Contributing to the CRA Standardization Process

M. August Bournique

M. August Bournique

Amsterdam Based Consultant and Attorney

- California Licensed Attorney
- Litigation and risk management
- 7 years of working with tech
- ETSI Special Rapporteur on CRA Verticals

DISCLAIMER: The presentation is general information and not legal advice about your specific situation. I am not your lawyer.

Everything in this presentation is my own opinion and not that of my clients or any official body.

What is the CRA again…

EU WIDE PRODUCT REGULATION

- Digital products placed on the EU market
- Software and hardware … not services

GOALS OF THE CRA

- Transparency around product security and breaches
- Safer software and hardware
- The transformation of software into a “regulated industry”
- EU digital sovereignty

Is the CRA a risk for me and my FOSS project?

NO ...

THE CRA DOESN'T COVER FOSS

- Traditional FOSS Projects aren't "Products placed on the market"
- Project contributors are free of liability

UNLESS...

- The FOSS is "commercial" and provided "for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge"
- The project is integrated as a component of a commercial product and provided for profit

Why should FOSS projects care about the CRA?

PRESSURES ON FOSS

- Some FOSS is commercial
- Integrators and partners will want FOSS that complies with the CRA

POTENTIAL BENEFITS TO FOSS

- CRA and standardization have FOSS input
- Stewards a new form of market actor that could benefit FOSS organizations
- Potential for funding, both for compliance and maintainers

CRA Standardization

THE PROCESS

- Request from European Commission (EC)
- Written by Standards Organizations (ESOs)
- EC Harmonization consultants and public comment
- EC approval as freely available harmonized standard

THE ADVANTAGE OF A HARMONIZED STANDARD

- Allows “Self-Assessment” using harmonized standard for almost all FOSS products
- Shifts burden of proof for liability when product follows a harmonized standard

Over thirty CRA standards are in process

3 HORIZONTAL STANDARDS

1. Principles for Cyber Resilience
2. Generic Security Requirements
3. Vulnerability Handling

30 PLUS VERTICAL STANDARDS

1. Identity Management
2. Browsers
3. AntiVirus Software
4. **VPNS (Consumer & Enterprise)**
5. **Network Management Systems**
6. **SIEM**
7. Boot Managers
8. PKI
9. **Operating Systems**
10. Internet of Things (4 Standards)
11. **Physical and Virtual Interfaces**
12. Hypervisors and Containers
13. Internet Equipment (Routers etc.)
14. Firewalls ….

Smartcards, Secure Gateways,and more….

Focus on verticals

THE VERTICAL STANDARDS ARE MORE IMPORTANT TO FOSS

- More likely to obtain harmonization
- Standards likely expand to cover additional product types
- Verticals look at individual product types not aggregate products
- Can provide clarification for components
- More space for contributions and technical expertise
- Design process is more open to public, SMEs and FOSS

Vertical standard structure

PRODUCT BASED STANDARDS

- Standards can only cover the product itself, not the process of its design or use

RISK FOCUSED STRUCTURE

- Products are defined by Core Functionality
- Risk Factors derived from low, medium, and high risk uses
- Security Requirements cover risks associated with Risk Factors
- Mitigations (tests, features, and documentation) to meet security requirements
- Sample Use Cases to help manufacturers determine which set of Factors, Requirements and Mitigations are appropriate to their product.

Example of the vertical approach

A NETWORK INTERFACES STANDARD (EN 304 625) SAMPLE

- **Risk Factor**
  [NET], The degree of public access to attached network. Rated from “NET L-0” (private) to “NET L-3” (public).
- **Security Requirement**
  MI-SSCA: Static source code analysis for memory errors
- **Mitigation**
  All software and firmware in the product shall be checked for (listed) memory errors using a source code analysis tool
- **Use Case**
  When a the product has a **[NET]** greater than “NET L-0”

How to Get Involved...

REVIEW AND COMMENT ON VERTICAL STANDARDS

- Early draft standards are available for review at ETSI Labs **https://labs.etsi.org/rep/stan4cra**
- All final draft standards will be available for comment next month on the ETSI Labs

GET MORE INVOLVED

- Talk to OSI, Linux and Eclipse Foundations (or other ESO members) about being named a delegate (technical contributor) to a specific vertical standard effort or possibly the Horizontals
- Seek a grant from Cyberstand to join ETSI or CEN-CENELEC and attend meetings **https://cyberstand.eu**

Resources

MY LINKEDIN
https://www.linkedin.com/in/august-bournique-668b66165/

MY WEBSITE
https://bourniquelaw.com/

ETSI LABS
https://labs.etsi.org/

CYBERSTAND.EU
https://cyberstand.eu/

JOINT STANDARDIZATION WEBSITE
https://www.stan4cra.eu/

BSI CRA DASHBOARD
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CRA/Dashboard_CRA.pdf?__blob=publicationFile&v=2