WIND™

EE Times

CYBERSECURITY ESSENTIALS FOR THE INTELLIGENT EDGE

Executive Briefing

Introduction

According to the IDC, there will be an estimated 42 billion connected devices by 2025. Each of these devices represents a point of entry that can be exploited by a cyberattack. For devices and systems with safety-critical functionality, a security breach can have catastrophic consequences.

In this interactive executive briefing, Wind River will walk you through the tech must-haves to successfully protect your systems and devices through their life cycle. Follow fast-paced mini web seminar series and a white paper covering how and where security needs to be baked into the life of your product.

> "You can have a secure system that is not safety critical, but you cannot have a safety-critical system that isn't secure."
>
> ***Matt Jones,*** *Chief Architect, Wind River*

Microweb Tech Series Insights:

- **Why your security strategy should start well before the first line of code is ever written**
- **Why making your embedded systems secure requires a full lifecycle approach**
- **Why you must anticipate that a security breach will happen**

All episodes are available on demand. You can access them VIA TechOnline:

WATCH ALL NOW

The Cybersecurity Journey Through the Full Product Lifecycle

Architecting a secure device starts well before the first line of code is written and ends only when the device is taken out of service.

WATCH NOW

Capturing Use Case Security Requirements

Planning for security requirements up front greatly reduces friction and cost throughout development and deployment. Learn how they will influence the direction your project takes, and what you will need to prove you've met them.

WATCH NOW

Building a Security Policy

Building your security policy starts with determining the device's assets, identifying threats to those assets, and defining mitigations to those threats. Your policy has to factor in your risk tolerance as you determine which mitigations to implement.

WATCH NOW

Designing with a Trusted Foundation

Your device is only as secure as its weakest link, so you must build on top of a proven and trusted platform with hardware-based security features as well as trustworthy software vendors, code pedigree, and secure software development practices. Architecting a secure device starts well before the first line of code is written and ends only when the device is taken out of service.

WATCH NOW

Hardening and Fortifying

You must anticipate that a breach will happen. Learn to model different threat scenarios and put in place mechanisms to protect your applications, data, IP, and the resiliency of the device. Your threat model should assume that an attacker will get root (admin) access.

WATCH NOW

Ongoing Threat Prevention

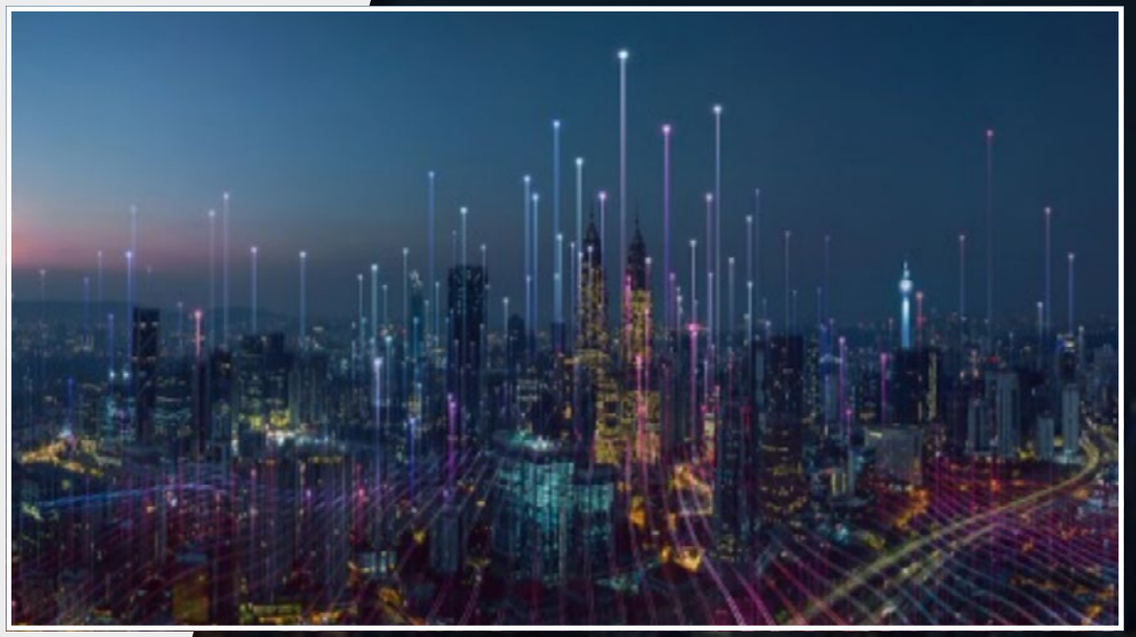
Securing your device or system is a complete lifecycle effort. Threats must be actively monitored and resolutions must be implemented. Learn why proactive endpoint integrity monitoring is a must in today's interconnected world.

WATCH NOW

Putting It All Together

Baking security into your system is not easy, but it must be done. Learn where to go to get the help you need to build a secure and safe device.

WATCH NOW



White Paper: Secure Everything, Anywhere, Anytime

Embedded Security Must Be Designed in and Continue Through the Lifespan of the Device

By the year 2025, it estimated that there will be more than 42 billion* connected devices. This growth in connected devices will come primarily from the proliferation of the Internet of Things (IoT). As IoT and the embedded industry grows, so does the attack surface for potential security threats. Every connected device, from the simplest home monitor to the most sophisticated systems of systems represents a new point of entry which can be exploited by a cyber-attack. With billions of devices already connected and tens of billions more coming, securing IoT devices and protecting the data they generate becomes an even greater imperative.

The Cost of a Cybersecurity Breah is High

It is estimated that cybercrime damage will hit $6 trillion annually by 2021.3 But in many sectors of IoT and embedded, including commercial markets like medical, industrial, infrastructure, and military, devices perform functions considered mission-critical. This means they cannot fail or execute in unintended ways. In these mission critical devices, the cost of a cybersecurity breach goes well beyond the loss of data, IP theft and damage to a company's brand. A security breach these devices can result in a catastrophic event or even loss of life. With so much at stake, cybersecurity has evolved into a public security concern.

> "A fielded embedded system is an extension of the enterprise network. A poorly secured embedded system can be an easy path for an attacker to get into your enterprise network and create significant damage."
>
> ***Arlen Baker,*** *Wind River Security Architect*

Security is a Constant

Stopping or preventing a cyber-attack has become a never ending effort. Over the last five years, security breaches have increased 67%*. And breaches are likely to keep increasing as hackers start to use new weapons like artificial intelligence (AI). AI-based attacks find vulnerabilities and can deceive preventative security safe-guards. There will always be a bad actor on a mission to see how far they can go and what they can get. For most hackers, data is the prize. The average cost of a stolen record is $150* . But some hackers have more of a malicious intent. Their goal is to have total system takeover. For this reason alone, establishing a good security strategy that transcends across the enterprise into individual devices now becomes table stakes rather than nice to have. And, project teams must be more diligent about designing

security in at the beginning of a project and the threat landscape effectively throughout the lifespan of the device. Stopping or preventing a cyber-attack has become a never ending effort. Over the last five years, security breaches have increased 67%*. And breaches are likely to keep increasing as hackers start to use new weapons like artificial intelligence (AI). AI-based attacks find vulnerabilities and can deceive preventative security safe-guards. There will always be a bad actor on a mission to see how far they can go and what they can get. For most hackers, data is the prize. The average cost of a stolen record is $150* . But some hackers have more of a malicious intent. Their goal is to have total system takeover. For this reason alone, establishing a good security strategy that transcends across the enterprise into individual devices now becomes table stakes rather than nice to have. And, project teams must be more diligent about designing security in at the beginning of a project and the threat landscape effectively throughout the lifespan of the device.

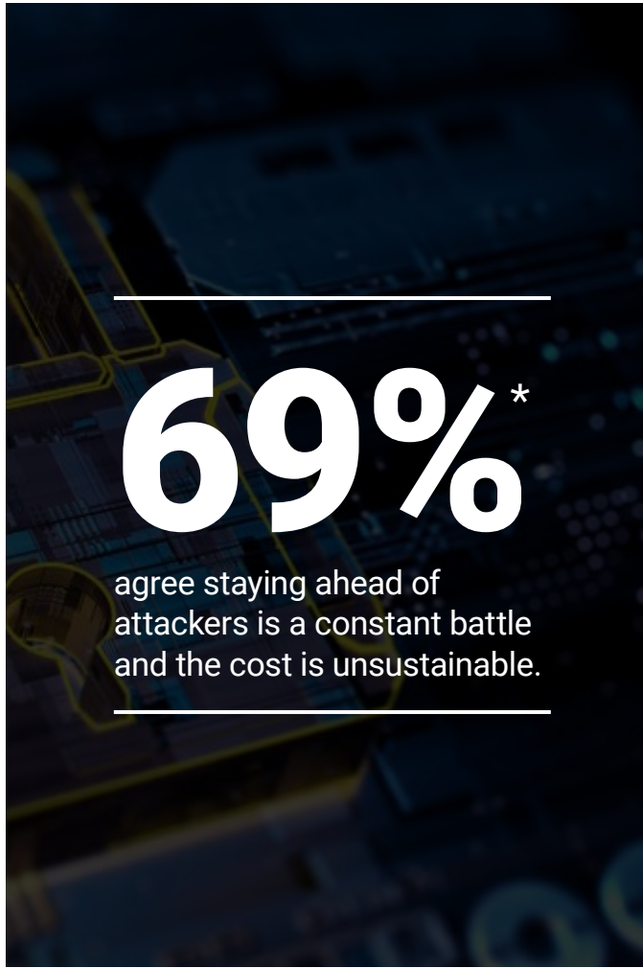
Growing Complexity and Expanding Requirements

As the breadth and complexity of IoT devices grows exponentially, so do the requirements needed to prevent cyber-attacks. In IoT markets with critical functionality characteristics, cybersecurity requirements come from many sources. There are industry standard security requirements from the National Institute of Standards and Technology (NIST) 800-53, the Federal Information Processing Standard (FIPS 140-2) and Common Criteria certifications. There are also industry-specific requirements from the International Electrotechnical Commission (IEC) 62443 for industrial markets, and the Society of Automotive Engineers (SAE) J3061 for automotive markets. There is also unique requirements for security being defined by individual projects, IT departments, Risk Management Teams, supply chain customers, and other government agencies.

Establishing a Device Security Policy is the First Step

Now more than ever, it is critical to have a security policy in place for the every device project. Without one, development teams often must create Band-Aid solutions and have to scrap and rework products as security breaches occur. Many of the standard security requirements mentioned above are geared more for the enterprise level than device level.As a result, an analysis is required to determine how the intent of the requirement applies to the device. These requirements are then input into the security assessment process to define the security policy of the device. This policy defines the assets (in this case the device), the threats to the assets, and the security implementations needed to protect the assets from the threats.

IoT and traditional embedded products are designed for just about every market segment: aerospace, automotive, defense, industrial, medical, networking, and smart cities. For all markets there is an industry standard model that guides the development of a security policy. This model is called



confidentiality, integrity, and availability (CIA) triad. The CIA Triad defines the necessary principles needed to protect a device from unauthorized access, use, disclosure, disruption, modification, or destruction. The CIA Triad is based on the following three principles:

Confidentiality: Confidentiality implementations are used to protect the privacy of data in embedded systems. This includes data in motion, data at rest or stored on the device, data being processed by the device, and data passing to and from the device.

Integrity: Integrity implementations ensure that the embedded device data has not been modified or deleted by an attacker. This includes data being generated or consumed by the embedded device as well as its programming data (the operating system, applications, configurations data, etc.).

Availability: Availability implementations are used to ensure that an embedded device performs its intended function. This means an attacker cannot change a device's intended functional purpose. This is of paramount importance to devices that perform life- or mission-critical tasks.

Project teams determine which components of the CIA Triad are required based on the risk exposure, regulatory requirements, and IP protection needs and is balanced against cost, performance, and the device deployment operational environment. There is no single silver-bullet solution for protecting a device or system from all possible attacks. Rather, a layering approach that uses different mitigation controls delivers a multifaceted protection shield and, ultimately, a much stronger cybersecurity implementation.

Security Designed-In

The concept of layering in the different security controls of confidentiality, integrity, and availability comes from the National Security Agency and is known as defense in depth.4 Although there are many variables that determine which security components a product must have, there is one commonly agreed-upon approach: Security must be looked at from end-to-end and mechanisms to adapt to the changing threat landscape must be designed-in. A device must be built on a trusted foundation that allows the flexibility to add new protection throughout the lifecycle of deployment.

Development, Security, and Operations (DevSecOps)

One approach gaining traction is DevSecOps, which allows a software development team to introduce security features earlier (think: shift left) in the development lifecycle. It also embeds security in all parts of the development process, thus helping to minimize vulnerabilities. This approach must keep security front and center from the start of a project and throughout the development lifecycle.

Simulation and Automation

To handle the complexity and quantity of cyber-attacks, development teams need to enable simulation and automation capabilities. For complex IoT systems, many developers do not have access to the physical hardware they are designing for. It is not uncommon for different parts of a system to be built using engineering teams geographically dispersed. Imagine trying

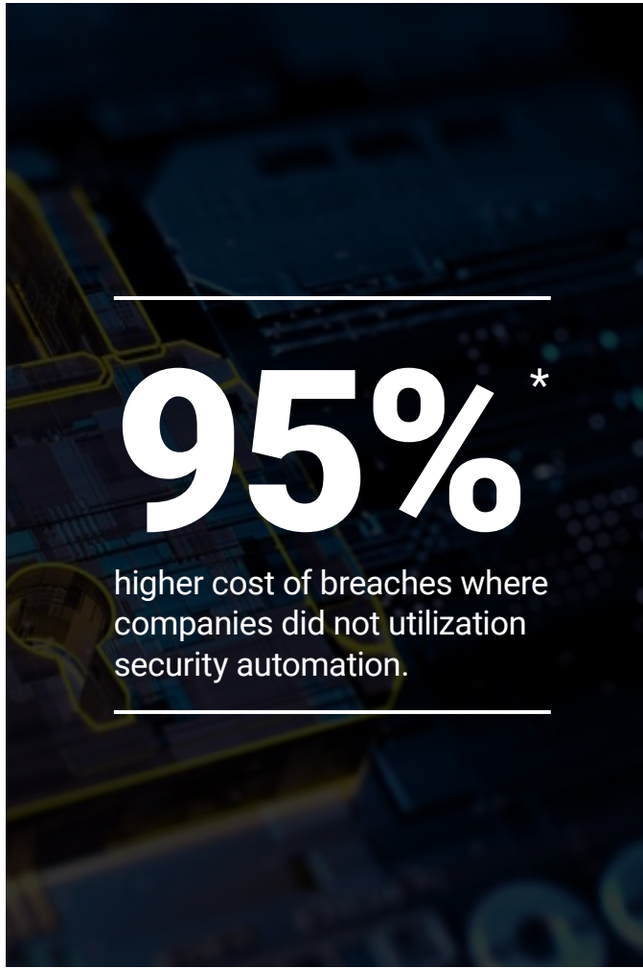
to test security vulnerabilities of a multimillion-faceted space station with components being built by several different engineering teams. It is virtually impossible. One approach is to simulate entire systems of devices, the infrastructure they run in, and the applications that run on top of. System simulation is an efficient and effective means of researching, analyzing, and testing a wide variety of attack methods and security countermeasures. System simulation allows developers to inject faults and vulnerabilities in their designs to see what would happen before the actual product deploys.

Simulation tools also enable development teams to automatically run hundreds of thousand of test scenarios to determine what could happen if there was an intrusion. This is a critical advantage for devices and systems that absolutely cannot fail.

Ongoing Monitoring and Mitigation

Cybersecurity is an ongoing effort for the life of the product. Once a product is deployed in the field threats must be constantly monitored and mitigated during deployment. In 2019, there were more than 12,000+* security vulnerabilities identified. Of these, more than one third were considered high-risk vulnerabilities. And, 60% of 2019 breaches involved vulnerabilities for which a patch was available but not applied.6 How a company monitors and mitigates cybersecurity threats should be defined in the security policy before a project is started.

60% of 2019 breaches involved vulnerabilities for which a patch was available but not applied.[6]



Why Wind River

Wind River® is the global leader in providing secure, safe, and highly reliable embedded software solutions consisting of platforms, services, support, and experience. Our customers can leverage state-of-the-art, robust, and reliable software platforms that protect privacy, maintain data integrity, and ensures availability with seamless system integration and developer collaboration. Our platforms serve as a trusted foundation so you can innovate securely and protect your device against current and future threats.

Wind River is dedicated to finding the right security solution tailored to industry-specific needs. We have successfully worked with customers across vertical markets in ensuring that they meet their security requirements.

Our proven secure-by-default platforms and deep industry experience allow you to build your device with confidence on industry-leading technology, knowing private data is protected, critical systems are isolated, and system management is securely built into the ecosystem. This allows you to reduce risk, speed up iterations, and deploy with confidence throughout the product lifecycle.

Platforms

The industry-leading VxWorks®, Wind River Linux, and Wind River Helix™ Virtualization Platform runtime platforms provide a trusted foundation from which to build embedded devices of all kinds. These proven platforms include

a rich set of security capabilities for implementing components of the CIA Triad and secure processes based on industry standards.

VxWorks, compared to other operating systems, has the fewest known CVEs in its kernel. In addition, the VxWorks engineering team proactively monitors all CVEs from third-party open source components to minimize the attack surface.

Wind River Linux includes more than 250 security packages in its distribution. These packages are tested and validated by our team of engineers. In addition, the Wind River

Linux engineering team proactively monitors all CVEs from third-party open source components to minimize the attack surface.

Wind River Helix Virtualization Platform leverages the security capabilities of both VxWorks and Wind River Linux.

Operating System Hardening and Anti-Tampering

Wind River offers robust Linux system-hardening and security capabilities to help devices remain secure during runtime and at rest. These added security capabilities maintain the integrity and confidentiality of critical data and configurations while assuring continued operations.

Platform Customization

Our team of engineers can help customers customize platforms to achieve specific market requirements. In addition to our trusted platforms, Wind River provides cybersecurity solutions that can be customized for customers specific security needs.

System Simulation

Wind River Simics provides automation, fault injection, and time manipulation to test to quality and security vulnerabilities. Developers can create a simulated controlled environment to inject faults to determine what will happen with a device, the network it is connected to, and the application that runs on it if there is a security breach. These tests can be conducted before and even after deployment to ensure ongoing security. This automated process streamlines and speeds the development process.

Long Term Support and Maintenance

Wind River customers are not alone in their efforts to secure their devices. Wind River offers a wide range of support options, including standard lifecycle, Long Term Support, custom platform maintenance, and security vulnerability services. Our team of cybersecurity engineers monitors CVEs and triages to determine impacts and how to remedy them. Wind River also provides security notices for our customers, and we maintain a public database of all CVEs and our actions to implement patches. In addition, we have a dedicated global product security incident response team (PSIRT) managing the receipt, investigation, internal coordination, and public reporting of security vulnerability information related to Wind River products and technologies.

Security Experts

The Wind River Professional Services team has more than 35 years of providing security solutions to the embedded industry, spanning all vertical market segments. Our experts have a deep understanding of the threat landscape for just about every use case. They can provide a security assessment to help design teams architect a project's security policy and steps for implementation. In addition, Wind River experts are a strong resource to support any engineering team navigating the dynamic security requirements of a design. Our team of embedded software experts holds the highest level of security clearance and can support top secret conversations with U.S. Department of Defense customers. Wind River Professional Services can take a customer platform and application through Federal Information Processing Standards (FIPS) and common criteria evaluations that are required for products being sold to the U.S. and Canadian governments. In addition, many customers use the Wind River Professional Services team and its deep industry experience to provide CVE backports to help extend the longevity of a deployed device.

Stay Current, Stay Educated

One of the most important ways design teams can build more secure products is to stay current on the latest industry developments in cybersecurity. Wind River provides a number of education and development training courses to help customers come up to speed fast and implement the latest technologies.

- **Stack Attack course:** Software attack and countermeasure
- **Anti-tamper short course:** U.S. Government course on policy, procedure, documentation, and program management with a technical understanding of attacks and countermeasures on systems
- **Embedded Security Essentials:** Software security topics in the specific context of embedded systems

Whether you are currently building embedded devices or are thinking about moving your IT application to the edge, designing for cybersecurity is one of your top requirements. It starts with building on a proven and trusted foundation that allows you to design in security and plan to address the ever-changing cyber-security threats you will face. Regardless of where you are in the design, build, and deploy process, Wind River has a security solution for you.

CONTACT WIND RIVER

Top 10 IoT security risks:

1. Weak passcodes,
2. insecure network services,
3. insecure ecosystem interfaces,
4. lack of secure update mechanism,
5. use of insecure or outdated components,
6. insufficient privacy protection,
7. insecure data transfer and storage,
8. lack of device management,
9. insecure default settings, and
10. lack of physical hardening —

creates a larger attack surface, which threat actors can leverage to take control of a device or system.

References

1. https://www.ibm.com/security/data-breach
2. Office of the Undersecretary of Defense Acquisition and Attainment, "Cybersecurity Maturity Model Certification (CMMC)," https://www.thesslstore.com blog/20-surprising-iot-statistics-you-dont-already-know/
3. Cybercrime Magazine, "Cybercrime Damages $6 Trillion By 2021," https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
4. National Security Agency, "Defense in Depth," https://apps.nsa.gov/iaarchive/library/ia-guidance/archive/defense-in-depth.cfm
5. Accenture Security, "Third Annual State of Cyber Resilience: Innovate for Cyber Resilience,"
6. Business Wire, "Cybersecurity Spending, Breaches Increased in 2019"

   Over 70% of all traffic is encrypted and it travels over an untrusted network — the public internet. So criminals and nation states can syphon that data today and then use quantum to unlock it in the future. Why does it matter it attackers can unlock today's data five or even 15 years from now? "Even in 2020, documents in the a. Top 10 IoT security risks: weak passcodes, insecure network services, insecure ecosystem interfaces, lack of secure update mechanism, use of insecure or outdated components, insufficient privacy protection, insecure data transfer and storage, lack of device management, insecure default settings, and lack of physical hardening – creates a larger attack surface, which threat actors can leverage to take control of a device or system National Archives related to the Kennedy assassination, nearly 60 years ago, still retain redactions for current national security concerns," Grobman said. https://www.sdxcentral.com/articles/news/mcafee-cto-talks-coronavirus-cybersecurity-and-quantum/2020/02/