Wen Xu

Postdoctoral Fellow
School of Computer Science
Georgia Institute of Technology
756 West Peachtree Street NW
Atlanta, GA 30332-4016

Email: wen.xu@gatech.edu

Employment

Georgia Institute of Technology, Atlanta, GA ..... August 2021–Present
Postdoctoral Fellow

Georgia Institute of Technology, Atlanta, GA ..... August 2016–July 2021
Research Assistant
Advisor: Dr. Taesoo Kim

Microsoft, Redmond, WA ..... May 2020–July 2020
Software Security Engineer Intern
Offensive Security Research (OSR) Team

Microsoft, Redmond, WA ..... May 2019–July 2019
Software Security Engineer Intern
Offensive Security Research (OSR) Team

Microsoft Research, Redmond, WA ..... May 2017–August 2017
Research Intern
Advisor: Marcus Peinado

Singapore Management University, Singapore ..... August 2015–February 2016
Research Assistant
Advisor: Dr. Xuhua Ding

Tencent KeenLab (previously Keen Team), Shanghai, China ..... July 2014–June 2016
Security Research Intern

Education

Georgia Institute of Technology, Atlanta, GA ..... August 2016–July 2021
Ph.D. in Computer Science
Advisor: Dr. Taesoo Kim

Shanghai Jiao Tong University, Shanghai, China .....September 2012–June 2016
B.S.E. in Computer Science
ACM Honored Class

Research Interests

Fuzzing, Systems Security

Publications

Conference Proceedings

[1] **Hardware Support to Improve Fuzzing Performance and Precision**.
Ren Ding, Yonghae Kim, Fan Sang, **Wen Xu**, Gururaj Saileshwar, and Taesoo Kim.
In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, November 2021.

[2] **FREEDOM: Engineering a State-of-the-Art DOM Fuzzer**.
Wen Xu, Soyeon Park, and Taesoo Kim.
In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, November 2020.

[3] **Fuzzing JavaScript Engines with Aspect-preserving Mutation**.
Soyeon Park, **Wen Xu**, Insu Yun, Daehee Jang, and Taesoo Kim.
In *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*, May 2020.

[4] **DESENSITIZATION: Privacy-Aware and Attack-Preserving Crash Report**.
Ren Ding, Hong Hu, **Wen Xu**, and Taesoo Kim.
In *Proceedings of the Annual Network and Distributed System Security Symposium (NDSS)*, February 2020.

[5] **Finding Semantic Bugs in File Systems with an Extensible Fuzzing Framework**.
Seulbae Kim, Meng Xu, Sanidhya Kashyap, Jungyeon Yoon, **Wen Xu**, and Taesoo Kim.
In *Proceedings of the ACM Symposium on Operating Systems Principles (SOSP)*, October 2019.

[6] **libmpk: Software Abstraction for Intel Memory Protection Keys (Intel MPK)**.
Soyeon Park, Sangho Lee, **Wen Xu**, Hyungon Moon, and Taesoo Kim.
In *Proceedings of the USENIX Annual Technical Conference (ATC)*, July 2019.

[7] **Fuzzing File Systems via Two-Dimensional Input Space Exploration**.
Wen Xu, Hyungon Moon, Sanidhya Kashyap, Po-Ning Tseng, and Taesoo Kim.
In *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*, May 2019.

[8] **Designing New Operating Primitives to Improve Fuzzing Performance**.
Wen Xu, Sanidhya Kashyap, Changwoo Min, and Taesoo Kim.
In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, October–November 2017.

[9] **Seeing Through The Same Lens: Introspecting Guest Address Space At Native Speed**.
Siqi Zhao, Xuhua Ding, **Wen Xu**, and Dawu Gu.
In *Proceedings of the USENIX Security Symposium (Security)*, August 2017.

[10] **CAB-Fuzz: Practical Concolic Testing Techniques for COTS Operating Systems**.
Su Yong Kim, Sangho Lee, Insu Yun, **Wen Xu**, Byoungyoung Lee, Youngtae Yun, and Taesoo Kim.
In *Proceedings of the USENIX Annual Technical Conference (ATC)*, July 2017.

[11] **From Collision To Exploitation: Unleashing Use-After-Free Vulnerabilities in Linux Kernel**.
Wen Xu, Juanru Li, Junliang Shu, Wenbo Yang, Tianyi Xie, Yuanyuan Zhang, and Dawu Gu.
In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, October 2015.

[12] **Own Your Android! Yet Another Universal Root**.
Wen Xu and Yubin Fu.
In *Proceedings of the USENIX Workshop on Offensive Technologies (WOOT)*, August 2015.

[13] **Ah! Universal Android Rooting Is Back**.
Wen Xu.
In *Black Hat USA Briefings*, August 2015.

[14] **Sheriff: A Regional Pre-Alert Management Scheme in Data Center Networks**.
Xiaofeng Gao, **Wen Xu**, Fan Wu, and Guihai Chen.
In *Proceedings of the International Conference on Parallel Processing (ICPP)*, September 2015.

Journal Articles

[15] **Finding Bugs in File Systems with an Extensible Fuzzing Framework**.
Seulbae Kim, Meng Xu, Sanidhya Kashyap, Jungyeon Yoon, **Wen Xu**, and Taesoo Kim.
ACM Transactions on Storage (ToS), May 2020.

Presentations

An Advanced and Extensive Fuzzing Framework for File System Testing
Google, Sunnyvale, CA ..... July 2019

Fuzzing File Systems via Two-Dimensional Input Space Exploration
KAIST, South Korea ..... April 2019

Comprehensive Browser Fuzzing: From DOM to JS
w/ Soyeon Park, ZeroCon 2019, South Korea ..... April 2019

The Road of Growth of 0ops Team
Shanghai, China ..... April 2016

From Collision To Exploitation: Unleashing Use-After-Free Vulnerabilities in Linux Kernel
Nanyang Technological University, Singapore ..... November 2015

Root Hundreds of Thousands of Android Devices with One Generic Exploit
HITB GSEC, Singapore ..... October 2015

Professional Service

Journal Reviewing Activities

IEEE Transactions on Very Large Scale Integration Systems (TVLSI) 2021
IEEE Transactions on Dependable and Secure Computing (TDSC) 2021
Jordanian Journal of Computers and Information Technology (JJCIT) 2021

Teaching Experience

Lecturer, Information Security Lab (CS6265, Georgia Tech), Fall 2021

Teaching Assistant, Information Security Lab (CS6265, Georgia Tech), Fall 2018

Teaching Assistant, Information Security Lab (CS6265, Georgia Tech), Fall 2016

Honors and Awards

Pwn2own

- Pwn2own 2016 Microsoft Edge Winner (Tencent KeenLab) 2016
- Pwn2own 2016 Master of Pwn (Tencent KeenLab) 2016
- Pwn2own 2015 Adobe PDF Reader Winner (KeenTeam) 2015

Capture-The-Flag (CTF)

- 8th place (r00timentary) at DEFCON CTF 2019 2019
- **1st place** (DEFKOR00T) at DEFCON CTF 2018 2018
- 3rd place (a*0*e) at DEFCON CTF 2017 2017
- 2nd place (b1o0p) at DEFCON CTF 2016 2016
- 5th place (0ops) at Belluminar 2015 2015
- 6th place (0ops) at DEFCON CTF 2015 2015
- 5th (0ops) at PlaidCTF 2015 2015
- **1st place** (0ops) at CodeGate CTF 2015 2015
- 6th (0ops) at BCTF 2015 2015
- 6th (0ops) at Ghost in the Shellcode 2015 2015
- 2nd (0ops) at Hack.lu CTF 2014 2014
- 6th (0ops) at HITCON CTF 2014 2014

Miscellaneous

- Pwnie Award nominee (PingPong Root/CVE-2015-3636) 2015
- The Outstanding Undergraduate Award from China Computer Federation (CCF) 2016

Public and Community Service

Organizer of 0CTF Hacking Competition (DEFCON CTF pre-qualifier since 2016) 2014-2018

Co-founder of 0ops CTF Team 2013

Reported Software Vulnerabilities

Apple

- **Safari (WebKit)**: CVE-2019-6212, CVE-2019-8562 (w/ Hanqing Zhao), CVE-2019-8596, CVE-2019-8609, CVE-2019-8619 (w/ Hanqing Zhao), CVE-2019-8628 (w /Hanqing Zhao), CVE-2019-8673 (w/ Soyeon Park), CVE-2019-8676 (w/ Soyeon Park), CVE-2019-8720, CVE-2019-9803, CVE-2019-9806, CVE-2019-9807
- **macOS/iOS Kernel**: CVE-2019-8786

Google

- **Chrome**: CVE-2016-1646 ($7.5K), CVE-2019-5806 ($3K), CVE-2019-5817 ($1K), Issue 943424 ($3K), Issue 943538 ($3K), CVE-2019-13730 ($5K, w/ Soyeon Park), CVE-2019-13764 ($5K, w/ Soyeon Park), CVE-2020-6382 ($2K, w/ Soyeon Park)
- **Android**: CVE-2015-6612 (w/ Qidan He)

Microsoft

• **Script engine (ChakraCore)**: CVE-2016-0193 (w/ Zhen Feng), CVE-2019-0609 (w/ Soyeon Park), CVE-2019-1023 (w/ Soyeon Park)

Mozilla

• **Firefox**: Issue 1626152 ($4K)

Linux Kernel

• **ext4**: CVE-2018-1092, CVE-2018-1093, CVE-2018-1094, CVE-2018-1095, CVE-2018-10840, CVE-2018-10876, CVE-2018-10877, CVE-2018-10878, CVE-2018-10879, CVE-2018-10880, CVE-2018-10881, CVE-2018-10882, CVE-2018-10883

• **Btrfs**: CVE-2018-14609, CVE-2018-14610, CVE-2018-14611, CVE-2018-14612, CVE-2018-14613

• **XFS**: CVE-2018-10322, CVE-2018-10323, CVE-2018-13093, CVE-2018-13094, CVE-2018-13095

• **F2FS**: CVE-2018-13096, CVE-2018-13097, CVE-2018-13098, CVE-2018-13099, CVE-2018-13100, CVE-2018-14614, CVE-2018-14615, CVE-2018-14616

• **HFS+**: CVE-2018-14617

• **Network**: CVE-2015-3636 (w/ Shi Wu)

Qualcomm

• **Camera drivers**: CVE-2014-0975, CVE-2014-0976, CVE-2014-4321, CVE-2014-4324, CVE-2014-9410 (w/ Sen Nie, Shi Wu and Liang Chen)

Last updated: February 25, 2022