Brussels, 23 January 2023

AIOTI Views on the Cyber Resilience Act

Introduction

AIOTI welcomes the move to regulate for greater cyber security. Our members are committed to providing security in our products, we welcome steps to create maximum trust among users and consumers of the safety, security, and resilience of their digital products.

We want to point out that the value chain of manufacturing electronic devices is more complex than portrayed in the proposed regulation. For example, chip manufacturers often do not know the actual use of their processors. Similarly, software suppliers do not know how their product will be used. These decisions are made later in the value chain, for example, by the original equipment manufacturer (OEM). It is at the device level that decisions are made on which security features are implemented and knowledge of the criticality of end markets is known. We propose, therefore, that the minimum scope for EU Cyber Resilience Act (EU CRA) is at the device level: chips and embedded software components are removed from the proposed legislation.

The comments below are intended to explore areas where greater precision in the regulations might result in more effective regulation.

Scope

Effective legislation works best when it focusses on those issues which are critical to achieving the desired outcome. The key question should be 'what are the key practices which we must change to reach our objectives'. In this way efforts can be focussed on areas where we can make most difference without unduly burdening an unnecessarily wide range of other stakeholders.

First of all, the scope of the CRA lacks clarity and consistency with existing legislation: for example, the proposed CRA rightfully excludes Software-as-as-Service (SaaS) from its scope (Recital 9) yet how software is defined in Article 3(1) seems to nonetheless include SaaS: this creates confusion, particularly as SaaS already falls under the scope of the NIS 2 directive as "essential services". The CRA needs to focus on products only and bring greater legal clarity by refining the software category.

Additionally, we would like to probe the rationale for including, amongst others, microprocessors, microcontrollers, operating systems and hypervisors in the scope Critical Products in Annex III to the draft regulation.

There are a few problems:

I. Chip vendors and OS/Software platform vendors cannot know where and how their products are being used by a device maker. For example, the device maker may choose not to use the security features of the chip and/or the system software or use them in a way that is different from the supplier intent.

II. Device maker development and manufacturing processes rely on configuration of the chip. For example, chip security hardware features may need to be configured or activated at a suitable point of the device maker manufacturing flow. Another example is the programming of (on-chip) memory with device maker specific code and data is not known to the chip vendor.

III. Device maker software development requires the device maker to write, modify, configure, and build the device software. This is typically the case for all imported software, including open-source, and any chip-vendor supplied chip specific software.

IV. For the reasons stated in (I), (II) and (III), chip vendors who supply chip specific firmware necessarily do so without any warranty. Supplying code in this way is also a mitigation against item (V) below.

V. Traditionally legal liability rests with the device maker, who may try to pass relevant aspects of liability to other parties in the supply chain including chip vendors and OS/Software platform vendors.

In summary, the trust related questions around access control, confidentiality and integrity of stored and transmitted data, restriction on processing of personal data can only be shown to be fulfilled by the device maker.

Similarly, design related questions around secure by default, resilience to denial-of-service attacks, updates, minimisation of negative impacts, vulnerability management can only be shown to be fulfilled by the device maker.

So the problem is that the EU CRA draft Essential Security Requirements do not reflect the supply chain relationship between the silicon vendors, software providers and the device manufacturer.

There are other problems of definition linked to ‘chips’ which would cause uncertainty:

(i) By ‘chip’ do we mean hardware only or does it include firmware, drivers, or SDK?

(ii) By “OS” – do we mean only the kernel, or does it include software to enable updates, secure communication, other?

(iii) if a Chip vendor modifies open-source code for their chip and republishes it as open source is this exempt from EU CRA?

(iv) Finally, we are particularly concerned about the lack of clarity which delegated acts may bring when further specifying the definitions of the product categories covered by Annex III, as well as defining a new category of “highly critical” products (Article 6-2, 6-3 and 6-5): such a process provides no clear, risk-based criteria for businesses, nor any transparency or possibility for stakeholders’ input.

Root of Trust

We acknowledge_that chip vendors and the software providers need to provide mechanisms that are necessary for a device manufacturer to build a secured device.

We suggest that the chip vendor focus must be on hardware security features required for a Root of Trust – the anchor on which the device security ultimately relies. This will include, but is not limited to, secure on-chip storage, secure boot, control of hardware, control of hardware debug, provision of_processor features required by an operating system, and processor features that make the software harder to exploit.

The software vendor needs to focus on providing a robust software delivery that exposes the required interfaces to the device manufacturer and uses the features provided by the chip vendor.

As outlined above, the device manufacturer will need to correctly enable the features provided by the chip vendor and correctly use the functionality provided by the software vendors. That correct use must be_part of the evaluation of the security robustness of the device build by the device_manufacturer.

In our experience of working with chip makers of all sorts across the globe, they are already developing secure System on Chip (SoC) designs. They use various certification schemes for independent assessment of the security features, and they have significant expertise in vulnerability reporting.

Vulnerability/incident handling and reporting

We are concerned about the requirement to deliver a product *"without any known exploitable vulnerability"*, which we believe is not a realistic bar to set. A product's security can be influenced by numerous factors, including the product's deployment environment, the development of different technologies, and by the evolving cyber-attack landscape. These impact whether a vulnerability can actually be exploited or not. Such a requirement would discourage manufacturers from conducting meaningful security testing, potentially leading some to avoid scanning products (this way, keeping those potential vulnerabilities "unknown"), and thereby leading to less secure products being delivered on the market. There should be a more risk-based approach to remediating vulnerabilities, aligned with existing global industry standards and frameworks, to ensure entities focus on remediating the most critical vulnerabilities first.

Article 11 on reporting also brings a number of concerns: reporting "actively exploited vulnerability" might lead manufacturers to report an exploitation that could potentially impact the product before a fix/patch has been made available, which is not in line with existing Coordinated Vulnerability Disclosure (CVD) practices and standards to protect customers. Releasing public information about an unmitigated vulnerability can lead to additional cyber-attacks. Moreover, incident reporting language in this article seems inconsistent with relevant parts of the NIS 2 Directive, as it does not specify what type of incidents need to be reported and requires incidents to be reported to ENISA instead of a CSIRT. These inconsistencies can significantly impact overall product security by creating unnecessary uncertainty for the manufacturers that need to undertake such reporting processes.

Finally, the 24h timeline for this notification obligation is unrealistic and not consistent with existing privacy and security rules (such as GDPR): "without undue delay and in no less than 72 hours" is a more appropriate window for businesses to focus on fixing the incident, while gathering the necessary complete information that can help competent authorities to understand the nature of the incident and conduct an effective triage so they can prioritise reports.

Evaluation Schemes

There are some successful industry body security evaluation schemes for IoT and connected devices that could be used to help evaluate EU CRA requirements.

We suggest that industry body evaluation schemes that include the EU CRA requirements and are under the supervision of an independent Certification Body (CB) be able to assess Critical Class I products.

Existing independent security by design evaluations of devices can be simply adapted to provide evaluation capacity via third party assessment. This will help device manufacturers get their products certified under high quality schemes with acceptable time to market and cost impact.

We therefore propose that a clarification is added to the description of conformance applying to Critical Class I products "Application of a standard or third-party assessment" that specifically allows use of industry body schemes that include the EU CRA security requirements where they are managed by an independent CB.

PSA Certified is an example of an industry body scheme that uses high quality labs under an independent CB to enable efficient security certification of devices, system software and chips.

National Market surveillance

The language around market surveillance made at national level remain unclear concerning its scope and its application in practice between member, which could lead to important fragmentation that could be avoided by framing such member state right while still supporting the capacity to defend national security.

Therefore, we suggest to strengthen the language "significant concerns in relation to materialization of an adverse impact", which appear vague and general with a disproportionately wide remit and toolkit of measures.

Additionally the deletion of the last part of (e): "significant concerns" could be considered in the case of absence of relevant specified schemes, the European Commission could lean on international standards and schemes (eg. ISO) and this language should be added, even for critical products.

Finally, with such a wide scope of national security, a text specifying and underlining the principle of non-discrimination would bring crucial legal certainty for all actor on the market and address the stability and fairness of the national mechanism to remove products from the market.

Conclusions

Security will not be improved by asking chip vendors to be assessed under the_EU CRA draft. First, they don't know where their chips go. Second, the security criteria specified in the draft regulation doesn't apply in an obvious way to a chip without considering the full device software stack.

Given these issues it might be better if the regulation made clear that what is in scope are 'devices' (including its embedded Software), not including in isolation microprocessors/controllers and OS/imported software.

About AIOTI

AIOTI is the multi-stakeholder platform for stimulating IoT and Edge Computing Innovation in Europe, bringing together small and large companies, academia, policy makers and end-users and representatives of society in an end-to-end approach. We work with partners in a global context. We strive to leverage, share and promote best practices in the IoT and Edge Computing ecosystems, be a one-stop point of information on all relevant aspects of IoT Innovation to its members while proactively addressing key issues and roadblocks for economic growth, acceptance and adoption of IoT and Edge Computing Innovation in society. AIOTI's contribution goes beyond technology and addresses horizontal elements across application domains, such as matchmaking and stimulating cooperation in IoT and Edge Computing ecosystems, creating joint research roadmaps, driving convergence of standards and interoperability and defining policies.