Chien-Ying Chen

Ph.D. Candidate in Computer Science at UIUC

Champaign, IL, USA
cchen140@illinois.edu
linkedin.com/in/cyer

Summary

Highly skilled in **Real-time System/Embedded System Development** and **System Security Research**.

- Hybrid Background: **Electronic Engineering** (BS) + **Computer Science** (MS and PhD)
- Industry Experience: **3-year work experience** in developing **mass production Android smartphones** at HTC
- Good Leadership: Leading **2 research projects** and **a team of 7 students** for building an autonomous car
- Good Teamwork: Worked as the 2nd author in 6 of the **11 published papers** in 5 different projects

Education

Ph.D. Candidate in Computer Science — 2014 – Present
University of Illinois at Urbana-Champaign — GPA: 3.96/4.0

- Research focused on security in real-time system (RTS) kernel and embedded systems
- Published 9 (system and security focused) papers and 1 (pending) patent

M.S. in Computer Science — 2007 – 2009
National Tsing Hua University (Taiwan) — GPA: 91.65/100

- Developed a solar power harvesting system and a WSN/IoT development platform
- Received 2 medals (in 2 system design contests), published 2 papers and 2 patents

B.S. in Electronic Engineering — 2003 – 2007
National Yunlin University of Science and Technology (Taiwan) — GPA: 3.82/4.0 **(top of the class)**

- Developed an autonomous robot that can automatically scan and build an indoor map
- Received *College Student Research Award* and 7 *Presidential Awards*

Work Experience

Academia **Research Assistant** in Information Trust Institute — 2014 – Present
University of Illinois at Urbana-Champaign, Urbana, IL

- Leading 2 NSF-funded, system security research projects, advised by Prof. Sibin Mohan
- Developed an RTOS schedule simulator (in Java) that is used in many data-intensive research projects

Academia **Teaching Assistant** for (CS438) Communication Networks in Computer Science — 2019 Spring
University of Illinois at Urbana-Champaign, Urbana, IL

- Developed an auto-grader system (in Perl and Python) for grading 68 students' programming assignments

Intern **Student Associate (Research Intern)** in IoT Security & Privacy Center — 2017 Summer, 2016 Summer
SRI International, Menlo Park, CA & Manhattan, NY

- Hacked an iHealth wireless oximeter via Bluetooth to leak user measurement data
- Developed an IoT network monitor and proposed a threat model for IoT applications

Industry **Senior Engineer** in IA RD Logic (Hardware RD) Department — 2009 – 2013
HTC Corporation (Taiwan)

- Developed mass production Android smartphones: T-Mobile G2, HTC Wildfire S, Desire VT , One V
- Brought up ARM-based boards; analyzed part power consumption; Debugged sensor, camera and LCM functions

Project Highlights

- **Autonomous Cars:** Led a team to build a 1/10th scale autonomous car. The computation platform on the car consists of a Jetson TX2 board, a dual-camera module and an auxiliary module (for IMU, motor drivers and power supply). Techniques involved include SLAM, object detection, route planning and PID control (for steering and throttle).
- **Real-Time Linux:** Developed and implemented (in C) both an attack algorithm that can leak process execution behavior and a kernel patch that supports schedule randomization mode in RT Linux (RTAS'16, RATS'19).
- **Embedded System Security:** Developed a restart-based mechanism for safety-critical cyber-physical systems. A prototype was built on a Zedboard (an ARM Cortex-A9-based board) running FreeRTOS with avionic applications.

Professional Skills

Software/System: Linux (PREEMPT_RT patch), FreeRTOS, ROS, C/C++, Java, Python
Embedded Systems: hardware development (schematic/PCB) and debugging (oscilloscopes/logic analyzer)

Publications

2019 "A Unified Digital Twin Framework for Real-time Monitoring and Evaluation of Smart Manufacturing Systems," in IEEE 15th International Conference on Automation Science and Engineering (CASE), Aug. 2019.

2019 "Towards Automated Safety Vetting of PLC Code in Real-World Plants," in IEEE Symposium on Security & Privacy (S&P), May 2019.

2019 "A Novel Side-Channel in Real-Time Schedulers," in IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), Apr. 2019.

2018 "Preserving Physical Safety Under Cyber Attacks," in IEEE Internet of Things Journal, Dec. 2018.

2018 "Securing real-time internet-of-things," in MDPI Sensors, Dec. 2018.

2018 "SDCWorks: A Formal Framework for Software-Defined Control of Smart Manufacturing Systems," in ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), Apr. 2018.

2018 "Guaranteed Physical Security with Restart-Based Design for Cyber-Physical Systems," in ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), Apr. 2018.

2017 "Jumping the Air Gap: Modeling Cyber-Physical Attack Paths in the Internet-of-Things," in ACM Workshop on Cyber-Physical Systems Security & Privacy (CPS-SPC), Nov. 2017.

2016 "TaskShuffler: A Schedule Randomization Protocol for Obfuscation Against Timing Inference Attacks in Real-Time Systems," in IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), Apr. 2016.

2016 "Scheduleak: An algorithm for reconstructing task schedules in fixed-priority hard real-time systems," (abstract only) in IEEE RTSS Workshop on Security and Dependability of Critical Embedded Real-Time Systems (CERTS), Nov. 2016.

2010 "DuraCap: a Supercapacitor-Based, Power-Bootstrapping Maximum Power Point Tracking Energy-Harvesting System," in ACM/IEEE International Symposium on Low Power Electronics and Design (ISLPED), Aug. 2010.

2010 "EcoSpire: An Application Development Kit for an Ultra-Compact Wireless Sensing System," in IEEE Embedded Systems Letters, Oct. 2009.

2009 "Privacy Preserving Association Rules by Using Greedy Approach," in the World Congress on Computer Science and Information Engineering, Mar. 2009.

NSF Projects

Present SaTC-1718952, "An Exploration of Schedule-Based Vulnerabilities in Real-Time Embedded Systems"

Present CPS-1544901, "Software Defined Control for Smart Manufacturing Systems"

Patents

2018 US Patent (pending), "Modeling cyber-physical attack paths in the Internet-of-things"

2013 Taiwanese Patent NO.99100899, "Energy Harvesting System"

2012 US Patent NO.8188703 (B2), "Energy Harvesting System"