*Research Statement*

# Gedare Bloom

## 1 Introduction

My approach to research is to ask: **What security problems face embedded systems that will be fielded for decades?** Embedded and cyber-physical systems are increasingly vulnerable to attack because of network access, and harder to analyze due to hardware and software complexity. **My research aims to improve the security of distributed, real-time embedded cyber-physical systems**. I investigate solutions along the hardware-software interface by applying techniques from security, computer architecture, operating systems (OSs), and real-time analysis.

As a practical matter, **my role as a maintainer for the RTEMS open-source hard real-time OS gives me a direct line for transitioning research to practice**. RTEMS is used in projects such as robotics frameworks (Orocos, Rock), unmanned vehicles (Mitre's Centaur, DRDC's Raptor UGV, NASA's Curiosity rover), satellites and space probes (NASA, ESA, CubeSat), automotive (BMW), defense (Boeing, U.S. Army), building automation (LOYTEC), medical devices, industrial controllers, especially as part of the Experimental Physics and Industrial Control System (EPICS) package in use at most particle accelerators (Argonne, Brookhaven, Los Alamos, and Oak Ridge National Labs, SLAC, CERN), and more. My tangible contributions include the first 64-bit port of RTEMS and a modern thread scheduling infrastructure that I implemented to evaluate my research.

## 2 Ongoing Research

### Automotive Security: Fail-Operational Intrusion Detection System

Automotive vehicle cybersecurity becomes more important as automobiles become more connected and intelligent. The security of every vehicle on the road is necessary to ensure the safety of every person on or near roadways. The objective of this project is to protect in-vehicle networks from remote cyber attacks. The method of protection is a distributed in-vehicle network intrusion detection system (IDS) with fail-operational mode changes that can provide graceful degradation of service and initiate recovery without compromising human safety. The fail-operational approach to IDS accounts for CPS requirements and could revolutionize CPS security by arming engineers and end users with the understanding and ability to protect from malicious attacks while maintaining operational safety guarantees. Three Ph.D. students and three REU participants have been partially supported by this project. One of these Ph.D. students defended his dissertation and graduated in May 2018. Another of the students worked in the Vehicle Security Center at Oak Ridge National Lab during Summer 2017. This project so far has produced six papers with more accepted to appear or in submission. The project is supported in part by NSF grant 1646317 (PI: Gedare Bloom, $250,551, 10/2016-09/2019).

### Real-Time Operating System and Network Security for Scientific Middleware

This project adopts and adapts modern security techniques and tools into open-source real-time operating system (RTOS) software and middleware used for scientific industrial control systems. In particular, security enhancements are being made to the Real-Time Executive for Multiprocessor Systems (RTEMS) RTOS and the Experimental Physics and Industrial Control System (EPICS) open-source projects that are widely used in scientific CPS deployments. EPICS is in use at national and international scientific installations to control particle accelerators and telescopes. The result of this project will be a cyberattack-resilient scientific CPS infrastructure with immediate benefits to the high-energy physics scientific community. Techniques that are adopted in this project include: static analysis and security fuzzing as part of continuous integration; cryptographic security for the open-source software development life cycle; secure boot and update for remotely-managed scientific CPS software; open-source cryptographic libraries for secure communication; real-time memory protection; formal modeling and analysis of network protocols used by scientific CPS middleware; enhanced security event logging; and network-based intrusion detection for scientific CPS middleware. This project is currently supporting three Ph.D. students and one postdoc from NSF Grant 1839321 (PI: Gedare Bloom, $999,915, 10/2018-09/2021).

## 3 Future Research

My plans for future research follow three directions: **security for cyber-physical systems, security for real-time systems, and security for the Internet of Things (IoT)**. I will pursue these research directions using techniques from security, real-time OS, and computer architecture, and leveraging my experience building experimental infrastructures. Potential funding sources for this research are many and include NSF, DoD, NSA, NGA, space agencies (NASA, NRO, ESA), and industry partners. The following describes my plans for each of the three directions.

1. *CPS Security.* I will continue to work on advancing the state-of-the-art in CPS security extending from my current progress with automotive and industrial control security. The possibilities for **interdisciplinary research** in this area are significant. I plan to find collaborators in other departments to pair my security and embedded system knowledge (cyber) with their engineering subject matter expertise (physical). This research shows promise for domestic, international, and industry funding.

2. *Real-Time Security.* Security techniques for general-purpose systems are built on hardware building blocks such as processor privilege levels, memory management units, and modern techniques that leverage virtualization, trusted execution engines, and secure enclaves. Unfortunately, security building blocks are often missing or disabled on low-cost, latency-oriented real-time embedded systems, so the approaches for securing general-purpose systems do not translate to the real-time embedded systems domain. I plan to investigate practical security solutions for real-time embedded systems and to build capacity for real-time security, which is an underexplored area yet one which has huge potential for broader impact. I will propose this research for an NSF CAREER.

3. *IoT Security.* Device heterogeneity and emerging communication protocols make it difficult to understand the scope of an IoT application's attack surface, much less secure it. I am planning to construct IoT research testbeds to enable further research exploration in the area of IoT protocol and device security. Such testbeds require solving significant research challenges such as virtualization of physical world and cloud platforms, while the construction of a testbed will open research directions with a unique capability to explore them. The development aspects of creating IoT security testbeds will also make for excellent undergraduate projects. This project has garnered interest from government (DHS) and industry (Northrop Grumman).

## 4 Involving Undergraduates

I routinely find opportunities for undergraduate students to assist as an integral part of a research project team. I have a successful track record of publications involving students. Prior undergraduate student members of my lab include 5 African American female students and 3 male students. Undergraduate students receive training in the conduct of ethical and sound research practices, and mentoring to prepare them to enter the career path of their choice. My mentoring style is to guide students through incremental tasks leading toward a research goal, which sustains momentum and increases success. Despite their significant time constraints, I have found that **undergraduate students can be enthusiastic and hard-working when motivated and given incremental tasks for research problems**. I look forward to continuing to work with students at all levels.

## 5 Conclusion

My research investigates how real-time embedded systems can be made secure by improving how hardware and software support each other. I work all along the systems stack, from low-level digital logic to high-level runtime software support, to find solutions for the problems faced by modern systems. This research area will continue to matter, because the embedded and cyber-physical system market grows by billions of devices shipped each year, and users demand faster, cheaper devices with more features that cause security challenges. My future research aims to make real-time and cyber-physical systems secure, which is an important cross-cutting concern in all modern computer systems.