Tyler Tucker

tylertucker1@ufl.edu • 407.619.3678
linkedin.com/in/tyler-tucker • www.cise.ufl.edu/~tucker

EDUCATION

Ph.D. in Computer Science
University of Florida **2022** • Pursuing
• Advisor: Patrick Traynor

MS in Computer Science
University of Florida **2021** • GPA: 3.88
• Advisor: Patrick Traynor

BS in Electrical Engineering
University of Florida **2019** • GPA 3.5
• Graduated Cum Laude
• Minored in Computer Science

ACADEMIC AWARDS

Distinguished Paper Award
ACM Conference on Computer and Communications Security (CCS)
Fall 2024

Gartner Group Graduate Fellowship
University of Florida
Spring 2024, Spring 2024

Renwick Scholar
University of Florida
Spring 2019

1st Place, Senior Design
University of Florida
Spring 2018

COURSEWORK

Computer Science
Network Security
Cryptography
Mobile Security
Data Structures
Algorithms
Operating Systems
Computer Organization

Electrical Engineering
Communications
Microprocessors
Digital Integrated Circuits
Filters
Digital Logic

DISSERTATION PUBLICATIONS

SoK: Designing and Detecting LTE FBS [1]
In Submission to the ISOC Network and Distributed Systems Symposium (NDSS) 2026
In this systematization of knowledge (SoK) paper, we review academic publications addressing fake base stations (FBSes) in the cellular network and provide the first analysis of a commercial FBS product in academia, a notably missing contribution in the field for over a decade.

Detecting IMSI-Catchers by Characterizing Identity Exposing Messages in Cellular Traffic [2]
ISOC Network and Distributed Systems Symposium (NDSS) 2025
This work proposes a solution to detecting fake cellular base stations (*"IMSI-Catchers"*), based on their behavior rather than configuration. We profile both commercial cell towers and controlled IMSI-Catchers, then detect a rogue tower in the wild matching the latter profile, becoming the first academic work to substantiate findings of rogue cellular base stations in the wild.

Blue's Clues: Practical Discovery of Non-Discoverable Bluetooth Devices [3]
IEEE Symposium on Security & Privacy (SP) 2023
We develop a novel attack that wirelessly discovers hidden, or *Non-Discoverable*, Bluetooth Classic devices, defeating that security feature of Bluetooth while additionally enabling further DoS attacks and packet injection against unauthenticated devices. This attack affects every Bluetooth device ever manufactured (over 10 billion devices), therefore we disclose our attack to the Bluetooth Special Interest Group to work toward an effective defense.

LeopardSeal: Detecting Call Interception via Audio Rogue Base Stations [4]
International Conference on Mobile Systems, Applications, and Services (MobiSys) 2023
We introduce a new technique to detect adversarial cell towers in the wild using distance-bounding over the audio channel of a phone call and test this detection mechanism between dozens of cities throughout the United States

COLLABORATIVE PUBLICATIONS

SoK: Towards a Unified Approach of Applied Replicability for Computer Security [5]
ACM Conference on Computer and Communications Security (CCS) 2025
We address shortcomings of validity practices within the Cybersecurity academic community, using best practices from other fields and novel contributions to propose a universal framework to represent how authors provide artifacts from their work to external members of the community.

"Better Be Computer or I'm Dumb": A Large-Scale Evaluation of Humans as Audio Deepfake Detectors [6]
ACM Conference on Computer and Communications Security (CCS) 2024
Our team runs a 1000+ participant user study to find out how well humans perform at recognizing audio deepfakes (i.e., average accuracy of 73%), why they classify an audio sample as real or fake, and how their performance compares to ML-based detectors.

SoK: The Good, The Bad, and The Unbalanced: Measuring Structural Limitations of Current Deepfake Media Datasets [7]
USENIX Security Conference 2024
We reveal weaknesses in how audio deepfake competitions and datasets are carried out, then suggest that detectors present sufficient performance metrics while dataset designers consider the base rate of deepfake audio samples. This effort aims to improve audio deepfake detection research, allowing it to keep pace with the rapid advancement in deepfake generation algorithms.

FirmWire: Transparent Dynamic Analysis for Cellular Baseband Firmware [8]
ISOC Network and Distributed System Security Symposium (NDSS) 2022
We develop a rehosting environment to interact with emulated cellular baseband chips, finding 8 vulnerabilities (3 previously unknown) in baseband code from multiple vendors. To verify these vulnerabilities, we operate an adversarial cell tower that attacks phones using these baseband chips in a controlled environment.

SKILLS

Technical Communication
Conference Presentations
Expert Witness Research
Academic Paper Reviews

Software
Rust, Python, C, C++, Java, F#
Linux Server Management
Docker

Electronics
Embedded Programming
Software-Defined Radio
Altium PCB Design
Soldering

WORK EXPERIENCE

Florida Institute for Cybersecurity Research

Graduate Assistant • May 2019 – Current • Gainesville, FL

I work with Dr. Patrick Traynor on several wireless network security projects that address adversarial cell tower detection, audio deepfake defenses, and Bluetooth privacy. Additionally, I act as a Linux server admin and regularly review papers and artifacts for several top-tier security conferences.

Analysis Group

Consultant • September 2024 – Present • Boston, MA

I perform research tasks as a consultant with Analysis Group for litigation cases primarily concerning issues of data breaches and antitrust within the technology sector.

Analysis Group

Summer Associate Intern • June 2024 – August 2024 • Boston, MA

While at AG, I specialized in research tasks associated with litigation cases centered around technology disputes. I have since accepted a full-time offer from AG and will begin sometime in 2025.

Siemens

Controls Intern • Summer 2018 • Orlando, FL

At my second internship with Siemens, I set up a test environment for their SGT-A65 gas turbine generator while interfacing PLCs with Siemens proprietary software.

Digital Control Lab

Frontend Developer • Summer 2018 • Orlando, FL

After my senior design project, a professor hired me to refresh a consumer desktop GUI using a Python Qt program built from the ground up to include graphs, tabs, and resizing behavior expected from modern UIs.

Siemens

ELDP Intern • Summer 2017 • Atlanta, GA

I worked with a team of student interns to plan and create an alpha-level web framework using AWS for an energy "peak-shaving" efficiency program while also creating a Java Application to interface with Excel documents and a REST API to act as a tool to filter out car charger data collected by Siemens for maintenance.

Lockheed Martin

Systems Engineering Intern • Summer 2016 • Orlando, FL

I performed integration and testing tasks under the Special Programs division of Lockheed Martin's Missiles and Fire Control including collecting optical alignment data with sensitive range-finding cameras in field environments and creating a MATLAB application to process camera data and display the resulting plots.

PUBLICATIONS

[1] T. Oh, D. Kim, H. Bae, B. Oh, T. Tucker, C. Park, B. Hong, P. Traynor, and Y. Kim, "SoK: Designing and Detecting LTE FBS," in *Submission to the ISOC Network and Distributed Systems Symposium (NDSS)*, 2026, Acceptance Rate: TBD.

[2] T. Tucker, N. Benett, M. Kotuliak, S. Erni, K. Butler, and P. Traynor, "Detecting IMSI-Catchers by Characterizing Identity Exposing Messages in Cellular Traffic," in *Proceedings of the ISOC Network and Distributed Systems Symposium (NDSS)*, 2025, Acceptance Rate: 16.1%.

[3] T. Tucker, H. Searle, K. R. B. Butler, and P. Traynor, "Blue's Clues: Practical Discovery of Non-Discoverable Bluetooth Devices," in *Proceedings of the IEEE Symposium on Security and Privacy*, 2023, Acceptance Rate: 17.1%.

[4] C. Peeters, T. Tucker, A. Jain, K. R. B. Butler, and P. Traynor, "LeopardSeal: Detecting Call Interception via Audio Rogue Base Stations," in *ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2023, Acceptance Rate: 21%.

[5] D. Olszewski, T. Tucker, K. Butler, and P. Traynor, "SoK: Towards a Unified Approach of Applied Replicability for Computer Security," in *Submission to the ACM Conference on Computer and Communications Security (CCS)*, 2025, Acceptance Rate: TBD.

[6] K. Warren, T. Tucker, A. Crowder, D. Olszewski, A. Lu, C. Fedele, M. Pasternak, S. Layton, K. Butler, C. Gates, and P. Traynor, "Better Be Computer or I'm Dumb": A Large-Scale Evaluation of Humans as Audio Deepfake Detectors," in *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2024, Acceptance Rate: 16.9%.

[7] S. Layton, T. Tucker, D. Olszewski, K. Warren, C. Gates, K. Butler, and P. Traynor, "SoK: The Good, The Bad, and The Unbalanced: Measuring Structural Limitations of Current Deepfake Datasets," in *Proceedings of the USENIX Security Symposium (Security)*, 2024, Acceptance Rate: 18.3%.

[8] G. Hernandez, M. Muench, D. Maier, A. Milburn, S. Park, T. Scharnowski, T. Tucker, P. Traynor, and K. Butler, "FirmWire: Transparent Dynamic Analysis for Cellular Baseband Firmware," in *Proceedings of the Network and Distributed System Security (NDSS) Symposium*, 2022, Acceptance Rate: 16.2%.