COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

DISSERTATION DEFENSE

Andrew Loveless

Overcoming the Performance and Security Challenges of Building Highly-Distributed Fault-Tolerant Embedded Systems

Monday, April 24, 2023
10:00am – 12:00pm
Virtual – Zoom
Password:defense

ABSTRACT: Over the past few decades, embedded systems, like those in spacecraft and aircraft,have evolved into complex distributed systems with hundreds of nodes and thousands
of traffic flows. Meeting requirements in these systems is a significant challenge. For example, embedded systems are often required to mask faults, which typically requires redundant processing nodes to coordinate by exchanging messages. Unfortunately, this need for coordination can lead to high worst-case latencies that make it hard or impossible for systems to meet deadlines. Another challenge is security. As embedded systems have grown, designers have looked for new ways to reduce size, weight, and power. One popular approach is to use mixed-criticality networks, which let systems share a single network between critical and non-critical devices. These networks are designed to isolate the critical devices, like flight computers, from the non-critical devices, which often come from unsecured supply chains. However, the existence of shared network resources provides a potential means for attackers to bypass these isolation guarantees.

To overcome the performance challenge, I introduce two new Byzantine fault-tolerant state machine replication protocols. The first, IGOR, leverages multi-core processors to enable replicas to perform speculative eager executions on different sets of redundant sensor data at the same time. A coordination protocol is used in the background to determine which execution will determine the system's final state, reducing the system's latency to the time needed for either execution or coordination – whichever takes longer. The second, CrossTalk, exploits the popularity of redundant switched networks in modern systems. Using novel algorithms to move sensor data back and forth between the redundant planes, CrossTalk can ensure replicas maintain identical state without requiring any communication between the replicas. To illustrate the security challenge, I introduce PCspooF, a new cyberattack on Time-Triggered Ethernet (TTE) networks used in spacecraft, aircraft, and industrial control systems. PCspooF is the first attack capable of breaking TTE's isolation guarantees, allowing a single non-critical device to potentially disrupt synchronization of all critical devices. The disclosure of PCspooF has caused multiple large aerospace companies to implement mitigations, as well as driven changes to the TTE standard (SAE AS6802).

CHAIR: Prof. Ronald Dreslinski and Prof. Baris Kasikci