

Hui Lin (Hugo)

Address: 303 E White St, Apt 4, Champaign, IL, 61820
Tel: (773) 495-5156
Email: hlin33@illinois.edu, hugolin615@gmail.com

Objective: Searching for a full-time research position in the area of system and network reliability and security from a responsible and hard-working Ph.D. student, with good teamwork skills, leadership, and strong research experiences with the major in computer engineering (e.g., **computer security, network, operating system, virtual machine**, etc.) and minor in electrical engineering (e.g., **power system analysis, control theory**, etc.)

Research Project:

- **Software-defined Networking for dynamic access control**
 - Designed moving target defense that dynamically changes network connectivity in industrial control systems
 - Used integer linear programming (ILP) to design self-healing networks for industrial control systems
 - Deployed Onos in Geni nation-wide network platform
 - ◆ Implemented device drivers and distributed controller applications in Onos
 - ◆ Built wide-area networks consisting of real hardware switches in different geographical locations
- **Specification-based intrusion detection for malicious operations in industrial control systems**
 - Adapted Bro to parse and analyze proprietary network packets (e.g. Modbus, DNP3)
 - Connected Bro to power system assessment tools
 - ◆ Adapted power flow analysis algorithm for online detection
- **Android security**
 - Conducted research on vulnerabilities in package installation procedure; replaced an existing user application with a Trojan application
- **User level rootkit detection**
 - Used a hypervisor based on Intel® Virtual Technology for X86 to monitor user-level processes
 - ◆ Used extended page table (EPT) to specify access controls on memory pages
- **Computer security (attack/defense)**
 - Launched buffer overflow, XSS, SQL, XSRF attacks in a full-fledged web applications; built a signature-based network intrusion detection system
 - Built Dionaea honeypot and collected real malware/Trojan
 - Analyzed real incidents collected by National Center of Supercomputing Application
 - Online/offline sandbox analysis on Malware (by Threatexpert, Anubis, and Buster Sandbox Analyzer)
 - Performed reverse engineering on Malware (by IDA)
- **Operating system design**
 - Built the core of Linux kernel for X86 architecture (Using x86 assembly and C)
 - ◆ Built booting, paging, file system and device driver
 - ◆ Developed system call, exception, interrupt, text-mode video memory, loader, and scheduler
 - ◆ Developed dynamically load kernel modules to support a gamepad device

Work Experience:

- Summer 2015, Argonne National Lab, Research Aide, Argonne, IL
- Spring 2015, Advanced Digital Science Center, Research Intern, Singapore
- Summer 2013, Qualcomm®, Interim Engineering Intern in the Office of the Chief Scientist, San Diego, CA
- Summer 2011, Intel® Lab, Graduate Intern at Security and Cryptography Research Lab, Hillsboro, OR
Evaluation: “Exceeds Expectation”

Education History:

- 06/2010–present, Uni. of Illinois at Urbana-Champaign; **Ph.D.**, Electrical & Computer Eng. Dept., **GPA:** 4.0/4.0
- 08/2007–05/2010, Uni. of Illinois at Chicago; **M.S.**, Electrical & Computer Eng. Dept., **GPA:** 4.0/4.0

Skills & Tools:

- **Teamwork & Leadership:**
 - Mentored Ph.D. and undergraduate students on projects
 - Actively participated in UIUC ECE 391 course project to build the core of Linux Kernel on x86 architecture
- **Operating system:**
 - Proficient in **Linux Kernel, Windows Kernel** and their **device driver** development
 - Familiar with **Android** framework
- **Network**
 - Proficient with **Onos** network operating systems
 - Proficient with Software-defined Networking (SDN) controllers, e.g., **Pox, Ryu**
 - Proficient with **Geni** network experiment environment
 - Proficient with **Bro** and its script language
- **Computer architecture:**
 - Familiar with **Intel x86** (assembly) and **VT-x**
- **Development and simulation tools:**
 - Proficient with **gcc, gdb, and KVM**
 - Proficient in **Matlab, Opti, Microsoft Visual Studio, MySQL**
 - Proficient with **Maude**, an executable formal model checking tool
- **High-level programming language:**
 - Proficient in C, C++, Java, Python
- **Power System Analysis:**
 - Proficient with **Matpower**, and **PowerWorld**
 - Familiar with **DNP3, Modbus, and IEC 61850**

Appendix:

Selected Publications

1. **Hui Lin**, Ravishankar K. Iyer, Zbigniew Kalbarczyk, "RAINCOAT: RANdomized Network Communication in Power Grid Cyber INfrastructure to MIslead Cyber Attackers," the *47th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN '17)*, in submission.
2. **Hui Lin**, Chen Chen, Jianhui Wang, Junjian Qi, Dong Jin, Zbigniew Kalbarczyk, Ravishankar K. Iyer, "Self-Healing Attack-Resilient PMU Network for Power System Operation," in *IEEE Transactions on Smart Grid*, July 27th, 2016.
3. **Hui Lin**, Adam Slagell, Zbigniew Kalbarczyk, Peter W. Sauer, and Ravishankar K. Iyer, "Runtime Semantic Security Analysis to Detect and Mitigate Control-related Attacks in Power Grids," in *IEEE Transactions on Smart Grid*, March 28th, 2016.
4. **Hui Lin**, Homa Alemzadeh, Daniel Chen, Zbigniew Kalbarczyk, Ravishankar K. Iyer, "Safety-critical Cyber-physical Attacks: Analysis, Detection, and Mitigation," In *Proceedings of the Symposium and Bootcamp on the Science of Security (HotSOS '16)*, pp. 82-89, doi: <http://dx.doi.org/10.1145/2898375.2898391>.
5. **Hui Lin**, Adam Slagell, Catello Di Martino, Zbigniew Kalbarczyk, and Ravishankar K. Iyer. "Adapting Bro into SCADA: Building a Specification-based Intrusion Detection System for the DNP3 Protocol," In *Proceedings of 8th Annual Cyber Security and Information Intelligence Research Workshop, CSIIRW 2012, Oak Ridge, TN, USA, Oct. 30–Nov. 1, 2012*. Top Three Paper Award.
6. Gyungho Lee, Yixin Shi, and **Hui Lin**, "Indirect Branch Validation Unit," *Microprocessors and Microsystems*, Volume 33, Issues 7-8, October-November 2009, Pages 461-468.

List of Selected Courses, from University of Illinois at Urbana-Champaign

Course Name	Taken Time	Final Score
ECE 524, Advanced Computer Security	Fall, 2014	A
ECE 515, Control System Theory & Design	Spring, 2014	A
ECE 476, Power System Analysis	Fall, 2013	A
ECE 486, Control System	Spring, 2013	A+
CS 476, Program Verification	Spring, 2012	A+
ECE 542, Fault-Tolerant Digital System Design	Fall, 2011	A
CS 498, Special Topics on Malware Analysis	Fall, 2011	A
CS 533, Parallel Computer Architectures	Spring, 2011	A+
CS 526, Advanced Compiler Construction	Spring, 2011	A+
ECE 391, Computer Systems Engineering	Fall, 2010	A
ECE 422, Computer Security I	Fall, 2010	A

List of Selected Courses, from University of Illinois at Chicago

Course Name	Taken Time	Final Score
CS 473, Compiler Design	Spring, 2009	A
ECE 567, Advanced VLSI Design	Spring, 2009	A
CS 487, Secure Computer Systems	Fall, 2008	A
CS 501, Computer Algorithm II	Fall, 2008	A
ECE 465, Digital System Design	Spring, 2008	A
ECE 568, Advanced Micro Architecture	Spring, 2008	A
ECE 466, Computer Architecture	Fall, 2007	A
ECE 467, Introduction to VLSI Design	Fall, 2007	A
CS 401, Computer Algorithm I	Fall, 2007	A