

Fengwei Zhang

Wayne State University
5057 Woodward Avenue, Suite 3010
Detroit, Michigan 48202
☎ +1 (313) 577-1648
✉ fengwei@wayne.edu
🌐 <http://fengwei.me>

Research Interest

My primary research interests are in the areas of systems security, with a focus on hardware-assisted security, trustworthy execution environments, mobile malware analysis, tracing and debugging transparency, transportation security, system integrity checking, and plausible deniability encryption.

Education

- 08/2010–04/2015 **Ph.D. in Computer Science**, *George Mason University, Department of Computer Science, Volgenau School of Engineering*, Fairfax, VA, USA.
Thesis: Using Hardware Isolated Execution Environments for Securing Systems
Advisor: Prof. Angelos Stavrou
- 08/2008–05/2010 **M.S. in Computer Science**, *Columbia University, Department of Computer Science, Fu Foundation School of Engineering and Applied Science*, New York, NY, USA.
Computer Security Track
Advisor: Prof. Salvatore J. Stolfo
- 08/2006–05/2008 **B.S. in Computer Science**, *Southern Polytechnic State University, Department of Computer Science, School of Computing and Software Engineering*, Marietta, GA, USA.
2+2 Dual Bachelor Program
Honor Thesis: Information Security Metrics
Advisor: Prof. Andy Ju An Wang
- 09/2004–07/2008 **B.S. in Computer Science**, *North China University of Technology, Department of Computer Science, College of Information Engineering*, Beijing, China.
2+2 Dual Bachelor Program

Employment History

- 08/2015–present **Assistant Professor**, *Department of Computer Science, Wayne State University*, Detroit, Michigan, USA.
- 01/2014–01/2015 **Research Assistant**, *Center for Assurance Research & Engineering, George Mason University*, Fairfax, VA, USA.
- 08/2011–01/2014 **Research Assistant**, *Center for Secure Information Systems, George Mason University*, Fairfax, VA, USA.
- 05/2011–08/2011 **Research Intern**, *Advanced Technology Center, Microsoft Corporation*, Beijing, China.
- 08/2010–05/2011 **Teaching Assistant**, *Department of Computer Science, George Mason University*, Fairfax, VA, USA.
- 01/2008–05/2008 **Lab Administrator**, *School of Computing and Software Engineering, Southern Polytechnic State University*, Marietta, GA, USA.

Funding Support

- Co-PI, NSF "S&AS:INT: Autonomous Battery Operating System (ABOS): An Adaptive & Comprehensive Approach to Efficient, Safe, & Secure Battery System Management", (With Nathan Fisher, Daniel Grosu, and Weisong Shi), **\$1,249,998**, (09/2017 - 08/2021).
- Co-PI, NSF "CICI:RSARC:Infrastructure Support for Securing Large-Scale Scientific Workflows", (With Shiyong Lu), **\$499,785**, (09/2017 - 08/2020).

Publications

Patents

- 15/173,462 **Fengwei Zhang**, Kevin Leach, Angelos Stavrou, and Haining Wang. Methods and Systems for Increased Debugging Transparency. Filed on June 03, 2016, Under U.S. Patent Application Number 15/173,462.

Refereed Conference and Workshop Proceedings

- SEC EdgeSP'18 Zhenyu Ning, Jinghui Liao, **Fengwei Zhang**, and Weisong Shi. Preliminary Study of Trusted Execution Environments on Heterogeneous Edge Platforms. To appear in The *1st ACM/IEEE Workshop on Security and Privacy in Edge Computing*, In conjunction with The *3rd ACM/IEEE Symposium on Edge Computing (SEC'18)*, Bellevue, Washington, October, 2018.
- ISCA HASP'18 Saeid Mofrad, **Fengwei Zhang**, Shiyong Lu, and Weidong Shi. A Comparison Study of Intel SGX and AMD Memory Encryption Technology. In Proceedings of The *Hardware and Architectural Support for Security and Privacy*, In conjunction with The *45th International Symposium on Computer Architecture (ISCA'18)*, Los Angeles, California, June, 2018.
- DSN'18 Zhenyu Ning and **Fengwei Zhang**. DexLego: Reassembleable Bytecode Extraction for Aiding Static Analysis. In Proceedings of The *48th IEEE/IFIP International Conference on Dependable Systems and Networks*, Luxembourg, June, 2018. [Acceptance rate: 26%]
- DSN'18 Bing Chang, **Fengwei Zhang**, Bo Chen, Yingjiu Li, Wen-Tao Zhu, Yangguang Tian, Zhan Wang, Albert Ching. MobiCeal: Towards Secure and Practical Plausibly Deniable Encryption on Mobile Devices. In Proceedings of The *48th IEEE/IFIP International Conference on Dependable Systems and Networks*, Luxembourg, June, 2018. [Acceptance rate: 26%]
- ACSAC'17 Le Guan, Shijie Jia, Bo Chen, **Fengwei Zhang**, Bo Luo, Jingqiang Lin, Peng Liu, Xinyu Xing and Luning Xia. Supporting Transparent Snapshot for Bare-metal Malware Analysis on Mobile Devices. In Proceedings of The *33rd Annual Computer Security Applications Conference*, San Juan, Puerto Rico, December, 2017. **Distinguished Paper Award**. [Acceptance rate: 19%]
- RAID'17 Kevin Leach, **Fengwei Zhang**, and Westley Weimer. Scotch: Combining Software Guard Extensions and System Management Mode to Monitor Cloud Resource Usage. In Proceedings of The *20th International Symposium on Research in Attacks, Intrusions and Defenses*, Atlanta, Georgia, September, 2017. [Acceptance rate: 20%]
- USENIX Security'17 Zhenyu Ning and **Fengwei Zhang**. Ninja: Towards Transparent Tracing and Debugging on ARM. In Proceedings of The *26th USENIX Security Symposium*, Vancouver, BC, Canada, August, 2017. [Acceptance rate: 16%]
- SWC'17 Lei Zhou, **Fengwei Zhang**, and Guojun Wang. Using Asynchronous Collaborative Attestation to Build A Trusted Computing Environment for Mobile Applications. In Proceedings of The *3rd IEEE International Conference on Smart World Congress*, Newark, California, August, 2017.

- ISCA HASP'17 Zhenyu Ning, **Fengwei Zhang**, Weisong Shi, and Larry Shi. Position Paper: Challenges Towards Securing Hardware-assisted Execution Environments. In Proceedings of The *Hardware and Architectural Support for Security and Privacy*, In conjunction with The *44th International Symposium on Computer Architecture (ISCA'17)*, Toronto, ON, Canada, June, 2017.
- CLOUD'17 Kai Huang, Xing Gao, **Fengwei Zhang**, and Jidong Xiao. COMS: Customer Oriented Migration Service. In Proceedings of The *10th IEEE International Conference on Cloud Computing*, Honolulu, Hawaii, June, 2017.
- EuroSys EuroSec'17 Constantinos Koliass, Lucas Copi, **Fengwei Zhang**, and Angelos Stavrou. Breaking BLE Beacons For Fun but Mostly Profit. In Proceedings of The *10th European Workshop on Systems Security*, In conjunction with *The 12th European Conference on Computer Systems (EuroSys'17)*, Belgrade, Serbia, April, 2017 . [Acceptance rate: 9/24=37%]
- ISCA HASP'16 **Fengwei Zhang** and Hongwei Zhang. SoK: A Study of Using Hardware-assisted Isolated Execution Environments for Security. In Proceedings of The *Hardware and Architectural Support for Security and Privacy*, In conjunction with The *43rd International Symposium on Computer Architecture (ISCA'16)*, Seoul, South Korea, June, 2016.
- SANER'16 Kevin Leach, Chad Spensky, Westley Weime, and **Fengwei Zhang**. Towards Transparent Introspection. In Proceedings of The *23rd IEEE Conference on Software Analysis, Evolution, and Reengineering*, Osaka, Japan, March, 2016.
- ACSAC'15 Bing Chang, Zhan Wang, Bo Chen, and **Fengwei Zhang**. MobiPluto: File System Friendly Deniable Storage for Mobile Devices. In Proceedings of The *31st Annual Computer Security Applications Conference*, Los Angeles, California, December 2015. [Acceptance rate: 24%]
- CSCloud'15 Dan Fleck, Sharath Hiremagalore, Stephen Reese, Liam McGhee, and **Fengwei Zhang**. Class-Chord: Efficient Messages to Classes of Nodes in Chord. In Proceedings of The *2nd IEEE International Conference on Cyber Security and Cloud Computing*, New York, NY, November 2015.
- S&P'15 **Fengwei Zhang**, Kevin Leach, Angelos Stavrou, Haining Wang, and Kun Sun. Using Hardware Features for Increased Debugging Transparency. In Proceedings of The *36th IEEE Symposium on Security and Privacy*, San Jose, California, May 2015. [Acceptance rate: 13%]
- AsiaCCS'15 **Fengwei Zhang**, Kevin Leach, Haining Wang, and Angelos Stavrou. TrustLogin: Securing Password-Login on Commodity Operating Systems. In Proceedings of The *10th ACM Symposium on Information, Computer and Communications Security*, Singapore, April 2015. [Full paper acceptance rate: 18%]
- ESORICS'14 **Fengwei Zhang**, Haining Wang, Kevin Leach, and Angelos Stavrou. A Framework to Secure Peripherals at Runtime. In Proceedings of The *19th European Symposium on Research in Computer Security*, Wroclaw, Poland, September 2014. [Acceptance rate: 24.79%]
- DSN'13 **Fengwei Zhang**. IOCheck: A Framework to Enhance the Security of I/O Devices at Runtime. In Proceedings of The *43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, Budapest, Hungary, June 2013. [Student Paper]
- DSN'13 **Fengwei Zhang**, Kevin Leach, Kun Sun, and Angelos Stavrou. SPECTRE: A Dependable Introspection Framework via System Management Mode. In Proceedings of The *43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, Budapest, Hungary, June 2013. [Acceptance rate: 22%]
- NDSS'12 Kun Sun, Jiang Wang, **Fengwei Zhang**, and Angelos Stavrou. SecureSwitch: BIOS-Assisted Isolation and Switch between Trusted and Untrusted Commodity OSes. In Proceedings of The *19th Annual Network & Distributed System Security Symposium*, San Diego, California, February 2012. [Acceptance rate: 18%]

S&P SADFE'11 Jiang Wang, **Fengwei Zhang**, Kun Sun, and Angelos Stavrou. Firmware-assisted Memory Acquisition and Analysis tools for Digital Forensic. In Proceedings of The *6th International Workshop on Systematic Approaches to Digital Forensic Engineering*, In conjunction with The *32nd IEEE Symposium on Security and Privacy (S&P'11)*, Oakland, California, May 2011.

CSIIRW'08 Andy Ju An Wang, **Fengwei Zhang**, and Min Xia. Temporal Metrics for Software Vulnerabilities. In Proceedings of The *4th Annual Workshop on Cyber Security and Information Intelligence Research*, Oak Ridge, Tennessee, May 2008.

Refereed Journal Articles

TDSC'18 **Fengwei Zhang**, Kevin Leach, Angelos Stavrou, and Haining Wang. Towards Transparent Debugging. In *IEEE Transactions on Dependable and Secure Computing*, Vol.15, No.2, pp.321-335, 2018. Impact Factor: 4.410.

TIFS'18 Jinku Li, Xiaomeng Tong, **Fengwei Zhang**, Jianfeng Ma. FINE-CFI: Fine-grained Control-Flow Integrity for Operating System Kernels. In *IEEE Transactions on Information Forensics & Security*, Vol.13, No.6, pp.1535-1550, 2018. Impact Factor: 4.332.

CompSec'18 Li Yang, Teng Wei, **Fengwei Zhang**, Jianfeng Ma. SADUS: Secure Data Deletion in User Space For Mobile Devices. In *Elsevier Computers & Security*, Vol.77, pp.612-626, 2018. Impact Factor: 2.849.

CompSec'18 Bing Chang, Yao Cheng, Bo Chen, **Fengwei Zhang**, Wen Tao Zhu, Yingjiu Li, and Zhan Wang. User-Friendly Deniable Storage for Mobile Devices. In *Elsevier Computers & Security*, Vol.72, pp.163-174, 2018. Impact Factor: 2.849.

TDSC'14 **Fengwei Zhang**, Jiang Wang, Kun Sun, and Angelos Stavrou. HyperCheck: A Hardware-Assisted Integrity Monitor. In *IEEE Transactions on Dependable and Secure Computing*, Vol.11, No.4, pp.332-344, July-August 2014.

JAGR'08 Andy Ju An Wang, Min Xia, and **Fengwei Zhang**. Metrics for Information Security Vulnerabilities. In *Journal of Applied Global Research*, Vol.1, No.1, pp.48-58, 2008.

Technical Reports

TR'11 Kun Sun, Jiang Wang, **Fengwei Zhang**, and Angelos Stavrou. SecureSwitch: BIOS-Assisted Isolation and Switch between Trusted and Untrusted Commodity OSes. Technical Report GMU-CS-TR-2011-7, Department of Computer Science, George Mason University, Fairfax, VA, July 2011.

Teaching Experience

Instructor

Fall 2018 **CSC 6991—Topics in Computer Security**, *Wayne State University*.

Graduate-level elective course for M.S. and Ph.D. level students

Course website: <http://www.cs.wayne.edu/fengwei/18fa-csc6991>

Winter 2018 **CSC 4992—Cyber Security Practice**, *Wayne State University*.

Elective course for undergraduate seniors

Course website: <http://www.cs.wayne.edu/fengwei/18sp-csc4992>

Winter 2018 **CSC 3010—Ethics in Computer Science**, *Wayne State University*.

Required course for undergraduate

Course website: <http://www.cs.wayne.edu/fengwei/18sp-csc3010>

Fall 2017 **CSC 6991—Topics in Computer Security**, *Wayne State University*.

Graduate-level elective course for M.S. and Ph.D. level students

Course website: <http://www.cs.wayne.edu/fengwei/17fa-csc6991>

Winter 2017 **CSC 4992—Cyber Security Practice**, *Wayne State University*.

Elective course for undergraduate seniors

Course website: <http://www.cs.wayne.edu/fengwei/17sp-csc4992>

- Fall 2016 **CSC 6991–Topics in Computer Security**, *Wayne State University*.
Graduate-level elective course for M.S. and Ph.D. level students
Course website: <http://www.cs.wayne.edu/fengwei/16fa-csc6991>
- Winter 2016 **CSC 5991–Cyber Security Practice**, *Wayne State University*.
Elective course for undergraduate seniors and M.S. level students
Course website: <http://www.cs.wayne.edu/fengwei/16sp-csc5991>
- Fall 2015 **CSC 6991–Advanced Computer Security**, *Wayne State University*.
Graduate-level elective course for M.S. and Ph.D. level students
Course website: <http://www.cs.wayne.edu/fengwei/15fa-csc6991>
- Teaching Assistant**
- Spring 2011 **CS 571–Operating Systems**, *George Mason University*.
Instructor: Prof. Hakan Aydin
- Spring 2011 **ISA 562–Information Security Theory and Practice**, *George Mason University*.
Instructor: Prof. Ahmed Alazzawe
- Fall 2010 **CS 310–Data Structures**, *George Mason University*.
Instructor: Prof. Richard Carver

Student Advising

Ph.D. Students

Zhengyu Ning (August 2015 - present)

Saeid Mofrad (June 2016 - present)

Jinghui Liao (July 2018 - present)

M.S. Students

Lucas Copi (August 2015 - December 2016)

Yang Zhang (June 2016 - December 2016)

Undergraduate Students

Jacob Bednard (March 2017 - present)

Aaron Zhang (May 2018 - present)

Visiting Scholars

Lei Zhou (August 2017 - present). Ph.D. Student, Central South University, China.

Mu Han (September 2017 - present). Associate Professor, Jiangsu University, China.

Ph.D. Dissertation Committee Member

Dong Ruan, *Department of Computer Science at WSU*.

"Models, Languages, and Algorithms for Scientific Workflow Monitoring and Exception Handling"
Advised by Prof. Shiyong Lu, Fall 2017.

Mahdi Ebrahimi, *Department of Computer Science at WSU*.

"Data and Task Placement Strategies for Big Data Workflows"
Advised by Prof. Shiyong Lu, Winter 2017.

Aravind Mohan, *Department of Computer Science at WSU*.

"A Big Data Management Framework for Running Workflows in the Cloud"
Advised by Prof. Shiyong Lu, Winter 2017.

Erfan Najmi, *Department of Computer Science at WSU*.

"Improving User Experience in Information Retrieval Using Semantic Web and Other Technologies"
Advised by Prof. Zaki Malik, Fall 2016.

Professional Service

Program Organization

- EuroSec Publicity Chair, European Workshop on Systems Security, 2018.
- CCSW Publicity Chair, ACM Cloud Computing Security Workshop, 2017.

Program Committee Membership

- CCS ACM Conference on Computer and Communications Security, 2018, 2017.
- ACSAC Annual Computer Security Applications Conference, 2018, 2017, 2016.
- EuroSec European Workshop on Systems Security, 2018.
- MASS IEEE International Conference on Mobile Ad-hoc and Sensor Systems, 2018.
- SecureComm EAI International Conference on Security and Privacy in Communication Networks, 2018.
- ICICS International Conference on Information and Communications Security, 2018.
- IoTSSP ACM MobiHoc Workshop on Mobile IoT Sensing, Security, and Privacy, 2018.
- ICC IEEE International Conference on Communications, 2018.
- C4W Collaborative Computing with Cloud and Client Workshop, 2018.
- CCSW ACM Cloud Computing Security Workshop, 2017.
- CCSPoster ACM Conference on Computer and Communications Security Posters, 2017.
- HASP Hardware and Architectural Support for Security and Privacy, 2017.
- ICPADS IEEE International Conference on Parallel and Distributed Systems, 2016.
- DependSys The Second International Symposium on Dependability in Sensor, Cloud, and Big Data Systems and Applications, 2016.

Referee and Reviewer Service

- TIFS IEEE Transactions on Information Forensics and Security.
- TDSC IEEE Transactions on Dependable and Secure Computing.
- TOPS ACM Transactions on Privacy and Security.
- TCPS ACM Transactions on Cyber-Physical Systems.
- JC Journal of IEEE Computer.
- ICM IEEE Internet Computing Magazine.
- JSA Journal of Systems Architecture
- ICPP 45th International Conference on Parallel Processing, 2016.
- S&P IEEE Symposium on Security and Privacy, 2015.
- DSN IEEE/IFIP International Conference on Dependable Systems and Networks, 2013, 2015.

University Service

- Salary Committee, Department of Computer Science, Wayne State University, 2018-present.
- Undergraduate Committee, Department of Computer Science, Wayne State University, 2016-present.
- Faculty Search Committee, Department of Computer Science, Wayne State University, 2016.

Talks and Presentations

Invited Talks

- June 2018 Transparent Malware Analysis on x86 and ARM. Shenzhen Institutes of Advanced Technology (SIAT), Chinese Academy of Sciences, Shenzhen, China. Host: Prof. Chengzhong Xu
- May 2018 Transparent Malware Analysis on x86 and ARM. International Forum for Security Research (InForSec), Tsinghua University, Beijing, China. Host: Prof. Haixin Duan

- May 2018 Transparent Malware Analysis on x86 and ARM. DEFCON China, May 11-13, 2018, Beijing, China.
- February 2018 Auditing and Advancing the Cyber Security of Traffic Signal Systems. The 1st Metro Detroit Workshop on Connected and Autonomous Driving (MetroCAD 2018), Detroit, MI. Host: Prof. Weisong Shi
- January 2018 Challenges Towards Securing Hardware-assisted Execution Environments. Graduate Seminar, Department of Computer Science, Wayne State University, Detroit, MI. Host: Prof. Loren Schwiebert
- July 2016 SoK: A Study of Using Hardware-assisted Isolated Execution Environments for Security. Department of Computer Science and Technology, Hunan University, Changsha, China. Host: Prof. Sheng Xiao
- July 2016 SoK: A Study of Using Hardware-assisted Isolated Execution Environments for Security. Department of Computer Science and Technology, Xidian University, Xi'an, China. Host: Prof. Li Yang
- July 2016 SoK: A Study of Using Hardware-assisted Isolated Execution Environments for Security. Department of Computer Science and Technology, Central South University, Changsha, China. Host: Prof. Guojun Wang
- February 2016 Towards Transparent Debugging. Graduate Seminar, Department of Computer Science, Wayne State University, Detroit, MI. Host: Prof. Loren Schwiebert
- July 2015 Using Hardware Features for Increased Debugging Transparency. Department of Computer Science and Technology, Central South University, Changsha, China. Host: Prof. Guojun Wang
- July 2015 TrustLogin: Securing Password-Login on Commodity Operating Systems. Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing, China. Host: Prof. Zhan Wang
- July 2014 Using Isolated Execution Environments for Securing Systems. Summer Faculty Workshop, Southern Illinois University, College of Applied Sciences and Arts, Carbondale, IL. Host: Prof. Andy An Ju Wang

Conference Presentations

- August 2017 Scotch: Combining Software Guard Extensions and System Management Mode to Monitor Cloud Resource Usage. The 20th International Symposium on Research in Attacks, Intrusions and Defenses, Atlanta, Georgia. Session Chair: Prof. Angelos Stavrou
- June 2017 Position Paper: Challenges Towards Securing Hardware-assisted Execution Environments. Hardware and Architectural Support for Security and Privacy (HASP), Toronto, ON, Canada. Session Chair: Prof. Jakub Szefer
- May 2015 Using Hardware Features for Increased Debugging Transparency. The 36th IEEE Symposium on Security and Privacy, San Jose, California. Session Chair: Prof. Farinaz Koushanfar
- April 2015 TrustLogin: Securing Password-Login on Commodity Operating Systems. The 10th ACM Symposium on Information, Computer and Communications Security, Singapore. Session Chair: Prof. Yingjiu Li
- June 2013 IOCheck: A Framework to Enhance the Security of I/O Devices at Runtime. The 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Budapest, Hungary. Session Chair: Prof. Yair Amir
- June 2013 SPECTRE: A Dependable Introspection Framework via System Management Mode. The 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Budapest, Hungary. Session Chair: Prof. Marco Vieira

Honors and Awards

- December 2017 **Distinguished Paper Award**, *The 33rd Annual Computer Security Applications Conference (ACSAC'17), Orlando, Florida, USA.*
- April 2015 **Outstanding Graduate Student Award**, *George Mason University, Department of Computer Science.*
- October 2014 **Dissertation Completion Grant**, *George Mason University.*
Grant amount: \$8,000
Term of award: Spring 2015 semester
- June 2013 **Travel Grant**, *Trusted Infrastructure Workshop, Pennsylvania State University, University Park, PA.*
- June 2012 **Travel Grant**, *Joint Summer Schools on Cryptography and Principles of Software Security, Pennsylvania State University, University Park, PA.*
- May 2008 **Magna Cum Laude**, *Graduated from Southern Polytechnic State University, Marietta, GA.*
- 2007–2008 **Honors Program Member**, *Southern Polytechnic State University, Marietta, GA.*
- 2007–2008 **Alpha Chi Member**, *National College Honors Scholarship Society.*
- 2006–2008 **Dean's List**, *Southern Polytechnic State University, Marietta, GA.*

Membership

- Association for Computing Machinery (ACM)
Institute of Electrical and Electronics Engineers (IEEE)
The Advanced Computing Systems Association (USENIX)