Ron Thompson

ronthompsoniii@protonmail.com | linkedin.com/in/ronthompson1992 | zenw00kie.github.io

I am a Computer Science PhD candidate specializing in medical device security, combining top-tier academic research in addition to eight years of hands-on experience in data engineering, quantitative analysis, and national security. My research, published at venues like USENIX Security, focuses on translating the operational realities of complex environments—from hospital networks to industrial control systems—into effective, usable security solutions. I deconstruct workflows in threat modeling and vulnerability management to build better tools and processes, bridging the gap between deep technical analysis & real-world operational needs.

EDUCATION

Tufts University | Medford, MA | Sep 2021 – May 2026 (Exp)
PhD in Computer Science
Thesis: It's a Beautiful Day to Secure Patients: Developing Cyber Resiliency in Healthcare Grounded in Clinical Realities

University of Colorado, Boulder | Boulder, CO | May 2019 - May 2020
Post-Baccalaureate Coursework in Computer Science

Georgetown University | Washington, D.C. | Aug 2010 – May 2014
BA in Government conc International Law; Minor in History

WORK EXPERIENCE

Tufts University | Medford, MA — Sep 2021 – Present
A private, R-1 research, university located in Medford, Massachusetts.
Research Assistant, Tufts Security & Privacy Lab (Advised by Daniel Votipka)

Research at the intersection of usable security, systems security, and healthcare while grounded in regulatory frameworks including FDA pre/post-market guidance, EU MDR/IVDR, AAMI TIR57, and the NIST CSF. Some research includes:

- ***Clinician-Centered Security***: Led a multi-national study investigating clinicians' security perceptions, revealing a mismatch between clinical workflows and existing security controls.
- ***Vulnerability Intelligence Platform***: Designed and built a large-scale OSINT platform (`lamplighters`) to scrape, parse, and standardize security advisories from hundreds of sources (CNAs, NVD). Project involves data orchestration (`Apache Airflow/Prefect`), containerization (`Docker`), entity name resolution, and a mix of probabilistic and LLM-driven parsing to build a dataset for novel vulnerability severity metric research (CVSS, EPSS). Working with CISA Coordinated Vulnerability Disclosure team to provide ongoing data.
- ***Medical Device Threat Modeling***: Led a qualitative study with 12 industry experts to develop a process model of how practitioners perform threat modeling in real-world, regulated environments.
- ***Threat Modeling Tool Development***: Led a team of undergraduates to architect and build a tool (TMNT); personally developed the core Domain-Specific Language (DSL) and recommendation engine. The application is built on a set of `gRPC` microservices with a `Django` and `d3.js` frontend.
- ***SBOM Management & Triage Tooling***: Advising on the development of an observability platform built on Dependency-Track to analyze how security analysts augment SBOMs and triage component vulnerabilities.

MedCrypt | Remote — May 2022 – Dec 2023
A start-up providing medical device manufacturers with cybersecurity services.
Co-Op & Freelance Consultant

Built threat models and created security artifacts for medical device manufacturers to support FDA/EU regulatory submissions, applying frameworks including NIST 800-30 and AAMI TIR57. Co-developed and conducted a threat modeling training workshops for medical device manufacturers. Supported the company's Vulnerability Management as a Service (VMaaS) offering.

GroundWatch | Boulder, CO — Jan 2020 – Aug 2021
A start-up that built technology solutions for the US Department of Defense.
CEO/Co-Founder

Co-founded a startup focused on situational awareness and sensor fusion for a Counter-UAS platform for clients including USASOC. Designed the data processing pipeline to ingest and fuse raw signals from audio and visual

sensors, feeding predictive models to identify and track potential threats. Stack included: `Python`, `Docker`, `Redis`, `ELK`, and `RabbitMQ`.

Point72 Asset Management | New York, NY/Stamford, CT — Apr 2016 – Mar 2019

A long-short hedge fund run by Steve Cohen and managing $13B

Quantamental Analyst, Healthcare Portfolio Team — Aug 2017 – Mar 2019

Developed a full data pipeline to ingest, process, and model alternative healthcare data (claims, EHR, purchasing), using a mix of `Python (pandas, scikit-learn)`, `Spark`, `Jenkins`, `RabbitMQ`, `SQL Server`, and `Ansible`, for a quantamental MedTech and Life Sciences portfolio. Built an analytical REST API in `Python (flask)` to empower fundamental analysts to conduct statistical analysis of complex datasets.

Associate, Market Intelligence — Dec 2016 – Aug 2017

External Consultant, Market Intelligence — Apr 2016 – Dec 2016

Additional Data Science & DevOps Experience | Various — Apr 2014 – Sep 2021

Contract Consulting | Second Foundation Capital & Second Foundation Advisors — Apr 2019 – Sep 2021

A family office focused on private equity and associated consulting business.

Contract Consulting | Environmental Defense Fund — Sep 2019 – Feb 2020

A nonprofit environmental advocacy group.

Digital Analytics Director & Cybersecurity Lead | Jeb! 2016 — Aug 2015 – Mar 2016

A Presidential campaign to get Jeb Bush elected as President of the United States for the 2016 election.

Consultant - Rapid Prototype Application Developer | Booz Allen Hamilton — Apr 2015 – Aug 2015

A management and information technology consultancy..

Data Engineer & Consultant | 0ptimus Consulting — Apr 2014 – Apr 2015

A data consultancy working mainly with political organisations.

SELECTED PUBLICATIONS

A full list of publications can be found at zenw00kie.github.io.

Thompson, R. E., Boshar, L., Vasserman, E. Y., & Votipka, D. "Navigating the Patchwork: Investigating the Availability & Consistency of Security Advisories." *Proceedings of the 2025 IEEE Secure Development Conference (SecDev '25')*.

Thompson, R. E., McLaughlin, M., Powers, C., & Votipka, D. "'There are rabbit holes I want to go down that I'm not allowed to go down': An Investigation of Security Expert Threat Modeling Practices for Medical Devices." *Proceedings of the 33rd USENIX Security Symposium (USENIX Security '24)*

Thompson, R. E., et al. "The Threat Modeling Naturally Tool: An Interactive Tool Supporting More Natural Flexible and Ad-Hoc Threat Modeling." *Proceedings of the Workshop on Security Information Workers (WSIW '24), Co-located with USENIX SOUPS 2024*.

SKILLS & CERTIFICATIONS

- Security & Research: Threat Modeling, Vulnerability Management (CVSS), Medical Device Security (FDA), ICS/OT Security, Usable Security, Network Security, Experimental Design, Bayesian Modeling, Qualitative & Quantitative Analysis, SBOM
- Network Analysis: Network Traffic Analysis (PCAP, Wireshark)
- Programming & Data: Python, R, Java, SQL, Spark, Bash, Git
- DevOps & Data Engineering: Amazon Web Services (AWS), Google Cloud Platform (GCP), Apache Airflow, Prefect, Jenkins, Docker, PostgreSQL, SQL Server, REST APIs, Redshift, Redis, ELK, Databricks, Linux, Github Actions
- Certifications: Virtual Industrial Control Systems Cybersecurity Training (CISA), Industrial Control System Cybersecurity Lab (CISA)
- Clearance: DoD Secret (Inactive)