Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software

October 16, 2023

Summary:

CISA, the National Security Agency (NSA), Department of Justice (DOJ), and 15 international partners released the guidance Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software on October 16, 2023. This guidance was published as the government places more emphasis on secure by design and secure by default technology. "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, whereas "secure by default" means products are resilient against prevalent exploitation techniques out of the box without added charge.

Software developers are encouraged to design products with security in mind throughout the production process to minimize the risk that government and critical infrastructure face and mitigate cyber intrusions. The guidance encourages software manufacturers three software product security principles:

1. **Take ownership of customer security outcomes**
2. **Embrace radical transparency and accountability**
3. **Build organizational structure and leadership to achieve these goals**

Principle 1: Take Ownership of Customer Security Outcomes

The first priority of the guidance is to take ownership of customer security outcomes. The government and other customers should not be solely responsible for security and products need to be developed with this mindset. The guidance outlines three best practices for software manufacturers including implementing **application hardening**, support **application features** related to cybersecurity, and creating secure application **default settings** until customers configure them to integrate into their systems.

Demonstrating the principle includes implementing the following best practices:

Secure by default practices

1. Eliminate default passwords
2. Conduct filed tests
3. Reduce hardening guide size
4. Actively discourage use of unsafe legacy features
5. Implement attention grabbing alerts
6. Create secure configuration templates

Secure product development practices

1. Document conformance to a secure SDLC framework
2. Document cybersecurity performance goals (CPG) or equivalent conformance
3. Vulnerability management

4. Responsibility use open-source software
5. Provide defaults for developers
6. Foster a software developer workforce that understands security
7. Test security incident event management (SIEM) and security orchestration, automation, and response (SOAR) integration
8. Align with Zero Trust Architecture (ZTA)

Pro Secure Business Practices

1. Provide logging at no additional charge
2. Eliminate hidden taxes
3. Embrace open standards
4. Provide upgrade tooling

Principle 2: Embrace Radical Transparency and Accountability

The second priority of the guidance is to embrace radical transparency and accountability. This requires vendors to share information and maintaining updated common vulnerability and exposure (CVE) records. Transparency will aid in the establishment and development of conventions for industry, especially those with fewer resources. Transparency also builds accountability into the technology.

Radical transparency will help distribute that information and benefit the defenders more than our adversaries.

Demonstrating the principle includes implementing the following best practices:

Secure by default practices

1. Publish aggregate security relevant statistics and trends
2. Publish patching statistics
3. Publish data on unused privileges

Secure product development practices

1. Establish internal security controls
2. Publish high-level threat models
3. Publish detailed secure SDLC self-attestation
4. Embrace vulnerability transparency
5. Publish Software Bill of Materials (SBOMs)
6. Publish a vulnerability disclosure policy

Pro Secure Business Practices

1. Publicly name a secure by design senior executive sponsor
2. Publish a secure by design roadmap
3. Publish a memory-safety roadmap
4. Publish results

Principle 3: Lead from the Top

The third priority of the guidance is to lead from the top. Leadership and senior executives are essential to creating change. Investment from leadership to prioritize security in the development of products is needed for secure by design to succeed.

> *"Attainment of quality leadership requires that the upper managers personally take charge of managing for quality. In companies that did attain quality leadership, the upper managers personally guided the initiative. I am not aware of any exceptions."*
>
> J.M. Juran, *Juran on Quality by Design*

Demonstrating the principle includes implementing the following best practices:

1. Include details of a secure by design program in corporate financial reports
2. Provide regular reports to your board of directors
3. Empower the secure by design executive
4. Create meaningful internal incentives
5. Create a secure by design council
6. Create and evolve customer councils

Secure by Design Tactics

Following the Secure Software Development Framework (SSDF) developed by NIST, producers can 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 guide provides a list of best practices for software developers when developing a secure by design roadmap:

- Using **memory safe programing languages** wherever possible
- Incorporate architectural features that enable fine- grained memory protection
- Acquire and maintain well-**secured software components**
- Use **web template frameworks** (SSDF PW 5.1) that implement automatic escaping of user input to avoid web attacks such as cross-site scripting.
- Use **parameterized queries** (SSDF PW 5.1) rather than including user input in queries, to avoid SQL injection attacks.
- Use **static and dynamic application security testing (SAST/DAST)** to analyze product source code and application behavior to detect error-prone practices.
- Peer **review code**
- Incorporate **SBOMs**
- Establish **vulnerability disclosure programs**
- Ensure that every **CVE** is correct and **complete**
- Implementing **defense in depth** by designing infrastructure so that the compromise of a single security control does not result in compromise of the entire system
- Design products that **satisfy CISA's Cybersecurity Performance Goals**

Secure by Default Tactics

To increase the security of products, producers should prioritize secure by default settings and update products to conform to the best practices. Ways in which producers can do this is by:

- Eliminating default passwords
- Mandate multifactor authentication for privilege users
- Implement single sign-on (SSO)
- Encourage secure logging by providing high-quality audit logs to customers at no extra charge or additional configuration
- Provide recommendations on software authorized profile roles and their designated use case
- Prioritize forward-looking security over backwards compatibility
- Track and reduce “hardening guide” size
- Consider the user experience consequences of security settings.