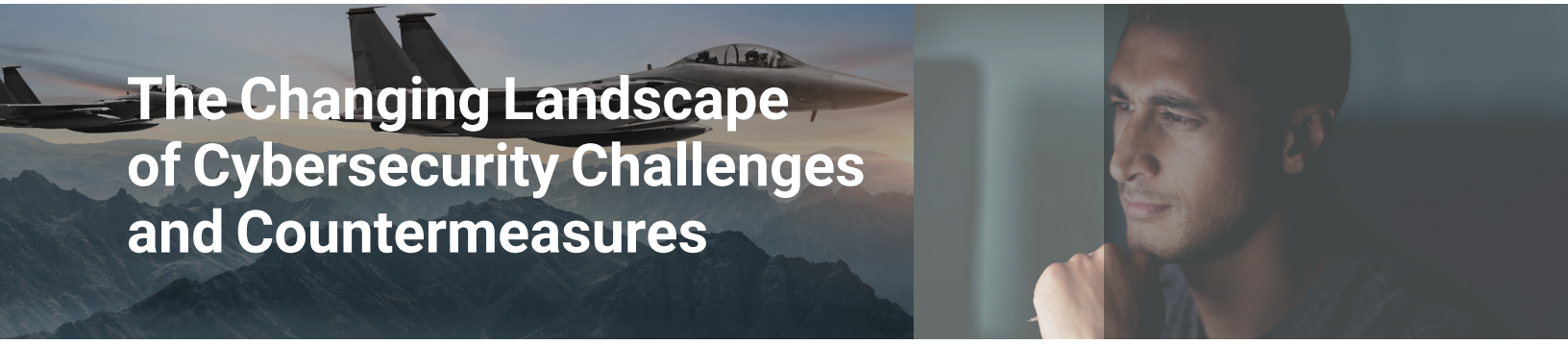
Cybersecurity Trends in Aerospace and Defense Applications

WNDRVR



The Changing Landscape of Cybersecurity Challenges and Countermeasures

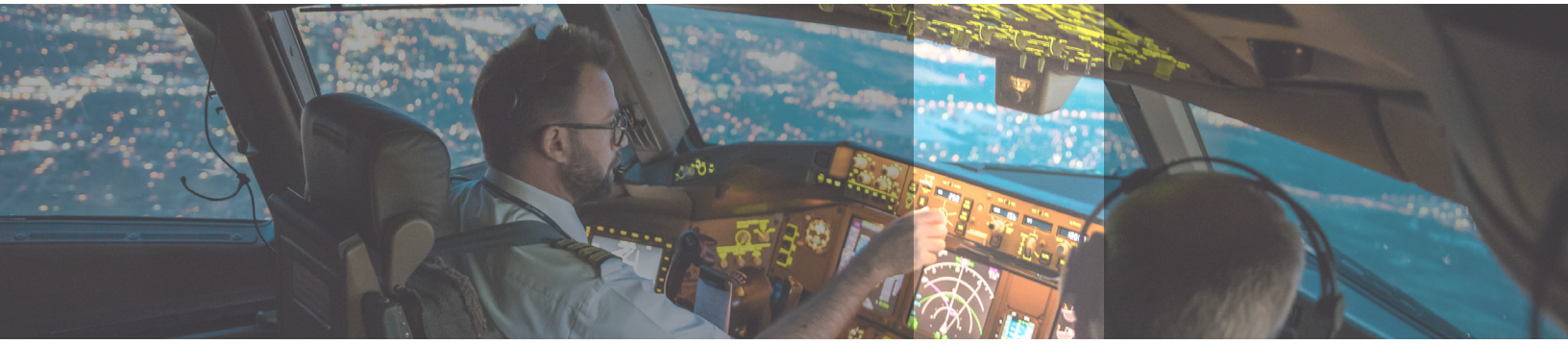
The nature of cybersecurity has taken a dire turn across the aerospace and defense industry as threat vectors multiply and incidents such as the SolarWinds attack have caught many organizations unprepared.

Cybersecurity has always been a never-ending battle between developers devising new kinds of protection for systems and hackers creating new mechanisms for thwarting these protections. In the U.S., this threatening dance reached a pinnacle in March 2020, with an unanticipated attack from a group dubbed Cozy Bear, identified by *The Washington Post* as a hacking arm of the Russian government. The attack on the American company SolarWinds was traced to malware spread through a back door exploited by a trojanized component. It breached massive numbers of high-profile computer systems, including those of many major U.S. government agencies, private financial organizations, and universities. The SolarWinds attack, which targeted the company's software update product Orion, was a reminder that new vulnerabilities continue to arise, taxing the abilities of those tasked with protecting data and systems.[1]

Aerospace and defense companies have a particularly difficult mission in protecting and maintaining mission-critical systems and insulating them from cybersecurity threats. An online cybersecurity expert discussion recently hosted by *Defense Daily* explored emerging vulnerabilities and detailed the challenges faced by the industry in identifying and mitigating attacks.

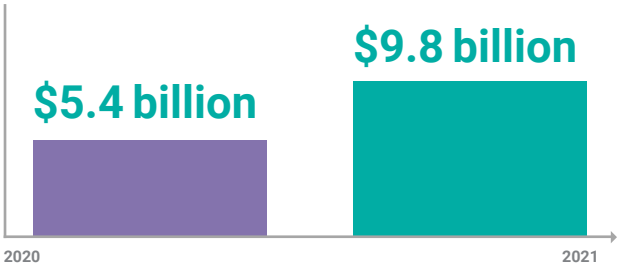
The annual cost of cybercrime to the global economy by 2025[2]

1 *Lucian Constantine, "SolarWinds Attack Explained: And Why It Was So Hard to Detect," CSO, December 15, 2020*
2 *Steve Morgan, "Cybercrime to Cost the World $10.5 Trillion Annually by 2025," Cybercrime Magazine, November 13, 2020*



Participants in the discussion were Cal Biesecker, discussion moderator, Homeland Security reporter for *Defense Daily*, and editor of the newsletter *Homeland Security Report*; Matt Areno, the principal engineer and lead of Intel Corporation's Security Assurance and Cryptography Team; Steve Edwards, Technical Fellow and director of Secure Embedded Solutions at Curtiss-Wright; and Irby Thompson, vice president of Security Product Sales at Wind River®.

The following sections highlight the ideas and key points that were covered during this discussion.



U.S. DoD cybersecurity spending requests jumped by 81% from 2020 to 2021[3]

3 *John Keller, "Top Technology Challenges This Decade for the Warfighter," Military & Aerospace Electronics, January 28, 2021*

Introduction: Wake-up Call

The severity of the SolarWinds attack and other recent high-profile cyberattacks is just reason for a rethinking of the basic tenets of effective cybersecurity. Panelists weighed in on what they considered the most disturbing security issues facing the industry today.

Irby Thompson stated, "One of the main things that is keeping me up at night is the audacity and breadth of the recent attacks we have seen, with SolarWinds being a supply chain attack and Hafnium[4] being a zero-day vulnerability attack; and watching nation states jump on these and hack anything and everything that they can get their hands on. It seems like the gloves have come off. Instead of doing targeted information operations, we are now seeing, on a very broad scale, trying to own systems en masse. We always seem to be one hack away from total compromise."

Matt Areno added, "All of these things that we security researchers have thought about, have considered, have worried about, have come to fruition. What keeps me up at night is not what I'm seeing in the news — it's what I'm not seeing."

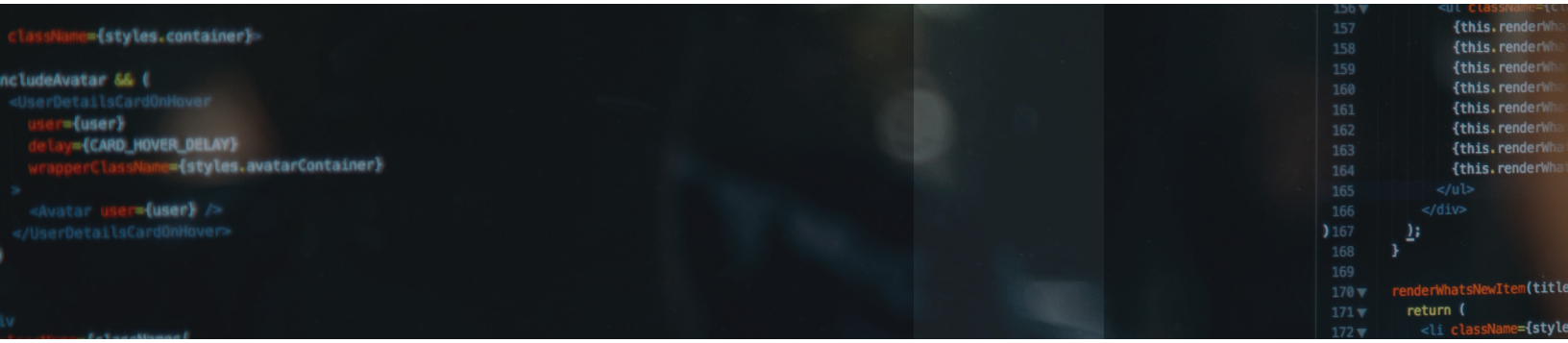
"I think another thing that keeps me up at night," said Steve Edwards, "is the insider threat. We try to protect against the attacks coming from outside, but what about the attacks coming from the inside? Somebody who might put a piece of malware in the operational code that you don't know about. There may be too broad an access to certain things."

Thompson noted that many commercial companies don't have national security as their primary interest. "Many of the commercial companies that are new to A & D," he said, "don't really understand the threats they

"It seems like the gloves have come off. Instead of doing targeted information operations, we are now seeing, on a very broad scale, trying to own systems en masse. We always seem to be one hack away from total compromise."

—Irby Thompson
Wind River

4 *Tom Burt, "New Nation-State Cyberattacks," Microsoft on the Issues, March 2, 2021*



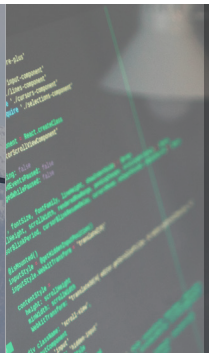
are up against. A hack connected to a leading computer system board company a few years ago was a good example: Even if a company does things right, if they are international and they don't have good control of their supply chain, they become a threat vector to the overall defense space."

From an Intel perspective, speaking about security from the commercial side, Areno noted, "We don't have the same leeway that defense contractors and others have. We are a global company. We serve governments all around the world. We have got to continue that support for those governments. That is why you have seen a big push from Intel in the compute lifecycle assurance initiative and our transparency supply chain initiative. [This is] to help people understand what our supply chain looks like, what we are doing to mitigate risk and concerns, and how we are trying to work with governments [on] those regulations — developing laws and procedures — to help them have some level of confidence in the integrity of the product we are providing."

ESPIONAGE CONCERNS FOR THE A&D INDUSTRY

Attacks such as the SolarWinds incident, which appears to be linked to espionage by a rival nation state, raise deeper concerns for the aerospace and defense industry over aircraft breaches, weapon systems hacks, and similar threats.

"The challenge being," Thompson explained, "that if your enterprise network is compromised and you are doing your development of your weapons platform or your aerospace system on that enterprise network, it certainly makes sense that it can be jumped. Attacks can be jumped all the way down into the code that is going to be deployed. One of the benefits of working in defense is that you can classify certain activities and you can put them on closed networks, but it creates a burden to do that. It is a balancing act."


Thompson continued, "There is work being done at the highest federal levels, looking at how we can change the way we do business so that we can provide real-time threat information to private companies to prevent the next Hafnium or to mitigate that kind of threat vector. It takes a coalition of the willing to solve the problem."

"The supply chain is a big concern," Edwards said. "We're buying hardware [and] software that ends up being developed all around the world. That is part of the globalization of the economy.... It's semiconductors being made in Asia or software in India. We are using commercial components; nobody is using military-grade components anymore. Very few systems are developed using [the DoD model] trusted foundry.[5] You are using a lot of commercial processors, FPGAs, memory — so you have got to be very diligent in your supply chain, and that is a hard thing to get your head around because it is so complex."

LOOKING AT THREATS FROM A FRESH PERSPECTIVE

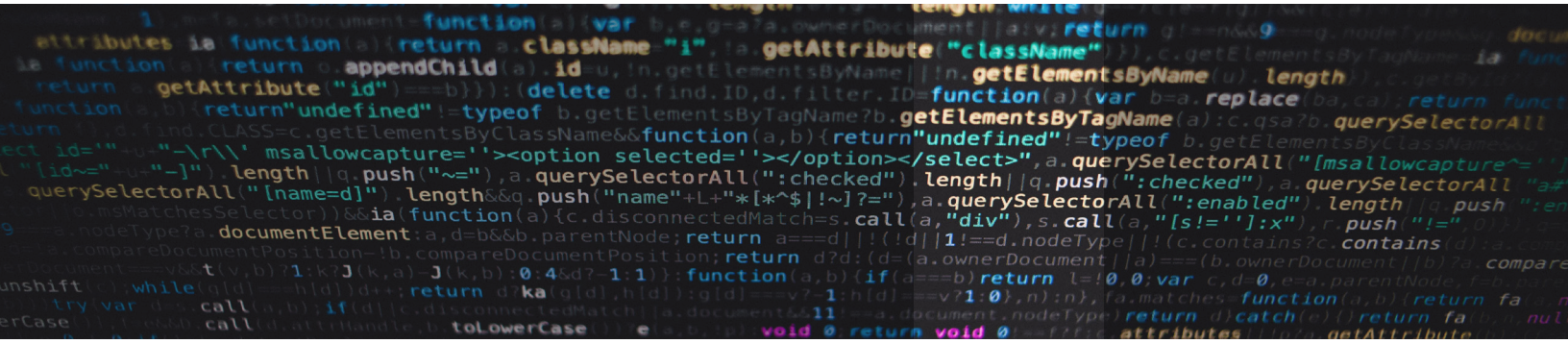
A change over the last several years, according to Thompson, is that "there was a push for cyber-resilience, and the idea here is instead of assuming we can keep the bad guys out, let's look at how to deal with the insider threat and the bad guys getting some level of access. 'Zero trust' is another buzzword initiative. Let's assume that the hackers are already in, to some degree. How does that change the way we build our system? How do we make it so there is not a single-point failure to access information or to have the system integrity go down?"

"What we really learned from SolarWinds: Look at what someone can do when they have access [to] your network," Areno commented. "It is more than just using access within your network to further attack things

> The dark web — the part of the deep web where malware, exploit kits, and cyberattack services are peddled — is estimated to be growing exponentially. By some estimates, the deep web is 5,000 times larger than the surface web.
>
> —*Cybercrime Magazine*[6]

5 *C. Todd Lopez, "DoD Adopts 'Zero Trust' Approach to Buying Microelectronics," DoD News, May 19, 2020*

6 *Steve Morgan, "Cybercrime to Cost the World $10.5 Trillion Annually by 2025," Cybercrime Magazine, November 13, 2020*



in your network. How can they exploit or attack others, your customers, the people that you work with — how can they leverage the trust that exists between companies by taking over your network and doing something?"

SECURITY BY DESIGN

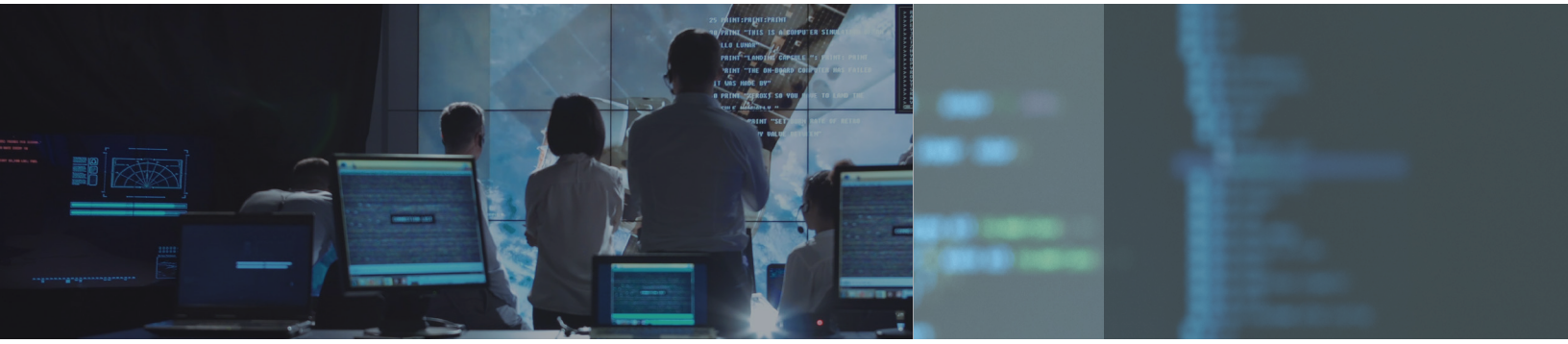
Can a rating system created by a standards body or other organization help measure the threat potential?

"It is a hard problem to measure the [quality] of security," Thompson said. "At the same time, having some standards, or at least an external audit that gives you a rating on the cleanliness of your supply chain, of your software development processes — I think [that] is absolutely required. I think it is the direction we need to go. The current system we have is failing us."

Areno added, "I remember being at an industry conference a year or two ago. We were talking about the need to be able to provide identity and attestation of devices and be able to provide some type of verification of the source, of the firmware — cataloging this information to be able to establish this type of trust. We talked about how important that was and how we needed it, and then we looked around at each other and said, 'OK, who is doing this?' And eventually someone said, 'I guess I can quit my job and start up the company to do it.' That's part of the problem. Who does it? Who is in charge of it? What does it entail?"

"There are lots of good best practices out there," Edwards said, "but nobody is really monitoring or policing to see that everyone conforms to them. Everybody has got their own cybersecurity that they want to follow, and it is not coordinated from the top down. I don't think there is one point to go to and say, 'What are my requirements from a cybersecurity perspective?'"

> "There are lots of good best practices out there, but nobody is really monitoring or policing to see that everyone conforms to them."
>
> — **Steve Edwards**
> Curtiss-Wright



LEVERAGING GOVERNMENT BUYING POWER

Can the government do more to leverage its buying power to gain more security in the components it chooses for platforms and solutions?

"Yes," Thompson said, "the government is trying to flex its muscle with more flow-down requirements in all contracts, the CMMC [Cybersecurity Maturity Model Certification] being one of the latest iterations. In some ways, the challenge that we have is that there are so many different government bodies bringing so many different requirement sets that it is overwhelming to a performer to know what applies and what doesn't. If we had a Central Office of Cybersecurity, it could be prescriptive of what applies in any given situation."

Thompson noted that the challenge the government faces is that "a lot of critical infrastructure is privately owned and operated. [It has] limited authority over what can and should be done there at this point."

To Thompson's point, Areno said, "The difficulty is that it is not constrained to just the U.S. Government. All across the world [governments] are recognizing that this is … a problem, and they are not always working together. I would be huge fan of an international effort to do this; we've got to come together and recognize that this is not a single-nation problem."

Edwards stated his agreement, adding, "The government is trying, but [it's] also playing a little bit of catch-up. They have been behind the commercial [sector] in terms of dealing with cybersecurity, I think. And they are flowing down requirements that we didn't see five years ago. I think we will see more of that in the future. It is a hard problem … are we really incentivized to solve the cybersecurity [problems], or are we incentivized to deliver the product at the cheapest price and win the contract for the government?"

> "The difficulty is that it is not constrained to just the U.S. Government. All across the world [governments] are recognizing that this is … a problem, and they are not always working together."
>
> **— Matt Areno**
> Intel Corporation

COST ANALYSIS FOR COMMERCIAL COMPLIANCE WITH NIST 800-171

Would it be beneficial for commercial companies to meet the compliance guidelines of NIST 800-171, which specifies handling of Controlled Unclassified Information (CUI)?

Areno's response was, "There is a lot of work that goes into those and in being compliant.... Any company that is looking into that has to do a cost analysis. How much effort is it going to take to ... do this, and what I am going to get out of it? When there is no requirement, it becomes a little bit harder of a sell.... I think for the most part [compliance could] weed out and protect against a lot of attacks that are out there. It ensures that companies are protected against everything. But it would certainly raise the bar."

Edwards concurred, stating, "I think it is about economics. Companies are trying to make a profit on the products they sell, and it takes money and effort to invest in cybersecurities." So requirements would need to exist, he noted, whether they came from "the government flowing them down to their prime contractors or, in the commercial industry, for people to really say there are cybersecurity standards that you have to meet for you to sell this. For example, think about a washing machine that happens to be connected to the internet, so you can check on your wash cycle via your phone app. If there are no requirements for that, people aren't going to invest in it. It is money they are investing that they are not going to see any return on."

SECURITY FOR AEROSPACE VS. ENTERPRISE IT

How is the security for aerospace environments different from those of enterprise IT environments?

"I think it is about economics. Companies are trying to make a profit on the products they sell, and it takes money and effort to invest in cybersecurities."

— **Steve Edwards,**
Curtiss-Wright

"Certainly," said Areno, "I think there is a difference there just from the safety perspective. There is a lot of difference if an aircraft gets hacked in the middle of the air as opposed to a portion of a corporate network going down during the day.... There are concerns about how we update and provide better security on these systems that are out in the field. That is one of the things I am proud to say that I am working on at Intel … one of the new capabilities that we are finalizing and getting ready to release [is] called Edge-Control Bridge. This is a microcode update that we can provide on our products that is significantly improving the security capabilities, allowing us to do encrypted boot off a PCI Express device, in-line encryption of memory, partitioning of cores within the processor. A lot of these capabilities are things that we can backport to existing solutions. That becomes especially important in these safety-critical systems, because the hardware and the software must stay the same. But how can I improve the security of it?"

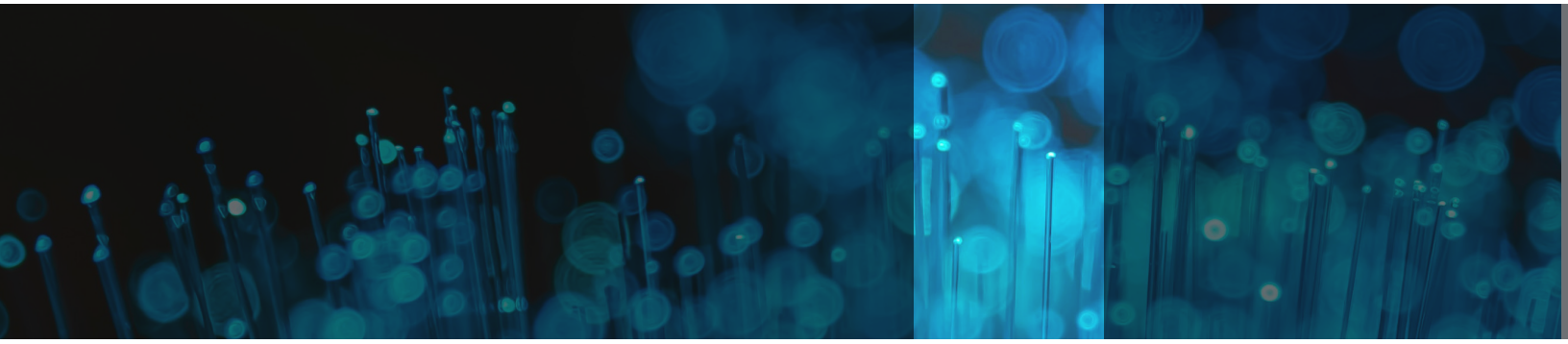
Thompson said, "I think that is huge, being able to do microcode updates that add security without having to change the hardware. That is where security starts."

Edwards said, "That is one of the great things we are seeing from companies like Intel, is that they are adding a lot more value into their products from a security perspective, whether that is authenticated boot capability, inline memory encryption.... Those types of things don't solve all the problems, but they certainly provide a nice baseline to build upon. That is important."

> "Insecurity or vulnerability is the invalidation of an assumption. When you are designing a system, you have all these explicit and implicit assumptions you make, and the hacker's job is to invalidate one of your assumptions. That is how they get in."
>
> **— Irby Thompson,**
> Wind River

THINKING THROUGH ASSUMPTIONS ABOUT SECURITY

"Insecurity or vulnerability is the invalidation of an assumption," Thompson said. "When you are designing a system, you have all these explicit



and implicit assumptions you make, and the hacker's or attacker's job is to invalidate one of your assumptions. That is how they get in. To get people to think through all their assumptions and put them down on paper, and think through the implications if they get invalidated, is hugely valuable. And it really is just a mental exercise that you have to get people in the mindset of doing."

IS AIR GAPPING EFFECTIVE AGAINST CYBERATTACKS?

"Yes," said Edwards, "an air gap is an effective means. You are not connected to the network, so you have eliminated one attack vector. But that doesn't mean that attacks still can't happen. You have got the insider threat. You've got the fact that whatever code you are bringing into that closed system from the outside, whether it is a commercial operating system like Linux or … Ethernet drivers or whatever — there is potential for malware in any of that code you're bringing in. There are things you can do; there are scanning tools out there. They won't catch all bugs or all malware, but they will catch the common ones. They will catch common vulnerabilities. Those are some of the tools you can use, [along with] good coding practices from your engineers to prevent them from introducing their own vulnerabilities. Make sure when it gets out to the field you are not introducing a whole new set of vulnerabilities."

"Obviously there is benefit to an air gap," Areno continued. "Everything is a mitigation. Everything is a step to make it harder for the attacker. [But] back to what keeps me up at night: the things I don't hear about. I have that concern with air gap — just because there is no network connection, what are the other acts that can exist there that you don't hear very much about? With all the near-field communication, the Bluetooth, the other communication mechanisms that exist, you are always worried that something else is going to hit there. With these devices, it turns into the introduction of the malware. How many components do you have in a computing system; how many pieces of firmware exist in one single system? All it takes is one."

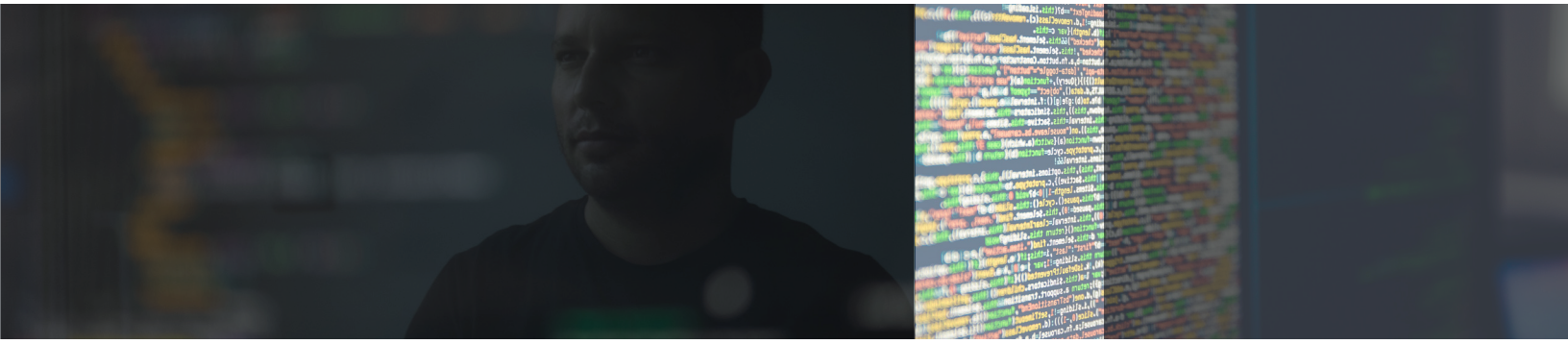
> "We are seeing attackers going lower and lower in the execution stack. It is not going to surprise me if a year or two down the road we hear about a specific component inside a computing system with malicious firmware that is doing these types of attacks."
>
> **— Matt Areno**
> Intel Corporation

Thompson observed, "I think that air gapping your network probably makes it an order of magnitude harder for an attacker. It is an improvement, [but] it is not bullet-proof. I think Intel has technologies — SGX, for example, that basically removes a lot of the trusted computing base. That probably makes it half an order of magnitude harder for an attacker to attack specific code and data. But it is not impossible. It is trending in the right direction, and I think that it is how many of these technologies are getting deployed and used in the field. Security isn't convenient, and when push comes to shove, convenience seems to win out over security a lot of the time. And that is where we really need to maintain the standard of security. We have the technologies; we are just not using them properly."

WHAT ARE THE EMERGING ANTI-TAMPERING APPROACHES FOR RTOS IMPLEMENTATIONS?

"Wind River is obviously well known for its VxWorks® RTOS," Thompson said. "The good news is that malware is generally OS-specific — not always, but generally speaking, if malware is targeting another operating system, it is not going to work. Window malware is not going to work on RTOS. An RTOS also has a smaller attack surface than a full-blown, rich desktop OS. There is some benefit there. [But] an RTOS is not immune to attacks. A software library that our RTOS uses may have a vulnerability. And in some cases it is harder to upgrade systems that have an RTOS. But at Wind River we are working hard to make sure that all the products we deploy are as secure as they can be. We also have premium security add-on options, like Titanium Security Suite, if you have specific requirement sets for anti-tamper or cybersecurity that you need to meet for your program."

> "Who are trusted partners, both on the hardware and the software sides? Which companies get it from a security point of view and are going to bring risk down instead of adding more risk to the table?"
>
> **— Irby Thompson,**
> Wind River

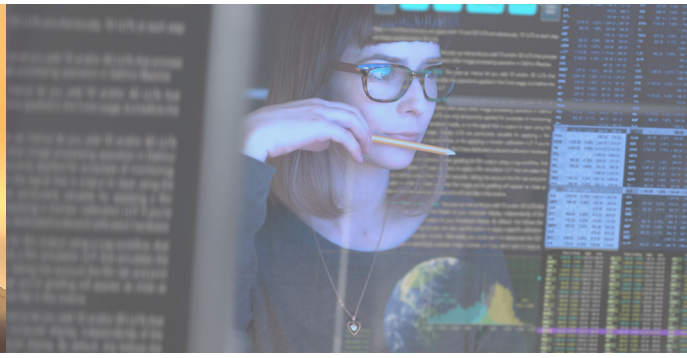


Edwards said, "The RTOS vendors do publish periodic vulnerabilities. They will let you know when something is a problem. For example, if VxWorks v7.1 or some other app has got a vulnerability, it gets published. Keep track of those and monitor them regularly. Understand that if they are going to impact your system, [you need to] look for a patch or the update to the next version that fixes that issue. The other thing about trusted suppliers is [that] most companies in our industry, in the defense industry, are being held to supply chain issues. Companies want to know what our supply chain processes are and if they are adequate. How do we buy hardware and software? Those are things you can check on to make sure that companies have processes in place — best practices — to be sure they are protecting their sourcing of materials. Then go with those who seem to have [the] better handle on it."

"Most companies in the defense industry are being held to supply chain issues. Companies want to know what our supply chain processes are and if they are adequate. Those are things you can check on."

— Steve Edwards,
Curtiss-Wright

Cybersecurity Enhancements with Container-Ready Wind River Solutions



As a complement to the discussion around updates and patches as important ingredients in maintaining cybersecurity, particularly on systems out in the field, many Wind River solutions have adopted container technology. VxWorks, the industry standard for a secure, embedded real-time operating system (RTOS), recently gained support for containers; and Wind River Linux has offered container support for several years.

Wind River Linux, Wind River Simics®, Wind River Studio, and the VxWorks real-time OS have been used in industrial environments across a broad range of sectors, including automotive, energy, aerospace, medical, and manufacturing. These components frequently save time in meeting certification requirements, when used in combination as part of platform solutions or infrastructure elements. Instead of having to separately achieve testing and certification for each operating system, virtualization application, processor, or storage system, system architects and developers can build packaged solutions that streamline and simplify the overall certification process by using components that have certifications. Support for container technology makes it easier to keep systems up-to-date for security and efficiency.

To learn more, visit Wind River at www.windriver.com.

Wind River is a global leader of software for the intelligent edge. Its technology has been powering the safest, most secure devices since 1981 and is in billions of products. Wind River is accelerating the intelligent transformation of mission-critical edge systems that demand the highest levels of security, safety, and reliability.