Designing for compliance with the EU Cyber Resilience Act

By Trevor Martin

Introduction

The EU Cyber Resilience Act (CRA) introduces mandatory cybersecurity requirements for Internet of Things (IoT) devices and other digital products sold within the EU. It aims to improve the security of connected devices, reduce vulnerabilities, and protect users from cyber risks. Here's a summary of the key requirements under the CRA:

1. Product Scope and Risk Management

- The CRA covers a wide range of digital products, including IoT devices, software, and embedded systems that connect directly or indirectly to other devices or networks.
- Manufacturers must perform risk assessments to identify potential cybersecurity threats and vulnerabilities, considering the device's intended use and operational environment.

2. Security by Design and Default

- IoT devices must prioritize security from the outset, embedding security features into the design (Security by Design).
- Devices should have secure configurations by default, so users do not need to adjust settings for security.
- Default passwords are prohibited; unique credentials or secure authentication processes are required.

3. Vulnerability Management and Updates

- Manufacturers must establish processes to detect, report, and mitigate vulnerabilities throughout the product lifecycle.
- They must provide security updates for a specified period, with clear update mechanisms that do not compromise device functionality.

4. Transparency and Documentation

- Manufacturers must document security features, update processes, and risk assessments for each product.
- They must inform consumers and regulators about the product's cybersecurity measures, potential risks, and compliance status.

5. Incident Reporting

- Significant cybersecurity incidents affecting IoT devices must be reported to the EU cybersecurity agency, ENISA, within 24 hours.
- Incident reporting enables ENISA and national authorities to monitor security risks and respond to emerging threats.

6. Compliance and Penalties

- Compliance is enforced through market surveillance, and non-compliant products may be restricted or removed from the EU market.
- Penalties for non-compliance can reach up to €15 million or 2.5% of the global annual revenue of the offending company, whichever is higher.

7. Certification and CE Marking

- The CRA introduces a CE marking requirement for cybersecurity, meaning compliant devices must display the CE mark to enter the EU market.
- Voluntary cybersecurity certifications may be developed for higher-assurance IoT products, although these are not mandatory under the CRA.

8. Responsibility Across Supply Chain Stakeholders

- Not only manufacturers but also importers and distributors, must ensure that products meet cybersecurity standards before reaching the EU market.

Designing for CRA Compliance

To meet the EU CRA for IoT devices, a security-focused design approach is essential. By incorporating advanced hardware and software capabilities, developers can create resilient IoT products that fulfil CRA requirements. Here's how to approach a compliant design using the latest Armv8-M-based MCUs with Cortex-M33/55 processors and TrustZone technology, alongside Arm Platform Security Architecture (PSA):

Implementing a Robust Security Model

- Design a layered security model that meets CRA standards, integrating security features directly into both hardware and software.
- The security model should cover device authentication, secure communication, data protection, and secure software execution.

Selecting the Right Microcontroller with Assistive Security Peripherals

- A lot of the effort required to meet the CRA can be minimised by using a microcontroller based on the latest Armv8-M-CPU such as a Cortex-M33/55 processor equipped with the TrustZone Security Peripheral. The purpose of Trust Zone is separate secure and non-secure code, enhancing isolation and reducing attack surfaces.
- Incorporate assistive security peripherals to meet CRA requirements effectively.

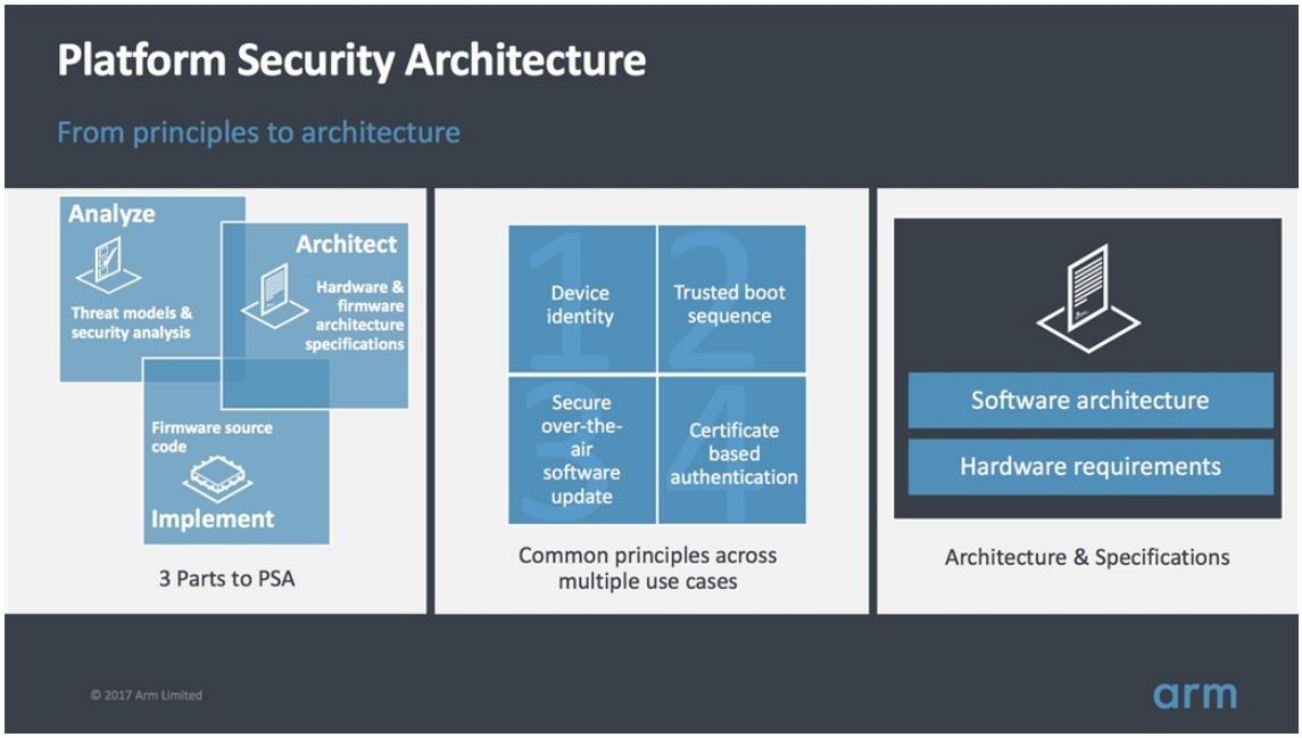
Key Assistive Security Features

- Secure Boot: Ensures only verified software can execute on the device, providing a trusted starting point for operation and thwarting unauthorized firmware modifications.
- Key Store: Safeguards cryptographic keys, enabling secure encryption, decryption, and authentication, which are essential for data integrity and confidentiality.
- Hardware Accelerators: Improves encryption and decryption performance, allowing secure communications without compromising efficiency or battery life.
- Tamper Protection: Detects and responds to physical tampering, ensuring the device remains secure against potential hardware attacks.
- True Random Number Generator (TRNG): Provides high-quality random numbers crucial for secure cryptographic operations, reinforcing protection against common cyberattacks.

- Additional Security Enclave: Isolates sensitive data and critical security operations from the main application processor, creating an extra layer of security within the hardware.

Arm Platform Security Architecture (PSA)

The Platform Security Architecture (PSA) framework offers comprehensive guidelines and resources to support secure development for ArmV8.x processors, streamlining the establishment of a robust processing environment. PSA defines a security architecture that enhances risk management, lifecycle management, and certification processes, aligning with the CRA's requirements for transparency and documentation.



Trusted Firmware for Cortex-M (TF-M)

A central component of PSA, Trusted Firmware for Cortex-M (TF-M), serves as a foundational secure processing environment for Arm-based devices. Developed to meet stringent security standards, TF-M provides a solid framework for implementing secure boot, cryptographic operations, and trusted execution environments. By isolating critical operations from the main application, TF-M protects sensitive data and processes, ensuring CRA security requirements are fully met.

Key Elements of the Trusted Firmware Secure Processing Environment

- Secure Boot and Chain of Trust: TF-M initiates a secure boot process, ensuring only authenticated and verified code is executed during system startup. This creates a chain of trust extending through all system layers, from bootloader to application code, protecting the device from unauthorized firmware modifications.
- Isolation with TrustZone Technology: TF-M uses Arm TrustZone to create distinct secure and non-secure domains within the processor, allowing sensitive data, like cryptographic keys and security-critical operations, to be handled in the secure domain. Hardware-enforced isolation reduces the attack surface and mitigates potential threats.
- Cryptographic Services: TF-M offers hardware-accelerated cryptography for secure data handling and communication, including encryption, decryption, digital signing, and secure key management via the key store. These services support secure communications, safeguarding user data, and ensuring confidentiality.
- Lifecycle Management and Secure Updates: TF-M enables secure lifecycle management, including handling security updates and patches throughout the product's life. It supports secure over-the-air (OTA) updates, allowing manufacturers to address vulnerabilities promptly and maintain CRA compliance.
- Tamper Detection and Response: Additional tamper detection mechanisms may be provided by the Microcontroller that respond to physical or logical tampering attempts, allowing the device to detect potential breaches and take preventive actions, such as data erasure or shutdown.
- Support for Secure Software Development and Certification: The Arm PSA is part of a secure development process for creating and certifying security-focused applications, including compliance with standards like PSA Certified and SESIP. The PSA framework provides resources like threat modelling, security analysis, and certification support, ensuring development aligns with best practices and meets EU regulatory standards.

In Summary

By implementing Trusted Firmware as the secure processing environment, IoT devices gain a resilient, CRA-compliant security foundation that safeguards user data, secures communications, and enables effective risk management across the product lifecycle.

If you have a new project and would like to discuss how to meet the EU Cyber Resilience Act please contact Hitex for a free consultation.

Further Information

For more information visit our website: www.hitex.co.uk or get in touch: info@hitex.co.uk. You can also connect with us: LinkedIn

View our complete knowledge base for more tips & tricks.