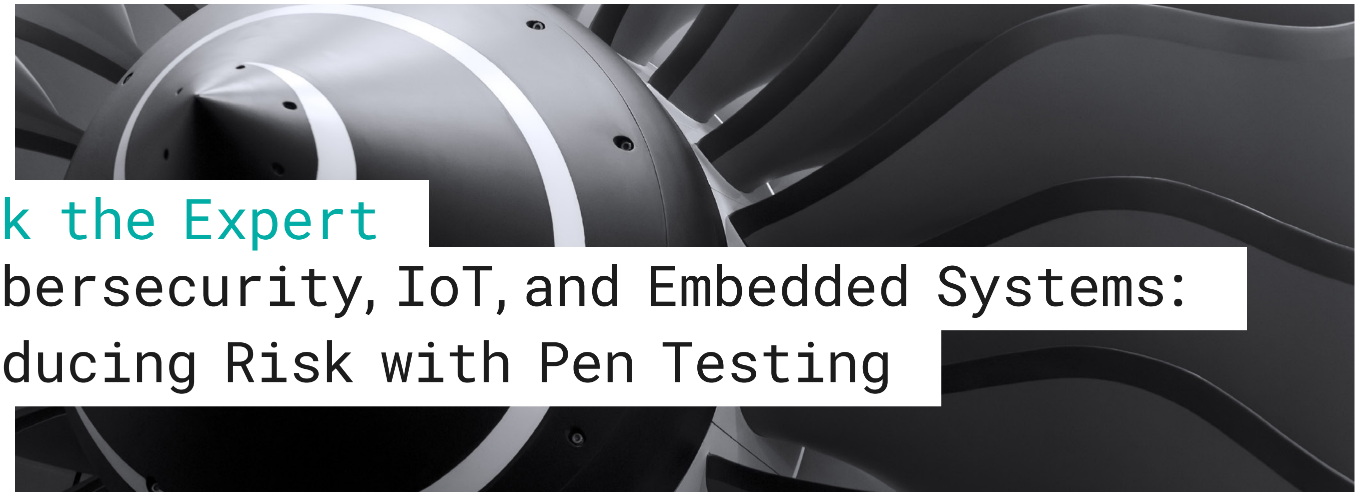
WNDRVR



Ask the Expert
Cybersecurity, IoT, and Embedded Systems: Reducing Risk with Pen Testing

SEAN EVOY
Product Line Manager, Wind River

Cybersecurity burst upon the embedded systems landscape in 2016, when the infamous Mirai Internet of Things botnet took down major websites using hundreds of thousands of compromised IoT devices.[1] Mirai was possible because IoT developers didn't include security high on the list of design requirements for their low-cost, widely deployed products. This was a wake-up call for embedded developers, whose systems were among the first to have to coexist with Industrial IoT (IIoT) devices.

Worse, critical embedded systems proved vulnerable to cybersecurity attack sooner than anyone had expected. Shortly after Mirai, a U.S. Department of Homeland Security (DHS) Cybersecurity Division team demonstrated a remote hostile penetration of a Boeing 757, using off-the-shelf hardware and software that readily passed through airport security.[2] And in 2019, DHS issued an alert warning of hacking vulnerabilities in Controller Area Network (CAN) data buses used on some large aircraft.[3]

Cybersecurity threats reach beyond aviation: Automobile automation of emergency braking, collision warning, and other driver assistance technologies are already widely deployed. Building automation systems have been subject to "cyber ransom" attacks that cost tenants millions of lost operating hours.

To complicate things, embedded systems specifications such as DO-178C/278A, dating from 2012, are challenged to adapt to today's fast-moving cybersecurity vulnerabilities. As system complexity grows, attack surfaces between interoperating systems increase exponentially, across new bus architectures, HMI, IP networks, and data protection, both at rest and in transit.

Foiling Cybersecurity Risks at the Source

As an embedded systems developer, you can get ahead of cybersecurity problems through vulnerability testing, called penetration testing ("pen testing") in the IT world, and fault injection in the embedded engineering community.

A pen test is a simulated attack on a system to detect known vulnerabilities. A library of known attacks, or faults, drives an automated tool that injects each fault and analyzes the device-under-test response. This testing uses unmodified binaries, so there is no risk of unintentional interference by test rigging. As new vulnerabilities accumulate in the fault library, you rerun the penetration exercise as part of your standard regression testing process.

Pen testing is one of the best ways to mitigate cybersecurity risk, because you use it throughout a system's lifecycle: during development, deployment, and after each modification. One of the most effective ways to deploy pen testing is via simulation engines, such as Wind River® Simics®. Simics lets you decouple your work from physical hardware, while still retaining the ability to connect physical hardware when required. Simics virtual hardware gives you on-demand access to any target system, supporting continuous integration and automated testing with members of your development team, or even suppliers.

Simics uses virtual hardware to conduct full-system simulations, which is often the only way to detect cybersecurity threats that originate with one component attacking others. The advantages of this approach are:

1. You can conduct tests not possible on physical hardware, such as spoofing malware to trigger a response that exposes its existence.
2. Developers can test defense-in-depth strategies, such as flagging a suspect component as inoperable, isolating it from the system.
3. Simics can act as a cybersecurity “sandbox,” safely containing suspect malware for forensic analysis.

Simics goes beyond simulating processors and boards; it assembles complete networked systems running the full production software stack runs. As noted earlier, these are unmodified binaries, including BIOS, firmware, operating systems, and applications. Recent Simics releases improve multi-core and parallel core support. Fully parallel simulation is on the horizon, and today Simics provides support for distributing complex, multi-core simulations across available host resources. The only restriction on the complexity of the system or its performance requirements is the capacity of the simulation host network.

And despite its simulation focus, you can still use pass-through technology to connect physical hardware via standard interfaces, such as Ethernet, I2C, PCI, SCSI, serial, and USB.

Regression testing is an important part of verifying security fixes. Simics isn’t new to the full-system regression testing role. It’s been successfully employed by the largest system integrators to ensure platform reliability. For example, NASA’s Independent Test Capability Team uses Simics in its NASA Operational Simulator (NOS), which models complete spacecraft missions in real time to verify flight-ready software and hardware.[4]

Make Simics Your Next Step in Cybersecurity Defense

With cybersecurity threats exploding for embedded systems, now is the time to begin pen testing your mixed-criticality systems. Because Simics can simulate systems from tiny stand-alone modules up through complete systems running complex missions, it should be part of your security testing tool kit.

About Sean Evoy

As the product manager for Wind River Simics and Wind River Workbench, Sean Evoy is responsible for bringing new product and solution innovation to market to assist customers with their most complex development lifecycle problems. The tools portfolio addresses customers across all Wind River market segments, including aerospace and defense, cybersecurity, industrial automation, utilities, and transportation.

Before managing Simics and Workbench, he was responsible for the Wind River Industrial Internet of Things offering. He has a Bachelor of Computer Science degree from Carleton University and a Bachelor of Arts degree with a major in history from the University of Ottawa.

[1] *blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/*
[2] *www.cbsnews.com/news/homeland-security-hacked-boeing-757-jetliner/*
[3] *aviationweek.com/air-transport/dhs-warns-hacking-vulnerability-aircraft-avionics*
[4] *www.youtube.com/watch?v=BEiP2YjknvE*