TLP:CLEAR

Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default

Publication: April 13, 2023

Cybersecurity and Infrastructure Security Agency

NSA | FBI | ACSC | NCSC-UK | CCCS | BSI | NCSC-NL | CERT NZ | NCSC-NZ

Table of Contents

OVERVIEW: VULNERABLE BY DESIGN

Technology is integrated into nearly every facet of daily life. Internet-facing systems are connected to critical systems that directly impact our economic prosperity, livelihoods, and even health, ranging from personal identity management to medical care. As only one example, cyber breaches have resulted in hospitals cancelling surgeries and diverting patient care globally. Insecure technology and vulnerabilities in critical systems may invite malicious cyber intrusions, leading to serious potential safety[1] risks.

Now more than ever, it is crucial for technology manufacturers to make Secure-by-Design and Secure-by-Default the focal points of product design and development processes. Some vendors have made great strides driving the industry forward in software assurance, while others lag behind. The authoring agencies strongly encourage every technology manufacturer to build their products in a way that prevents customers from having to constantly perform monitoring, routine updates, and damage control on their systems to mitigate cyber intrusions. Manufacturers are encouraged to take ownership of improving the security outcomes of their customers. Historically, technology manufacturers have relied on fixing vulnerabilities found after the customers have deployed the products, requiring the customers to apply those patches at their own expense. Only by incorporating Secure-by-Design practices will we break the vicious cycle of creating and applying fixes.

To accomplish this high standard of software security, the authoring agencies encourage manufacturers to prioritize the integration of product security as a critical prerequisite to features and speed to market. Over time, engineering teams will be able to establish a new steady-state rhythm where security is truly designed-in and takes less effort to maintain. Reflecting this perspective, the European Union reinforces the importance of product security in the Cyber Resilience Act, emphasizing that manufacturers should implement security throughout a product's life-cycle in order to prevent manufacturers from introducing vulnerable products into the market.

To create a future where technology and associated products are safer for customers, the authoring agencies urge manufacturers to revamp their design and development programs to permit only Secure-by-Design and -Default products to be shipped to customers. Products that are Secure-by-Design are those where the security of the customers is a core business goal, not just a technical feature. Secure-by-Design products start with that goal before development starts. Secure-by-Default products are those that are secure to use "out of the box" with little to no configuration changes necessary and security features available without

[1] The authoring agencies recognize that the term "safety" has multiple meanings depending on the context its used. For the purposes of this guide, "safety" will refer to raising technology security standards to protect customers from malicious cyber activity.

additional cost. Together, these two principles move much of the burden of staying secure to manufacturers and reduce the chances that customers will fall victim to security incidents resulting from misconfigurations, insufficiently fast patching, or many other common issues.

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI) and the following international partners[2] provide the recommendations in this guide as a roadmap for technology manufacturers to ensure security of their products:

- Australian Cyber Security Centre (ACSC)
- Canadian Centre for Cyber Security (CCCS)
- United Kingdom's National Cyber Security Centre (NCSC-UK)
- Germany's Federal Office for Information Security (BSI)
- Netherlands' National Cyber Security Centre (NCSC-NL)
- Computer Emergency Response Team New Zealand (CERT NZ) and New Zealand's National Cyber Security Centre (NCSC-NZ).

The authoring agencies recognize the contributions by many private sector partners in advancing security-by-design and security-by-default. This product is intended to progress an international conversation about key priorities, investments, and decisions necessary to achieve a future where technology is safe, secure, and resilient by design and default. Toward that end, the authoring agencies seek feedback on this product from interested parties and intend to convene a series of listening sessions to further refine, specify, and advance our guidance to achieve our shared goals.

For more information on the importance of product safety, see CISA's article, The Cost of Unsafe Technology and What We Can Do About It.

Secure-by-Design

"Secure-by-Design" means that technology products are built in a way that reasonably protects against malicious cyber actors successfully gaining access to devices, data, and connected infrastructure. Software manufacturers should perform a risk assessment to identify and enumerate prevalent cyber threats to critical systems, and then include protections in product blueprints that account for the evolving cyber threat landscape.

Secure information technology (IT) development practices and multiple layers of defense—known as defense-in-depth—are also recommended to prevent adversary activity from compromising systems or obtaining unauthorized access to sensitive data. The authoring agencies recommend manufacturers use a tailored threat model during the product

[2] Hereafter referred to as the "authoring agencies."

development stage to address all potential threats to a system and account for each system's deployment process.

The authoring agencies urge manufacturers to take a holistic security approach for their products and platforms. Secure-by-Design development requires the investment of significant resources by software manufacturers at each layer of the product design and development process that cannot be "bolted on" later. It requires strong leadership by the manufacturer's top business executives to make security a business priority, not just a technical feature. This collaboration between business leaders and technical teams extends from the early stages of design and development, through customer deployment and maintenance. Manufacturers are encouraged make hard tradeoffs and investments, including those that will be "invisible" to the customers, such as migrating to programming languages that eliminate widespread vulnerabilities. They should prioritize features, mechanisms, and implementation of tools that protect customers rather than product features that seem appealing but enlarge the attack surface.

There is no single solution to end the persistent threat of malicious cyber actors exploiting technology vulnerabilities, and products that are "Secure-by-Design" will continue to suffer vulnerabilities; however, a large set of vulnerabilities are due to a relatively small subset of root causes. Manufacturers should develop written roadmaps to align their existing product portfolios with more Secure-by-Design practices, ensuring to only deviate in exceptional situations.

The authoring agencies acknowledge that taking ownership of the security outcomes for customers and ensuring this level of customer security may increase development costs. However, investing in "Secure-by-Design" practices while developing new technology products and maintaining existing ones can substantially improve the security posture of customers and reduce the likelihood of being compromised. Secure-by-Design principles not only strengthen the security posture for customers and brand reputation for developers but also lowers maintenance and patching costs for manufacturers in the long term.

The Recommendations for Software Manufacturers section listed below provides a list of recommended product development practices and policies for manufacturers to consider.

Secure-by-Default

"Secure-by-Default" means products are resilient against prevalent exploitation techniques out of the box without additional charge. These products protect against the most prevalent threats and vulnerabilities without end-users having to take additional steps to secure them. Secure-by-Default products are designed to make customers acutely aware that when they deviate from safe defaults, they are increasing the likelihood of compromise unless they implement additional compensating controls.

- A secure configuration should be the default baseline. Secure-by-Default products automatically enable the most important security controls needed to protect enterprises from malicious cyber actors, as well as provide the ability to use and further configure security controls at no additional cost.
- The complexity of security configuration should not be a customer problem. Organizational IT staff are frequently overloaded with security and operational responsibilities, thus resulting in limited time to understand and implement the security implications and mitigations required for a robust cybersecurity posture. Through optimizing secure product configuration—securing the "default path"—manufacturers can aid their customers by ensuring their products are manufactured, distributed, and used securely in accordance with "Secure-by-Default" standards.

Manufacturers of products that are "Secure-by-Default" do not charge extra for implementing additional security configurations. Instead, they include them in the base product like seatbelts are included in all new cars. Security is not a luxury option but is closer to the standard every customer should expect without negotiating or paying more.

RECOMMENDATIONS FOR SOFTWARE MANUFACTURERS

This joint guide provides recommendations to manufacturers for developing a written roadmap to implement and ensure IT security. The authoring agencies recommend software manufacturers implement the strategies outlined in the sections below to take ownership of the security outcomes of their customers through Secure-by-Design and -Default principles.

Software Product Security Principles

Technology manufacturers are encouraged to adopt a strategic focus that prioritizes software security. The authoring agencies developed the below three core principles to guide software manufacturers in building software security into their design processes prior to developing, configuring, and shipping their products.

1. The burden of security should not fall solely on the customer. Software manufacturers should take ownership of the security outcomes of their customer's purchase and evolve their products accordingly.
2. Embrace radical transparency and accountability. Software manufacturers should pride themselves in delivering safe and secure products, as well as differentiating themselves among the rest of the manufacturer community based on their ability to do so. This may include sharing information they learn from their customer deployments, such as the uptake of strong authentication mechanisms by default. It also includes a strong commitment to ensure vulnerability advisories and associated common vulnerability and exposure (CVE) records are complete and accurate. However, beware

of the temptation to count CVEs as a negative metric, since such numbers are also a sign of a healthy code analysis and testing community.

3. Build organizational structure and leadership to achieve these goals. While technical subject matter expertise is critical to product security, senior executives are the primary decision makers for implementing change in an organization. Executive-level commitment for software manufacturers to prioritize security as a critical element of product development requires the development of partnerships with an organization's customers to understand:
    a. The product deployment scenario guidance along with tailored threat model
    b. Proposed implementation for security controls to align to Secure-by-Default principles
    c. Resource allocation strategies tailored to company size and the ability to replace legacy development practices with Secure-by-Design practices
    d. The need to maintain an open line of communication for feedback internally and externally (e.g., employee and customer feedback) regarding product security issues. Software security should be emphasized in internal forums (e.g., all-hands or brown bags), as well as external product marketing and customer engagement
    e. Measurements of effectiveness within customer deployments. Senior executive leaders will want to know where investments in security by design and default are helping customers by slowing the pace of security patches, reducing configuration errors, and minimizing attack surface.

To enable these three principles, manufacturers should consider several operational tactics to evolve their development processes.

Convene routine meetings with company executive leadership to drive the importance of Secure-by-Design and Secure-by-Default within the organization. Policies and procedures should be established to reward production teams that develop products adhering to these principles, which could include awards for implementing outstanding software security practices or incentives for job ladders and promotion criteria.

Operate around the importance of software security to business success. For example, consider assigning a "software security leader" or a "software security team" that upholds business and IT practices to directly link software security standards and manufacturer accountability. Manufacturers should ensure they have robust, independent product security assessment and evaluation programs for their products.

Use a tailored threat model during development to prioritize the most critical and high-impact

products. Threat models consider a product's specific use-case and enables development teams to fortify products. Finally, senior leadership should hold teams accountable for delivering secure products as a key element of product excellence and quality.

Secure-by-Design Tactics

The Secure Software Development Framework (SSDF), also known as National Institute of Standards and Technology's (NIST) SP 800-218, is a core set of high-level secure software development practices that can be integrated into each stage of the software development lifecycle (SDLC). Following these practices can help software producers become more effective at finding and removing vulnerabilities in released software, mitigate the potential impact of the exploitation of vulnerabilities, and address the root causes of vulnerabilities to prevent future recurrences.

The authoring agencies encourage the use of Secure-by-Design tactics, including principles that reference SSDF practices. Software manufacturers should develop a written roadmap to adopt more Secure-by-Design software development practices across their portfolio. The following is a non-exhaustive list of illustrative roadmap best practices:

- Memory safe programming languages (SSDF PW.6.1): Prioritize the use of memory safe languages wherever possible. The authoring agencies acknowledge that other memory specific mitigations, such as address space layout randomization (ASLR), control-flow integrity (CFI), and fuzzing are helpful for legacy codebases, but insufficient to be viewed as secure-by-design as they do not adequately prevent exploitation. Some examples of modern memory safe languages include C#, Rust, Ruby, Java, Go, and Swift. Read NSA's memory safety information sheet for more.
- Secure Hardware Foundation: Incorporate architectural features that enable fine-grained memory protection, such as those described by Capability Hardware Enhanced RISC Instructions (CHERI) that can extend conventional hardware Instruction-Set Architectures (ISAs). For more information visit, University of Cambridge's CHERI webpage.
- Secure Software Components (SSDF PW 4.1): Acquire and maintain well-secured software components (e.g., software libraries, modules, middleware, frameworks,) from verified commercial, open source, and other third-party developers to ensure robust security in consumer software products.
- Web template frameworks (SSDF PW.5.1): Use web template frameworks that implement automatic escaping of user input to avoid web attacks such as cross-site scripting.
- Parameterized queries (SSDF PW 5.1): Use parameterized queries rather than including user input in queries, to avoid SQL injection attacks.
- Static and dynamic application security testing (SAST/DAST) (SSDF PW.7.2, PW.8.2):

Use these tools to analyze product source code and application behavior to detect error-prone practices. These tools cover issues ranging from improper management of memory to error prone database query construction (e.g., unescaped user input leading to SQL injection). SAST and DAST tools can be incorporated into development processes and run automatically as part of software development. SAST and DAST should complement other types of testing, such as unit testing and integration testing, to ensure products comply with expected security requirements. When issues are identified, manufacturers should perform root-cause analysis to systemically address vulnerabilities.

- Code review (SSDF PW.7.1, PW.7.2): Strive to ensure that code submitted into products goes through peer review by other developers to ensure higher quality.
- Software Bill of Materials (SBOM) (SSDF PS.3.2, PW.4.1): Incorporate the creation of SBOM[3] to provide visibility into the set of software that goes into products.
- Vulnerability disclosure programs (SSDF RV.1.3): Establish vulnerability disclosure programs that allow security researchers to report vulnerabilities and receive legal safe harbor in doing so. As part of this, suppliers should establish processes to determine root causes of discovered vulnerabilities. Such processes should include determining whether adopting any of the Secure-by-Design practices in this document (or other similar practices) would have prevented the introduction of the vulnerability.
- CVE completeness: Ensure that published CVEs include root cause or common weakness enumeration (CWE) to enable industry-wide analysis of software security design flaws. While ensuring that every CVE is correct and complete can take extra time, it allows disparate entities to spot industry trends that benefit all manufacturers and customers. For more information on managing vulnerabilities, see CISA's Stakeholder-Specific Vulnerability Categorization (SSVC) guidance.
- Defense-in-Depth: Design infrastructure so that the compromise of a single security control does not result in compromise of the entire system. For example, ensuring that user privileges are narrowly provisioned and access control lists are employed can reduce the impact of a compromised account. Also, software sandboxing techniques can quarantine a vulnerability to limit compromise of an entire application.
- Satisfy Cyber Performance Goals (CPGs): Design products that meet basic security practices. CISA's Cybersecurity Performance Goals outline fundamental, baseline cybersecurity measures organizations should implement. Additionally, for more ways to strengthen your organization's posture, see the UK's Cyber Assessment Framework

[3] Some of the authoring agencies are exploring alternate approaches to gaining security assurances around the software supply chain.

which shares similarities to CISA's CPGs. If a manufacturer fails to meet the CPGs—such as not requiring phishing-resistant multi-factor authentication for all employees—then they cannot be seen as delivering Secure-by-Design products.

The authoring agencies recognize that these changes are significant shifts in an organization's posture. As such, their introduction should be prioritized based on criticality, complexity, and business impact. These practices can be introduced for new software and incrementally expanded to cover additional use cases and products. In some cases, the criticality and risk posture of a certain product may merit an accelerated schedule to adopt these practices. In others, practices can be introduced into a legacy codebase and remediated over time.

Secure-by-Default Tactics

In addition to adopting Secure-by-Design development practices, the authoring agencies recommend software manufacturers prioritize Secure-by-Default configurations in their products. These should strive to update products to conform to these practices as they are refreshed. For example:

- Eliminate default passwords: Products should not come with default passwords that are universally shared. To eliminate default passwords, the authoring agencies recommend products require administrators to set a strong password during installation and configuration.
    - Mandate Multifactor Authentication (MFA) for privileged users. We observe that many enterprise deployments are managed by administrators who have not protected their accounts with MFA. Given that administrators are high value targets, products should make MFA opt-out rather than opt-in. Further, the system should regularly prompt the administrator to enroll in MFA until they have successfully enabled it on their account. Netherlands' NCSC has guidance that parallels CISA's, visit their Mature Authentication Factsheet for more information.
- Single sign-on (SSO): IT applications should implement single sign on technology via modern open standards. Examples include Security Assertion Markup Language (SAML) or OpenID Connect (OIDC.) This capability should be made available by default at no additional cost.
- Secure Logging: Provide high-quality audit logs to customers at no extra charge. Audit logs are crucial for detecting and escalating potential security incidents. They are also crucial during an investigation of a suspected or confirmed security incident. Consider best practices such as providing easy integration with security information and event management (SIEM) systems with application programming interface (API) access that uses coordinated universal time (UTC), standard time zone formatting, and robust documentation techniques.

- Software Authorization Profile: Software suppliers should provide recommendations on authorized profile roles and their designated use case. Manufacturers should include a visible warning that notifies customers of an increased risk if they deviate from the recommended profile authorization. For example: Medical doctors can view all patient records, but a medical scheduler has limited access to certain information that is required for scheduling appointments.
- Forward-looking security over backwards compatibility: Too often, backwards-compatible legacy features are included, and often enabled, in products despite causing risks to product security. Prioritize security over backwards compatibility, empowering security teams to remove insecure features even if it means causing breaking changes.
- Track and reduce "hardening guide" size: Reduce the size of "hardening guides" that are included with products and strive to ensure that the size shrinks over time as new versions of the software are released. Integrate components of the "hardening guide" as the default configuration of the product. The authoring agencies recognize that shortened hardening guides result from ongoing partnership with existing customers and include efforts by many product teams, including user experience (UX).
- Consider the user experience consequences of security settings: Each new setting increases the cognitive burden on end users and should be assessed in conjunction with the business benefit it derives. Ideally, a setting should not exist; instead, the most secure setting should be integrated into the product by default. When configuration is necessary, the default option should be broadly secure against common threats.

The authoring agencies acknowledge these changes may have operational effects on how the software is employed. Thus, customer input is critical in balancing operational and security considerations. The authoring agencies believe that developing written roadmaps and executive support that prioritize these ideas into an organization's most critical products is the first step to shifting towards secure software development practices. While customer input is important, the authoring agencies have observed important cases where customers have been unwilling or unable to adopt improved standards, often network protocols. It is important for the manufacturers to create meaningful incentives for customers to stay current and not allow them to remain vulnerable indefinitely.

HARDENING VS LOOSENING GUIDES

Hardening guides may result from the lack of product security controls being embedded into a product's architecture from the start of development. Consequently, hardening guides can also be a roadmap for adversaries to pinpoint and exploit insecure features. It is common for many organizations to be unaware of hardening guides, thus they leave their device configuration settings in an insecure posture. An inverted model known as a loosening guide should replace such hardening guides and explain which changes users should make while also listing the resulting security risks.

Rather than developing hardening guides that list methods for securing products, the authoring agencies recommend software manufacturers shift to a Secure-by-Default approach by providing loosening guides. These guides explain the business risk of decisions in plain, understandable language, and can raise organizational awareness of risks to malicious cyber intrusions. Security tradeoffs should be determined by the customers' senior executives, balancing security with other business requirements.

RECOMMENDATIONS FOR CUSTOMERS

The authoring agencies recommend organizations hold their supplying technology manufacturers accountable for the security outcomes of their products. As part of this, the authoring agencies recommend that organizational executives prioritize the importance of purchasing Secure-by-Design and Secure-by-Default products. This can manifest through establishing policies requiring that IT departments assess the security of manufacturer software before it is purchased, as well as empowering IT departments to push back if necessary. IT departments should be empowered to develop purchasing criteria that emphasize the importance of Secure-by-Design and Secure-by-Default practices (both those outlined in this document and others developed by the organization). Furthermore, IT departments should be supported by executive management when enforcing these criteria in purchasing decisions. Organizational decisions to accept the risks associated with specific technology products should be formally documented, approved by a senior business executive, and regularly presented to the Board of Directors.

Key enterprise IT services that support the organization's security posture, such as the enterprise network, enterprise identity and access management, and security operations and response capabilities, should be seen as critical business functions that are funded to align with their importance to the organization's mission success. Organizations should develop a plan to upgrade these capabilities to leverage manufacturers that embrace Secure-by-Design and Secure-by-Default practices.

Where possible, organizations should strive to forge strategic partnership relationships with

their key IT suppliers. Such relationships include trust at multiple levels of the organization and provide vehicles to resolve issues and identify shared priorities. Security should be a critical element of such relationships and organizations should strive to reinforce the importance of Secure-by-Design and Secure-by-Default practices in both the formal (e.g., contracts or vendor agreements) and informal dimensions of the relationship. Organizations should expect transparency from their technology suppliers about their internal control posture as well as their roadmap towards adopting Secure-by-Design and Secure-by-Default practices.

In addition to making Secure-by-Default a priority within an organization, IT leaders should collaborate with their industry peers to understand which products and services best embody these design principles. These leaders should coordinate their requests to help manufacturers prioritize their upcoming security initiatives. By working together, customers can help provide meaningful input to manufacturers and create incentives for them to prioritize security.

When leveraging cloud systems, organizations should ensure they understand the shared responsibility model with their technology supplier. That is, organizations should have clarity on the supplier's security responsibilities rather than just the customer's responsibilities. Organizations should prioritize cloud providers that are transparent about their security posture, internal controls, and ability to live up to their obligations under the shared responsibility model.

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. CISA, and the authoring agencies do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial entities or commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoritism by CISA and the authoring agencies. This document is a joint initiative by CISA that does not automatically serve as a regulatory document.

RESOURCES

CISA

- CISA's SBOM Guidance
- CISA's Cross-Sector Cybersecurity Performance Goals
- Guidelines on Technology Interoperability
- CISA and NIST's Defending Against Software Supply Chain Attacks
- The Cost of Unsafe Technology and What We Can Do About It | CISA

- Stop Passing the Buck on Cybersecurity: Why Companies Must Build Safety Into Tech Products (foreignaffairs.com)
- CISA's Stakeholder-Specific Vulnerability Categorization (SSVC) Guidance
- CISA's Phishing Resistant MFA Fact Sheets
- Cyber Guidance for Small Businesses | CISA

NSA

- NSA's Cybersecurity Information Sheet on Memory Safety
- NSA's ESF Securing the Software Supply Chain: Best Practices for Suppliers

FBI

- Understanding and Responding to the SolarWinds Supply Chain Attack: The Federal Perspective
- The Cyber Threat - Response and Reporting
- FBI's Cyber Strategy

National Institute of Standards and Technology (NIST)

- NIST's Digital Identity Guidelines
- NIST's Cyber Security Framework
- NIST's Secure Software Development Framework (SSDF)

Australian Cyber Security Centre (ACSC)

- ACSC's IoT Code of Practice Guidance for Manufacturers

The United Kingdom's National Cyber Security Centre (UK)

- The UK's Cyber Assessment Framework
- The UK NCSC's Secure Development and Deployment guidance
- The UK NCSC's Vulnerability Management guidance
- The UK NCSC's Vulnerability Disclosure Toolkit
- University of Cambridge's CHERI
- So long and thanks for all the bits - NCSC.GOV.UK

Canadian Centre for Cyber Security (CCS)

- CCCS's Guidance on Protecting Against Software Supply Chain Attacks

- Cyber supply chain: An approach to assessing risks
- Canadian Centre for Cyber Security's CONTI ransomware guidance

Germany's Federal Office for Information Security (BSI)

- The BSI Grundschutz compendium (module CON.8)
- The international standard IEC 62443, part 4-1
- State of IT-security in Germany report, 2022
- BSI practices of web application security

Netherlands' National Cyber Security Centre

- NCSC-NL's Mature Authentication Factsheet

Other

- How Complex Systems Fail
- The New Look in complex system failure