**Sara Rampazzi**
Department of Computer and Information Science and Engineering

University of Florida
Florida Institute for Cybersecurity Research (FICS)
Malachowsky Hall,
1889 Museum Road,
Gainesville, FL 32611

srampazzi@ufl.edu
sararampazzi.com

**Research areas**

Cyber-physical system security & privacy, embedded systems design, modeling, and simulation with application to medical devices, automotive, and Internet of Everything

**Education**

**PhD in Electronics, Computer Science and Electrical Engineering**
University of Pavia (Italy), **2014**.

**MEng in Computer Science Engineering**
University of Pavia (Italy), **2010**.

**BS in Computer Science Engineering**
University of Pavia (Italy), **2008**.

**Grants and awards**

PI:

- **Toyota InfoTech Lab Research grant** on "Discovering Attacks on CAV Cameras", 70K, 2024
- **Toyota InfoTech Lab Research grant** on "Cyber-Physical Attacks on CAV Perception", 100K, 2023
- **Toyota InfoTech Lab Research grant** on "Secure Autonomous Driving Sensor Hardware and Hardware Designs", 70K, 2022
- **Meta Award** Explorations of Trust in AR, VR, and Smart Devices, 75K, 2020

Co-PI:

- **NSF Grant Award #2031077: RAPID: SaTC: COVID19**: Science of using wirelessly powered sensors to quickly scale up verifiable decontamination of individual N95 respirator masks, 200K, 2020

Recognition:

- **Medtronic Outstanding Research Contributor:** For researchers recognized for the value of their contributions to the security of Medtronic medical devices - https://global.medtronic.com/xg-en/product-security/outstanding-research-contributors.html

- Finalist: **ISSNAF Mario Gerla Young Investigator Award 2021** for research in Computer Science - https://www.issnaf.org/young-investigator-awards-finalists-2021

**Academic positions**

**Assistant Professor** — **Jan 2021-Present**
Computer & Information Science & Engineering
University of Florida

**Research Investigator** — **Feb 2018-Dec 2020**
Electrical Engineering & Computer Science,
University of Michigan

**Intermittent Lecturer**
Electrical Engineering & Computer Science, **Jan 2019-Apr 2019**
University of Michigan

**Affiliate Researcher** **Aug 2017-Feb 2018**
Electrical Engineering & Computer Science,
University of Michigan

**Postdoc fellow** **2014**
Computer Science Engineering,
University of Pavia

**Research experience**

**Senior personnel on THAW** **2018-2021**
University of Michigan

**Principal Researcher for MCity PASS project** **2018-2020**
University of Michigan

**Visiting researcher** **Spring 2014**
Univ. de Las Palmas de Gran Canaria *(Spain)*

**Teaching experience**

**Instructor** **Fall 2021 – Present**
*Course: CIS5370 - Computer and Information Security*
Dept. of Computer and Information Science and Engineering, University of Florida

*Course: CIS4360 - Computer and Information Security*
Dept. of Computer and Information Science and Engineering, University of Florida

*Course: CIS4930/6930 - Special Topics in CISE: Cyber-physical System Security*
Dept. of Computer and Information Science and Engineering, University of Florida

**Lecturer** **Winter 2019**
*Course: EECS 496 - Major Design Experience Professionalism*
Dept. of Electrical Engineering and Computer Science, University of Michigan

**Instructor of record** **2013-2014**
*Course: C coding*
Department of Mathematics, University of Pavia

**Instructor of record** **2010-2012**
*Course: Introduction to Computer Systems II*
Computer Science Engineering, University of Pavia

**Teaching Assistant** **2007-2010**
*Course: Introduction to Computer Systems*
Computer Science Engineering, University of Pavia

**Industry experience**

**Firmware developer for LTE systems** **2016-2017**
*Azcom Technology*
*Client:* **Blue Danube Inc.**

**Software engineer consultant** **2015-2016**
*Alten Italia*
*Client:* **Leonardo S.p.A.**
*Client:* **Magneti Marelli (Fiat Chrysler Automobiles Group)**

**Refereed conference publications**

* co-first and corresponding author

° corresponding (senior) author

Complete list available at:
https://scholar.google.com/citations?user=I9d0CrAAAAAJ&hl=en

Jennifer Sheldon, Weidong Zhu, Adnan Abdullah, Sri Hrushikesh Varma Bhupathiraju, Takeshi Sugawara, Kevin R. B. Butler, Md Jahidul Islam, Sara Rampazzi, "**Aqua-Sonic: Acoustic Manipulation of Underwater Data Center Operations and Resource Management**", Proceedings of the IEEE Symposium on Security & Privacy (IEEE S&P), May 20, 2024

Weidong Zhu, Grant Hernandez, Washington Garcia, Dave (Jing) Tian, Sara Rampazzi, Kevin Butler, "**Minding the Semantic Gap for Effective Storage-Based Ransomware Defense**", Proceedings of the 38th International Conference on Massive Storage Systems and Technology (MSST 2024).

Dipkamal Bhusal, Md Tanvirul Alam, Monish Kumar Manikya Veerabhadran, Michael Clifford, Sara Rampazzi, Nidhi Rastogi, "**PASA: Attack Agnostic Unsupervised Adversarial Detection using Prediction & Attribution Sensitivity Analysis**", Proceedings of the IEEE European Symposium on Security and Privacy 2024 (Euro S&P 2024).

Sri Hrushikesh Varma Bhupathiraju, Takami Sato, Michael Clifford, Takeshi Sugawara, Qi Alfred Chen, Sara Rampazzi, "**On the Vulnerability of Traffic Light Recognition Systems to Laser Illumination Attacks**" In Proceedings of VehicleSec Symposium 2024, February 2024

Takami Sato, Sri Hrushikesh Varma Bhupathiraju, Michael Clifford, Takeshi Sugawara, Qi Alfred Chen, Sara Rampazzi, "**Invisible Reflections: Leveraging Infrared Laser Reflections to Target Traffic Sign Perception**", Proceedings of the *Network and Distributed System Security Symposium (NDSS 2024)*

Yazhou Tu, Sara Rampazzi, Xiali Hei "**Towards Adversarial Process Control on Inertial Sensor Systems with Physical Feedback Side Channels**", *Proceedings of* the *5th Joint Workshop on CPS & IoT Security and Privacy (CPSIoTSec 2023).*

Eric Gustafson, Paul Grosen, Nilo Redini, Saagar Jha, Andrea Continella, Ruoyu Wang, Kevin Fu, Sara Rampazzi, Christopher Kruegel, Giovanni Vigna **"Shimware: Toward Practical Security Retrofitting for Monolithic Firmware Images"**, *Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2023)* (Acc. Rate 23%).

Yazhou Tu, Liqun Shan, Md Imran Hossen, Sara Rampazzi, Kevin Butler, Xiali Hei "**Auditory Eyesight: Demystifying µs-Precision Keystroke Tracking Attacks on Unconstrained Keyboard Inputs**", *Proceedings of USENIX Security 2023*. (Acc. Rate 29%).

Dipkamal Bhusal, Rosalyn Shin, Ajay Ashok Shewale, Monish Kumar Manikya Veerabhadran, Michael Clifford, Sara Rampazzi, and Nidhi Rastogi, "**SoK: Modeling Explainability in Security Analytics for Interpretability, Trustworthiness, and Usability"**, Proceedings of the *18th International Conference on Availability, Reliability and Security (ARES 2023)*

Jennifer Sheldon, Weidong Zhu, Adnan Abdullah, Kevin Butler, Md Jahidul Islam, Sara Rampazzi, "**Deep Note: Can Acoustic Interference Damage the Availability of Hard Disk Storage in Underwater Data Centers?"**, In Proceedings of the *15th ACM Workshop on Hot Topics in Storage and File Systems (HotStorage 2023)* (**SK Hynix Best Paper Award**)

Sri Hrushikesh Varma Bhupathiraju, Jennifer Sheldon, Luke A. Bauer, Vincent Bindschaedler, Takeshi Sugawara, Sara Rampazzi, "**EMI-LiDAR: Uncovering Vulnerabilities of LiDAR Sensors in Autonomous Driving Setting using Electromagnetic Interference**", *In Proceedings of ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2023)* (Acc. Rate 18.5%).

Yulong Cao, Sri Hrushikesh Varma Bhupathiraju, Pirouz Naghavi, Takeshi Sugawara, Z. Morley Mao, Sara Rampazzi "**You Can't See Me: Physical Removal Attacks on LiDAR-based Autonomous Vehicles Driving Frameworks**", In *Proceedings of USENIX Security 2023* (Acc. Rate 29%).

Yan Long, Pirouz Naghavi, Blas Kojusner, Kevin Butler, Sara Rampazzi, Kevin Fu, "**Side Eye: Characterizing the Limits of POV Acoustic Eavesdropping from Smartphone Cameras with Rolling Shutters and Movable Lenses**", *In Proceedings of IEEE Security and Privacy 2023*

Takami Sato, Sri Hrushikesh Varma Bhupathiraju, Michael Clifford, Takeshi Sugawara, Qi Alfred Chen, Sara Rampazzi "**WIP: Infrared Laser Reflection Attack Against Traffic Sign Recognition Systems**", *In Proceedings of VehicleSec Symposium 2023*. (**ETAS Best WIP/Short Paper Award, Qualcomm Best Demo Award**) (Acc. Rate 28.22%).

Cassidy Gibson, Vanessa Frost, Katie Platt, Washington Garcia, Luis Vargas, Sara Rampazzi, Vincent Bindschaedler, Patrick Traynor, Kevin Butler, "**Analyzing the Monetization Ecosystem of Stalkerware**", *In Proceedings on Privacy Enhancing Technologies (PETS)* 4: 105-119, 2022 (Acc. Rate 24%).

Nidhi Rastogi, Sara Rampazzi, Michael Clifford, Miriam Heller, Matthew Bishop, Karl Levitt, "**Explaining RADAR features for detecting spoofing attacks in Connected Autonomous Vehicles**", in *Proceedings of Workshop on Explainable Agency in Artificial Intelligence, 2022*.

Takeshi Sugawara, Ben Cyr, Sara Rampazzi°, Daniel Genkin, Kevin Fu, **"Light Commands: Laser-Based Audio Injection on Voice-Controllable Systems"**, in *29th USENIX Security Symposium* (USENIX), August 2020 (Acc. Rate 16.1%).

Sara Rampazzi*, Yazhou Tu, Bin Hao, Angel Rodriguez, Kevin Fu, and Xiali Hei, "**Trick or Heat? Attack on Amplification Circuits to Abuse Critical Temperature Control Systems**", in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS),* November 2019 (Acc. Rate 17%).

Yulong Cao, Chaowei Xiao, Benjamin Cyr, Yimeng Zhou, Won Park, Sara Rampazzi°, Qi Alfred Chen, Kevin Fu, Z. Morley Mao, "**Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving**", in Proceedings of the 2019 *ACM SIGSAC Conference on Computer and Communications Security (CCS),* November 2019 (Acc. Rate 17%).

Connor Bolton, Sara Rampazzi, Chaohao Li, Andrew Kwong, Wenyuan Xu, Kevin Fu, "**Blue Note: How Intentional Acoustic Interference Damages Availability and**

**Integrity in Hard Disk Drives and Operating Systems**". In Proceedings of the *39th Annual IEEE Symposium on Security and Privacy*, May 2018 (Acc. Rate 11.5%).

Sara Rampazzi, Francesco Leporati, Giovanni Danese, Marabelli Franco, Andrea Valsesia, "**A Novel Portable Surface Plasmon Resonance Based Imaging Instrument for On-Site Multi-Analyte Detection**". In *Federated Conference on Computer Science and Information Systems (FedCSIS '13),* Sept 2013.

Sara Rampazzi, Giovanni Danese, Lucia Fornasari, Francesco Leporati, Franco Marabelli, Nelson Nazzicari, Andrea Valsesia, "**Lab On Chip: Portable Optical Device for On-Site Multi-parametric Analysis**". In *IEEE Euromicro Conference on Digital System Design (Euromicro DSD'13),* 4-6 Sept 2013, pp. 807-810.

**Refereed journal publications**

Jianyi Zhang, Yuchen Wang, Yazhou Tu, Sara Rampazzi, Zhiqiang Lin, Insup Lee, Xiali Hei, "**ADC-Bank: Detecting Acoustic Out-of-Band Signal Injection on Inertial Sensors**", *Security and Privacy in Cyber-Physical Systems and Smart Vehicles. SmartSP 2023. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 552. 05 February 2024, Springer (pp. 53-72)* (**SmartSP Best Paper Award**)

Muhammad Sajidur Rahman, Pirouz Naghavi, Blas Kojusner, Sadia Afroz, Byron Williams, Sara Rampazzi, Vincent Bindschaedler, **"PermPress: Machine Learning-Based Pipeline to Evaluate Permissions in App Privacy Policies",** IEEE Access, 2022 (IF 3.476).

Yan Long, Alexander Curtiss, Sara Rampazzi, Josiah Hester, Kevin Fu, "**VeriMask: Sensor Platform for Decontamination of N95 Masks",** In *GetMobile: Mobile Computing and Communications 26*, no. 2, 2022. **(Selected for ACM SIGMOBILE Research Highlight).**

Yan Long, Sara Rampazzi, Takeshi Sugawara, Kevin Fu, "**Protecting COVID-19 Vaccine Transportation and Storage from Analog Cybersecurity Threats**", In Biomedical Instrumentation & Technology 55, no. 3, Oct 2021 (IF 0.13).

Yan Long, Alexander Curtiss, Sara Rampazzi, Josiah Hester, Kevin Fu, "**VeriMask: Facilitating Decontamination of N95 Masks in the COVID-19 Pandemic: Challenges, Lessons Learned, and Safeguarding the Future**", In Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (ACM IMWUT), Sept 2021 (IF 4.16).

Simone Marini, Francesca Vitali, Sara Rampazzi, Andrea Demartini, Tatsuya Akutsu, "**Protease target prediction via matrix factorization**". In Bioinformatics, 29 Aug. 2018, bty746 (IF 6.9).

Sara Rampazzi, Giovanni Danese, Francesco Leporati, Franco Marabelli, "**A Localized Surface Plasmon Resonance-Based Portable Instrument for Quick On-Site Biomolecular Detection**". In IEEE Transactions on Instrumentation and Measurement, Vol. 65 Is. 2, 1 Dec. 2015, pp. 317-327 (IF 5.3).

**Journal publications as member of the N95Decon Consortium**

Complete list available at https://www.n95decon.org/publications

Loïc Anderegg, John Doyle, Margaret L Gardel, Amit Gupta, Christian Hallas, Yuri Lensky, Nancy G Love, Bronwyn A Lucas, Edward Mazenc, Cole Meisenhelder, Ajay Pillarisetti, Daniel Ranard, Allison H Squires, Jessica Vechakul, Nathaniel B Vilas, Stuart Williams, Daniel Wilson, Tyler N Chen, N95DECON Consortium, "**Heat and**

**Humidity for Bioburden Reduction of N95 Filtering Facepiece Respirators**", Applied Biosafety, Jan 2021 (IF 0.72).

Samantha M Grist, Alisha Geldert, Anjali Gopal, Alison Su, Halleh B Balch, Amy E Herr, N95DECON Consortium "**Current Understanding of Ultraviolet-C Decontamination of N95 Filtering Facepiece Respirators**", Applied Biosafety, Jan 2021 (IF 0.72).

Sylvia J Smullin, Branden D Tarlow, N95DECON Consortium, "**Room Temperature Wait and Reuse for Bioburden Reduction of SARS-CoV-2 on N95 Filtering Facepiece Respirators**", Applied Biosafety, Jan 2021 (IF 0.72).

David Rempel, John Henneman, James Agalloco, Jill Crittenden, N95DECON Consortium "**Hydrogen Peroxide Methods for Decontaminating N95 Filtering Facepiece Respirators**", Applied Biosafety, Jan 2021, (IF 0.72).

David Rempel, N95DECON Consortium, "**Scientific Collaboration During the COVID-19 Pandemic: N95DECON.org**". In Annals of Work Exposures and Health, June 2020, (IF 1.960).

**Posters & Demo papers**

Trishna Chakraborty, S. Hrushikesh, Dipkamal Bhusal, Michael Clifford, Sara Rampazzi, Nidhi Rastogi, Qi Alfred Chen, "**Towards A Quantitative Risk Assessment of Physical Adversarial Attacks in the AV Perception Domain**", In the Poster Session of the *USENIX Security Symposium* 2023 (USENIX 2023).

Cesar Arguello, Hunter Searle, Sara Rampazzi, Kevin Butler, "**A Practical Methodology for ML-Based EM Side Channel Disassemblers**", In the Poster Session of the 7th IEEE European Symposium on Security and Privacy 2022.

Yulong Cao, Jiaxiang Ma, Kevin Fu, Sara Rampazzi, Z. Morley Mao, "**Automated Tracking System For LiDAR Spoofing Attacks On Moving Targets**". In the Demo Session of Automotive and Autonomous Vehicle Security (AutoSec) Workshop 2021, Feb 2021. (**Best Demo Award Runner-up**)

Yan Long, Alexander Curtiss, Sara Rampazzi, Josiah Hester, Kevin Fu, "**Automating Decontamination of N95 Masks for Frontline Workers in the COVID-19 Pandemic**". In the Poster Session of the ACM Conference on Embedded Networked Sensor Systems (Sensys 2020), Nov 2020 **(Best Poster Award Runner-up).**

Angel Rodriguez, Sara Rampazzi and Kevin Fu, "**IoT Two Factor Neurometric Authentication System using Wearable EEG**". In the Poster Session of the IEEE Workshop on the Internet of Safe Things (SafeThings 2019), May 2019.

**Patents**

Sara Rampazzi, Giovanni Danese, Lucia Fornasari, Francesco Leporati, Franco Marabelli, Nelson Nazzicari, Andrea Valsesia "**Detection device of molecular compounds based on Surface Plasmon Resonance**". European patent ITMI20131345 (A1) — 2015-02-07. Priority 2013. Published 2015.

**Selected Invited talks lectures and seminars**

"Cyber-physical system security: Exploiting the physics of sensors to undermine AI-based decisions", Invited webinar, Hardware.io - Hardware Security Conference and Training, 02/14/2022

"Sensor Security", Sara Rampazzi, Invited Keynote at 15th IEEE Workshop on Offensive Technologies (WOOT '21), 27/05/2021

"Autonomous Vehicle Security", Invited talk, Lansing Information Systems Security Association (ISSA) Meeting, 12/17/2020

"Wirelessly sensor technology for verifiable decontamination of N95 masks", COVID-19 Research Lightning Round Webinar, COVID Information Commons, 10/16/2020

"Light Commands: Hacking Voice Assistants with Lasers", talk, BlackHat Europe 2020, 12/10/2020

"Cybersecurity In The Internet Of Medical Things Era: Research And Challenges", Invited Seminar, Archimedes 2020 Leadership Workshop Webinar Series, 06/03/2020

"Cybersecurity in Hospitals: comparing EU and US strategies" Seminar & discussion panel in second level postgraduate Master in Cyberlaw and Policies for Digital Innovation, University of Milan Bicocca, 12/19/2018

"Cybersecurity and Implantable Devices". Invited talk in Women in Electrophysiology, Medical Education - Medtronic Accademy, 10/13/2018

"Sensor Security in Cyber-Physical Systems", seminar for graduate students of the Ph.D. School of Electrical and Electronics Engineering and Computer Science, University of Pavia, 07/15/2018

**Service to profession**

**Steering Committee:**
Conference on Offensive Technologies (USENIX WOOT)

**Program Chair:**
17th Workshop on Offensive Technologies (WOOT 2023)
2nd Annual Embedded System Workshop (EmSec 2020)

**Student Funding Chair:**
Network and Distributed System Security Symposium (NDSS 2024)

**Poster/Demo Chair:**
Poster Chair for USENIX Security Symposium 2022
Poster and Demo Chair for the VehicleSec Symposium 2023 and 2024

**Session Chair:**
ACM CCS 2020, USENIX 2021

**Conferences PC Member:**

- IEEE Workshop on the Internet of Safe Things (SafeThings) 2019, 2021
- USENIX Security Symposium (USENIX), 2021, 2022, 2023, 2024
- IEEE Security & Privacy 2023, 2024
- ACM Conference on Computer and Communications Security (CCS) 2020
- Workshop on Offensive Technologies (WOOT) 2020, 2021, 2022
- IEEE SecDev 2021
- DYnamic and Novel Advances in Machine Learning and Intelligent Cyber Security Workshop (DYNAMICS), 2020
- International Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2022
- VehicleSec Symposium 2023
- Workshop on CPS&IoT Security and Privacy (CPSIoTSec) 2022

**N95Decon.org Consortium member (2020-2021):**

Volunteer collective of scientists, with the goal of reviewing, publishing, and disseminating scientific information about N95 masks decontamination and reuse - https://www.n95decon.org/

**Journal Peer Reviewer** (https://www.webofscience.com/wos/author/record/788841): PLOS ONE; ACM Transactions on Privacy and Security; ACM Transactions on Computing for Healthcare; Science Magazine; IEEE Security & Privacy Magazine, Sensors; ACM IEEE Transactions on Dependable and Secure Computing.

**NSF SaTC Grant Proposal Review Panelist** (2018, 2022)

**Organization Committee member:**
Euromicro SEAA 2014/ DSD 2014 Conference

**Mentoring & Advising**

**Inclusion, Diversity, Equity and Access Committee Member**
University of Florida, CISE Dept, 2021 - 2023

**Computer Engineering Undergraduate Advisor**
University of Michigan, Winter 2019

**Mentor of:**

- Wiser – (Women In SEcurity Research) at University of Michigan (2018-2020)
- First Generation Engineering Program at University of Michigan (2018-2020)
- Society of Women Engineers Summer Camp mentor at University of Michigan (2018)

**IEEE Student Branch Computer Science Area Advisor**
IEEE Pavia Student Branch, Region 8, Italian section,
University of Pavia, 2011-2014.

**Technical Skills**

| | |
|---|---|
| PLs: | Matlab, C, Java |
| Design/Modelling/ Simulation tools: | Matlab-Simulink, COMSOL Multiphysics, StateFlow, IBM Rational Rhapsody. |
| Programming/ Validation/Testing tools: | IBM Rational Logiscope, GNURadio, QA System Cantata++, dSpace Target Link, ROS, MPLAB, MikroC for PIC and ARM |

**Languages**

| | |
|---|---|
| Italian | Native speaker |
| English | Fluent |
| Spanish | Scholastic |