Logan Blue

✆ *(321) 474 0990*
✉ *bluel@ufl.edu*
🖱 *www.cise.ufl.edu/~blue*
FICS: www.fics-institute.org/

Around here, however, we don't look backwards for very long. We keep moving forward, opening up new doors and doing new things, because we're curious...and curiosity keeps leading us down new paths. -Walt Disney

Education

2016–2023 (May) **Doctor of Philosophy in Computer Engineering**, *University of Florida*, Gainesville, Florida.
Emphasis: Cybersecurity Advisor: Patrick Traynor

2014–2016 **Master of Science in Computer Engineering**, *University of Florida*, Gainesville, Florida.
Emphasis: Cybersecurity

2010–2014 **Bachelor of Science in Mechanical Engineering**, *University of Florida*, Gainesville, Florida.

Experience

Research

May 2015 – Present **Graduate Researcher**, *Florida Institute of Cyber Security Research (FICS)*, Gainesville, Florida.

- **Thesis:** The advent of modern machine learning has made it such that the source of a human voice is not easily verifiable. By identifying fundamental differences between how humans and machines generate audio, it is possible to provide robust guarantees about the nature of the source.
- Appointed as Co-Lead Graduate Student by FICS faculty members. Tasked with leading, mentoring, and acting as point of contact for the 29 other graduate students within FICS.
- Constructed a deepfake detector that uses the effects of turbulent fluid flows in speech to differentiate organic and synthetic speakers with a precision rate of up to 100% and a recall rate of 99.2%.
- Constructed a deepfake detector that reconstructs the vocal tract of the speaker. This detector is capable of detecting deepfake audio samples with a precision of 99.9% and a recall of 99.5%.
- Designed, developed and implemented a smart speaker protocol to safely authorize user account access by authorized devices while mitigating long term exposure to compromise.
- Assisted with black box, transferable attacks that achieved mistranscription and misidentification rates as high as 100% by modifying only a few frames of audio.
- Performed big data analysis of a Healthcare network to assess their unique vulnerabilities which led to the discovery that medical devices have minimal security risk but medical support devices (servers and computers) are vulnerable.

- Developed a technique to recognize fundamental differences in audio created by humans and electronic speakers thus preventing adversarial requests, replayed audio and hidden commands with a 100%/1.72% TPR (True Positive Rate)/FPR (False Positive Rate) in quiet environments.
- Established a Two Microphone Authentication (2MA) system that can localize a source to within a narrow physical cone ($<30°$) with zero false positives thus eliminating replay attacks and preventing the injection of inaudible (hidden) commands.
- Redesigned, enhanced, and re-architected secure caller ID system moving it from a proof of concept towards a first-generation prototype.
- Researched the use of machine learning backed generative models in Format Transforming Encryption (FTE) to help prevent Internet censorship.
- Designed and built a secure caller ID system for modern telephony networks that detected 99% of tampered call audio with negligible false positives and with a worst-case 1.4 second call establishment overhead.
- Contributed to the study of how SMS is used and misused based on 400,000 text messages sent through public gateways. Retrieved, processed, cleaned, and augmented data. Designed and managed database to hold the data. Discovered pervasive account fraud for services that use phone based two factor authentication, sensitive information disclosure, and poor entropy in authentication codes generated by services used by millions.

Summer 2021 **Security Research Intern**, *Bank of America*, Gainesville, Florida (Remote Employment).
- Led 2 interns in creating a framework for generating an internal dataset to analyze the performance of Audio Deepfake Detectors.
- Contributed to building an attack that causes a Speaker Identification System to misidentify by adding noise.
- Mentored and assisted 3 additional interns on their related projects.
- Gave 3 presentations to working groups and managers about Audio Deepfake creation and detection techniques.

Summer 2020 **Security Research Intern**, *Bank of America*, Gainesville, Florida (Remote Employment).
- Validated the effectiveness of a third party voice recognition tool for securing internal telephony at the bank.
- Experimented with new potential techniques for the creation of Deepfake audio samples.
- Aided in the creation and testing of new security systems implemented at the bank due to the emergence of new threats.

Integrated Product and Process Design

Fall2013 – **Lab Assistance**, *Dr. Bruce Welt*, Gainesville, Florida.
Spring 2014 Mechanical design lead on the development and test of a 4th generation high pressure O2 transmission rate test device under the Integrated Product and Process Design (IPPD) program for OxySense.

Vocational

May 2014 – **Undergraduate Lab Assistant**, *Dr. Bruce Welt*, Gainesville, Florida.
Aug 2014 Created instructional SolidWorks modules to enhance student coursework for Dr. Bruce Welt.

Spring/Summer **3D Modeling**, *Dr. Martin Welt, Entrepreneur* , Gainesville, Florida.
2014 Created SolidWorks prototype models for the patent-pending eye-wear GlareAway (https://www.iglareaway.com/).

Publications

[1] Hadi Abdullah, Aditya Karleka, Saurabh Prasad, Muhammad Sajidur Rahman, Logan Blue, Luke A. Bauer, Vincent Bindschaelder, and Patrick Traynor. Attacks as Defenses: Designing Robust Audio CAPTCHAs Using Attacks on Automatic Speech Recognition Systems. In *Proceedings of the 2023 Network and Distributed System Security Symposium, NDSS '23*, February 2023.

[2] **Logan Blue**, Kevin Warren, Hadi Abdullah, Cassidy Gibson, Luis Vargas, Jessica O'Dell, Kevin Butler, and Patrick Traynor. Who Are You (I Really Wanna Know)? Detecting Audio DeepFakes Through Vocal Tract Reconstruction. In *31st USENIX Security Symposium (USENIX Security 22)*, August 2022. (Acceptance Rate: 18.0%)

[3] **Logan Blue**, Samuel Marchal, Patrick Traynor, and N. Asokan. Lux: Enabling Ephemeral Authorization for Display-Limited IoT Devices. In *6th ACM/IEEE Conference on Internet of Things Design and Implementation*, May 2021.

[4] Hadi Abdullah, Muhammad Sajidur Rahman, Washington Garcia, **Logan Blue**, Kevin Warren, Anurag Swarnim Yadav, Tom Shrimpton, Patrick Traynor. Hear "No Evil", See "Kenansville": Efficient and Transferable Black-Box Attacks on Speech Recognition and Voice Identification Systems. In *42nd IEEE Symposium on Security and Privacy*, San Jose, CA, May 2021. (Acceptance Rate: 14.5%)

[5] Luis Vargas, **Logan Blue**, Vanessa Frost, Christopher Patton, Nolen Scaife, Kevin R.B. Bulter, and Patrick Traynor. Digital Healthcare-Associated Infection: A Case Study on the Security of a Major Multi-Campus Hospital System. In *Proceedings of the 2019 Network and Distributed System Security Symposium, NDSS '19*, February 2019. (Acceptance Rate: 17.0%)

[6] Bradley Reaves, Luis Vargas, Nolen Scaife, Dave Tian, **Logan Blue**, Patrick Traynor, and Kevin R.B. Butler. Characterizing the Security of the SMS Ecosystem with Public Gateways. *ACM Transactions on Privacy and Security*, December 2018

[7] **Logan Blue**, Luis Vargas, and Patrick Traynor. Hello, Is It Me You're Looking For? Differentiating Between Human and Electronic Speakers for Voice Interface Security. In *Proceedings of the 11th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, June 2018. (Acceptance Rate: 35.9%).

[8] **Logan Blue**, Hadi Abdullah, Luis Vargas, Patrick Traynor, and Thomas Shrimpton. 2MA: Verifying Voice Commands via Two Microphone Authentication. In *Proceedings of the 13th ACM ASIA Conference on Information, Computer and Communication Security*, June 2018. (Acceptance Rate: 20.0%)

[9] Bradley Reaves, **Logan Blue**, Hadi Abdullah, Luis Vargas, Patrick Traynor, and Thomas Shrimpton. AuthentiCall: Efficient Identity and Content Authentication for Phone Calls. In *Proceedings of the 26th USENIX Security Symposium*, August 2017. (Acceptance Rate: 16.3%).

[10] Bradley Reaves, **Logan Blue**, and Patrick Traynor. Authloop: Practical End-to-End Cryptographic Authentication for Telephony over Voice Channels. In *Proceedings of 25th USENIX Security Symposium*, August 2016. (Acceptance Rate: 15.5%).

[11] Bradley Reaves, **Logan Blue**, Dave Tian, Patrick Traynor, and Kevin R. B. Butler. Detecting SMS Spam in the Age of Legitimate Bulk Messaging. In *Proceedings of the 9th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, July 2016. *short paper*. (Acceptance Rate: 28.0%).

[12] Bradley Reaves, Nolen Scaife, Dave Tian, **Logan Blue**, Patrick Traynor, and Kevin Butler. Sending Out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways. In *Proceedings of the 37th IEEE Symposium on Security and Privacy*, San Jose, CA, May 2016. (Acceptance Rate: 13.0%).

Patents

Awarded

2017 Identity and Content Authentication for Phone Calls, US Patent 10 764 043

2019 Method And Apparatus Differentiating Between Human And Electronic Speakers For Voice Interface Security, US Patent 11 176 960

In-progress

2017 Practical End-To-End Cryptographic Authentication for Telephony Over Voice Channels, US Patent 11 176 960

2020 Detecting Deepfake Audio Through Vocal Tract Reconstruction, US Patent 17 443 654

Non-Technical Media

[1] Logan Blue and Patrick Traynor. "Deepfake audio has a tell – researchers use fluid dynamics to spot artificial imposter voices." In *The Conversation*, September 2022. Available at `https://tinyurl.com/2rz2fzz8`. This work was republished by arsTechnica available at `https://tinyurl.com/2p8y6feb`. Japanese Translation republished by TEXAL available at `https://tinyurl.com/585h9prb`. Polish Translation republished by Gazeta Wyborcza available at `https://tinyurl.com/5n6a2xb5`.

[2] Logan Blue. Deep Fakes and moral panic. On *Future Tense – Australian Broadcasting Corporation*. February 2023. Available at `https://tinyurl.com/3er2kffb`.

Technical skills

Programming Languages Python, Java, Scrapy, C, C++, SQL, MATLAB, LabVIEW, HTML, MIPS

Operating Systems Linux
○ Manjaro, Debian Jessie, Debian Stretch, Debian Wheezy, Ubuntu, Android
Windows
○ Windows 11, Windows 10, Windows 8-8.1, Windows 7
Mac OS
○ OS 11, OS X

Applications and Tools	Vim, SSH, Pandas, Docker, Tensorflow/Keras, Cuda, Latex, Ansible, MongoDB, Virtualbox, MySQL, RSA, AES, ECC, RESTful APIs, Solidworks, Metasploit, Microsoft Office

Course Work

Computer Science

Computer Networks
- Cyber-physical System Security
- Applied Machine Learning
- Foundations of Digital Signals
- Privacy and Machine Learning
- Computer & Information Security
- Cellular & Mobile Security
- Embedded & Mobile Security
- Computer & Network Security
- Entrepreneurship for Engineers
- Intro to Data Science
- Intro to Cryptology
- Advanced Data Structures
- Penetration Testing
- Analysis of Algorithms
- Distributed System Principles
- Mobile Computing
- Network Algorithms and Data Structures
- Programming Lang. Principles

Mechanical Engineering

Mechanics of Materials
- Thermodynamics
- Elem. of Electrical Engineering
- Engineering Materials
- Mechanical Design
- Fluid Mechanics
- Control of Mechanical Engineering Systems
- Intreg. Product/Process Design
- Finite Element Analysis

University Service

Graduate Services

2016 – Present	**Graduate Reviewer**, *Florida Institute of Cyber Security Research (FICS)*, Gainesville, Florida. Reviewed academic papers for publication in various forms: - IEEE Security & Privacy (IEEE S&P) '22 - Transactions on Dependable and Secure Computing (TDSC) '21 - Network and Distributed System Security Symposium (NDSS) '21 - USENIX Security '21 - ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec) '20 - USENIX Security '20 - Network and Distributed System Security Symposium (NDSS) '20 - USENIX Security '19 - ACM Conference on Computer and Communication Security (CCS) '17 - USENIX Security '17 - ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec) '17 - Workshop of Offensive Technologies (WOOT) '16