RUIMIN SUN

Boston, MA | r.sun@northeastern.edu | http://www.ruiminsun.com

RESEARCH INTERESTS

Cybersecurity in mobile and cyber-physical systems

EDUCATION

UNIVERSITY of FLORIDA (UF) Aug. 2014 – May. 2019
Ph.D. in Electrical and Computer Engineering
Thesis: Leveraging Uncertainty to Improve System Security and Reliability
Advisor: Daniela Oliveira

UNIVERSITY of FLORIDA (UF) Aug. 2012 – May. 2014
M.S. in Electrical and Computer Engineering
Advisor: Xiaolin Andy Li

SOUTHEAST UNIVERSITY (SEU), CHINA Aug. 2008 – Jun. 2012
B.S. in Measurement Control and Automation
Thesis: Wireless Human Pulse Signal Measurement and Analysis System.
Advisor: Ruqiang Yan

EXPERIENCES

NORTHEASTERN UNIVERSITY Aug. 2019 – Present
Postdoctoral Research Associate

FLORIDA INSTITUTE of CYBER SECURITY Aug. 2014 – May. 2019
Research Assistant

VMWARE May. 2018 – Aug. 2018
Machine Learning Research Intern

PUBLICATIONS

[1] Alejandro Mera, Yi Hui Chen, **Ruimin Sun**, Engin Kirda, Long Lu. D-Box: DMA-enabled compartmentalization for embedded applications. The Network and Distributed System Security Symposium (NDSS), 2022. (to appear)

[2] Marcus Botacin, Fabricio Ceschin, **Ruimin Sun**, Daniela Oliveira, André Grégio. Challenges and Pitfalls in Malware Research. Computers & Security, Jul 1;106:102287. 2021. [Paper]

[3] **Ruimin Sun**, Alejandro Mera, Long Lu, David Choffnes. SoK: Attacks on Industrial Control Logic and Formal Verification-Based Defenses. IEEE European Symposium on Security and Privacy (EuroS&P), 2021. [Paper]

[4] Zhichuang Sun, **Ruimin Sun**, Long Lu, Alan Mislove. Mind your weight (s): A large-scale study on insufficient machine learning model protection in mobile apps. USENIX Security, 2021. [Paper]

[5] **Ruimin Sun**, Xiaoyong Yuan, Pan He, Qile Zhu, Aokun Chen, Andre Gregio, Daniela Oliveira, Xiaolin Li. Learning Fast and Slow: PROPEDEUTICA for Real-time Malware Detection. IEEE Transactions on Neural

Networks and Learning Systems (TNNLS), 2021. [Paper]

[6] **Ruimin Sun**, Marcus Botacin, Nikolaos Sapountzis, Xiaoyong Yuan, Matt Bishop, Donald E Porter, Xiaolin Li, Andre Gregio, Daniela Oliveira. A Praise for Defensive Programming - Leveraging Uncertainty for Effective Malware Mitigation. IEEE Transactions on Dependable and Secure Computing (TDSC), 2020. [Paper]

[7] Nikolaos Sapountzis, **Ruimin Sun,** Xuetao Wei, Yier Jin, Jedidiah R. Crandall, Daniela Oliveira. MITOS: Optimal Propagation Decisioning in Dynamic Information Flow Tracking. International Conference on Distributed Computing Systems (ICDCS), 2020. [Paper]

[8] Nikolaos Sapountzis, **Ruimin Sun**, Daniela Oliveira. DDIFT: Decentralized Dynamic Information Flow Tracking for IoT Privacy and Security. Workshop on Decentralized IoT Systems and Security (DISS), 2019. [Paper]

[9] **Ruimin Sun**, Xiaoyong Yuan, Andrew Lee, Matt Bishop, Donald E. Porter, Xiaolin Andy Li, Andre Gregio and Daniela Oliveira, 2017. The Dose Makes the Poison—Leveraging Uncertainty for Effective Malware Detection. IEEE Conference on Dependable and Secure Computing (DSC), 2017. [Paper]

[10]**Ruimin Sun**, Andrew Lee, Aokun Chen, Donald E. Porter, Matt Bishop, and DanielaOliveira, 2016, October. Bear: A Framework for Understanding Application Sensitivity to OS (Mis) Behavior. IEEE 27th International Symposium In Software Reliability Engineering (ISSRE), 2016. [Paper]

[11]**Ruimin Sun,** Matt Bishop, Natalie C. Ebner, Daniela Oliveira and Donald E. Porter, 2015. The Case for Unpredictability and Deception as OS Features. USENIX; login, 2015 Aug 1. [Paper]

[12]**Ruimin Sun,** Donald E. Porter, Daniela Oliveira, and Matt Bishop, M. The Case for Less Predictable Operating System Behavior. 15th Workshop on Hot Topics in Operating Systems (HotOS), 2015. [Paper]

PATENTS

[1] **Ruimin Sun**, Zhen Mo, Bin Zan, Vamsi Akkineni, Vijay Ganti. An Unsupervised Event Driven Targeted Analysis Approach. US Patent Application 16/242,396

[2] Zhen Mo, Dexiang Wang, Bin Zan, Vijay Ganti, Amit Chopra, **Ruimin Sun**. A Holo- Entropy Based Alarm Scoring Approach. US Patent Application 16/212,170

[3] David Ott, Lei Xu, **Ruimin Sun**, Vijay Ganti, False Positive Resolution Framework For Application Security Modeling Using Cross-Domain Context Information Sharing. *US Patent Application 16/255,551*

TALKS AND POSTER PRESENTATIONS

[1] SoK: Attacks on Industrial Control Logic and Formal Verification-Based Defenses EuroS&P, 2021

[2] SoK: Attacks on Industrial Control Logic and Formal Verification-Based Defenses
University of Wisconsin – Madison, 2020

[3] Leveraging Unpredictability to Improve System Security and Reliability Northeastern University, 2019

[4] Sherlock: AI-based Event-driven System Behavior Diagnosing Approach VMware 2018

[5] Leveraging Unpredictability for Real-time Malware Mitigation Miami University, Ohio, 2018

[6] The Case for Less Predictable Operating System Behavior HotOS 2015

[7] Bear: A Framework for Understanding Application Sensitivity to OS (Mis)Behavior ISSRE 2016

[8] The Dose Makes the Poison - Leveraging Uncertainty for Effective Malware Detection DSC 2017

[9] How Diverse OS can Improve Software Reliability towards OS (mis)Behavior (Invited Talk)
Beihang University, China, 2017

[10]The Case for Less Predictable Operating System Behavior FICS Conf. 2016
[11]Bear: A Framework for Understanding Application Sensitivity to OS (Mis)Behavior FICS Conf. 2017
[12]DeepMalware: Deep Models and Mechanisms for Malware Detection NSF-CBL 2017
[13]DeepMalware: Deep Models and Mechanisms for Malware Detection FICS Conf. 2017

TEACHING EXPERIENCES

SYSTEMS SECURITY
Lecture, CS 3740, Summer 2021, Northeastern University

CROSS LAYERED SECURITY
Guest Lecture, EEL 4930/EEL 5934, Spring 2015-2019, University of Florida

PROFESSIONAL SEVICES

PROGRAM COMMITTEE
ISSRE Fast Abstract 2018

STUDENT PROGRAM COMMITTEE
IEEE S&P 2019

REVIEWER
[1] IEEE Symposium on Security and Privacy (S&P) 2017 - 2021
[2] The ACM Conference on Computer and Communications Security (CCS) 2017 – 2021
[3] USENIX Security 2019 - 2021
[4] Annual Computer Security Applications Conference (ACSAC) 2015, 2016, 2017, 2018
[5] ACM Symposium on Information, Computer and Communications Security (AsiaCCS) 2014 - 2018
[6] IEEE Transactions on Information Forensics & Security (TIFS) 2018
[7] International Symposium on Research in Attacks, Intrusions, and Defenses (RAID) 2016, 2017
[8] International Conference on Dependable Systems and Networks (DSN) 2016, 2017
[9] ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) 2016
[10] ACM Conference on Human Factors in Computing Systems (CHI) 2017
[11] IEEE Conference on Dependable and Secure Computing (DSC) 2017

AWARDS
[1] Grace Hopper Celebration Scholarship, 2017
[2] IEEE S&P Travel Award, 2015
[3] GREPSEC II Travel Award 2015
[4] Wilson and Marie Collins Graduate Fellowship, University of Florida 2014
[5] 19th GENI Travel Award 2014
[6] Achievement Award in Engineering, University of Florida 2012-2014
[7] First prize in College Student Robotics Contest, Jiangsu Province 2011
[8] First prize in National Undergraduate Mathematical Contest in Modeling, SEU 2010

[9] First prize in the IEEE Standard Micro-Mouse Searching Maze Contest, SEU 2010

[10] Second prize in Autonomous Vehicle Contest, SEU 2009

[11] Third prize in National Challenging Cup College Student Contest, SEU 2011