受。

STAndroid 2015.08-2017.06 该项目立足于 Android 系统的权限系统, 利用类型系统验证依赖于权限的信息流安全; 我设计并完成了对类型系统健壮性的形式化验证, 并实现了基于此的信息泄露检测工具原型。该工作被 CCF-B 类会议 CSF 2018 接受。

RBScope 2013.02-2013.11 该项目关注利用静态分析的方法加强对新程序补丁处的符号执行; 主要思想是利用程序切片的方法去除和补丁不相关的程序片段, 从而使测试关注于和补丁相关部分并减小测试状态空间爆炸问题。我实现了基于 LLVM 的 Andersen 指针分析算法和对补丁的程序切片。

## 技能

精通 静态分析, 模糊测试, 符号执行, LLVM/Clang, C/C++, Java, Python, Rust, Bash, Lua

熟练 程序语言理论, 编译原理, 形式化验证, 二进制安全, Linux 编程, JVM, SMT 约束求解

了解 Go, Kotlin, OCaml, Haskell, Coq, Isabelle

## 助教经历

面向对象设计编程 2018 年秋学期 负责面向对象设计与编程 (Object Oriented Design and Programming, CE/CZ2002) 实验设计、答疑及批改。

软件工程 2018 年春学期 负责软件工程 (Software Engineering, CE/CZ2006) 实验指导、答疑及批改。

软件系统分析设计 2017 年秋学期 负责软件系统分析与设计 (Software Systems Analysis and Design, CE/CZ3003) 实验设计及答疑。

计算机安全 2017 年秋学期 负责计算机安全 (Computer Security, CE/CZ4062) 课程设计及批改。

密码学与网络安全 2017 年春学期 负责密码学与网络安全 (Cryptography and Network Security, CE/CZ4024) 课程作业设计及批改。

数据结构与算法 2016 年秋学期 负责数据结构与算法 (Algorithms, CE/CZ2001) 实验设计、答疑及批改。

编译技术 2016 年春学期 负责编译技术 (Compiler Techniques, CE/CZ3007) 实验设计、答疑及批改。

## 论文及获奖

**Hongxu Chen**, Shengjian Guo, Yinxing Xue, Yulei Sui, Cen Zhang, Yuekang Li, Haijun Wang, and Yang Liu. MUZZ : Thread-aware grey-box fuzzing for effective bug hunting in multithreaded programs. In *USENIX Security' 20, CCF-A, 网络与信息安全*, 2019.

**Hongxu Chen**, Yinxing Xue, Yuekang Li, Bihuan Chen, Xiaofei Xie, Xiuheng Wu, and Yang Liu. Hawkeye: Towards a desired directed grey-box fuzzing. In *CCS' 18 (CCF-A, 网络与信息安全)*, pages 2095–2108. ACM, 2018.

**Hongxu Chen**, Yuekang Li, Bihuan Chen, Yinxing Xue, and Yang Liu. FOT: A versatile, configurable, extensible fuzzing framework. In *ESEC/FSE '18 (CCF-A, 软件工程/系统软件)*, pages 867–870, 2018.

**Hongxu Chen**, Alwen Tiu, Zhiwu Xu, and Yang Liu. A permission-dependent type system for secure information flow analysis. In *CSF '18 (CCF-B, 网络与信息安全)*, pages 218–232. IEEE, 2018.

**Hongxu Chen**, Yuekang Li, Junjie Wang, Bihuan Chen, and Yang Liu. FOT: Fuzzing orchestration toolkit. In *NASAC 2017 原型竞赛一等奖*, 2017.

Wuxia Jin, Shuo Xu, Dawei Chen, Jiajun He, Dinghong Zhong, Ming Fan, **Hongxu Chen**, Huijia Zhang, and Ting Liu. Pyanalyzer: An effective and practical approach for dependency extraction from python code. In *ICSE'24 CCF-A, 软件工程/系统软件*, ICSE '24, New York, NY, USA, 2024. Association for Computing Machinery.

Yiran Zhang, Zhengzi Xu, Chengwei Liu, **Hongxu Chen**, Jianwen Sun, Dong Qiu, and Yang Liu. Software architecture recovery with information fusion. In *ESEC/FSE'23, CCF-A, 软件工程/系统软件*, ESEC/FSE 2023, page 1535 – 1547, New York, NY, USA, 2023. Association for Computing Machinery.

Can Yang, Zhengzi Xu, **Hongxu Chen**, Yang Liu, Xiaorui Gong, and Baoxu Liu. Modx: binary level partially imported third-party library detection via program modularization and semantic matching. In *ICSE'22 CCF-A, 软件工程/系统软件*, ICSE '22, page 1393–1405, New York, NY, USA, 2022. Association for Computing Machinery.

Cheng Wen, Haijun Wang, Yuekang Li, Shengchao Qin, Yang Liu, Zhiwu Xu, **Hongxu Chen**, Xiaofei Xie, Geguang Pu, and Ting Liu. Memlock: Memory usage guided fuzzing. In *ICSE '20 (CCF-A, 软件工程/系统软件)*, 2020.

Haijun Wang, Xiaofei Xie, Yi Li, Cheng Wen, Yang Liu, Shengchao Qin, **Hongxu Chen**, and Yulei Sui. Typestate-guided fuzzer for discovering use-after-free vulnerabilities. In *ICSE '20 (CCF-A, 软件工程/系统软件)*, 2020.

Cen Zhang, Yuekang Li, **Hongxu Chen**, Nguyen Anh Quynh, and Yang Liu. Biff: An effective binary fuzzing framework with cross-architecture support. In *NASAC 2019 原型竞赛一等奖*, 2019.

Xiaofei Xie, **Hongxu Chen**, Yi Li, Ma Lei, Yang Liu, and Jianjun Zhao. Deephunter: A coverage-guided fuzzer for deep neural networks. In *ASE '19 (CCF-A, 软件工程/系统软件)*. IEEE, 2019.

Yuekang Li, Yinxing Xue, **Hongxu Chen**, Xiuheng Wu, Cen Zhang, Xiaofei Xie, Haijun Wang, and Yang Liu. Cerebro: Context-aware adaptive fuzzing for effective vulnerability detection. In *ESEC/FSE '19 (CCF-A, 软件工程/系统软件)*, pages 533–544. ACM, 2019.

Xiaofei Xie, Lei Ma, Felix Juefei-Xu, Minhui Xue, **Hongxu Chen**, Yang Liu, Jianjun Zhao, Bo Li, Jianxiong Yin, and Simon See. Deephunter: A coverage-guided fuzz testing framework for deep neural networks. In *ISSTA '19 (CCF-A, 软件工程/系统软件)*, pages 146–157. ACM, 2019.

Yinxing Xue, Guozhu Meng, Yang Liu, Tian Huat Tan, **Hongxu Chen**, Jun Sun, and Jie Zhang. Auditing anti-malware tools by evolving android malware and dynamic loading technique. *TIFS' 17 (CCF-A, 网络与信息安全)*, 12(7):1529–1544, 2017.

Xiaofei Xie, Yang Liu, Wei Le, Xiaohong Li, and **Hongxu Chen**. S-looper: automatic summarization for multipath string loops. In *ISSTA '15 (CCF-A, 软件工程/系统软件)*, pages 188–198. ACM, 2015.