
P R E S E N T A T I O N

OPEN SOURCE SOFTWARE AS CRITICAL INFRASTRUCTURE

And how AI changes everything

B Y D R C H R I S T I A N F O L I N I

OSCE cyber/ICT confidence building measures, Zurich October 2nd 2026

Dr Christian Folini

- Security engineer with 20 years of experience
- Ex-Lead OWASP CRS
- Member Steering Committee Swiss National Cyber Strategy (NCS)
- Moderator Swiss National Dialogue on Digitalization of Political Rights
- Program Chair Swiss Cyber Storm Conference



Fig. 1 —Dr Christian Folini

Agenda



Leontopodium alpinum

- Characteristics of Modern Software
- OWASP CRS as an Example of Critical Open Source Software
- AI Changes Everything
- A Call to Action

Characteristics of Modern Software

What is software? How is it built? What characteristics does it have?

What are the effects of this?

What is Software and How is it Built?

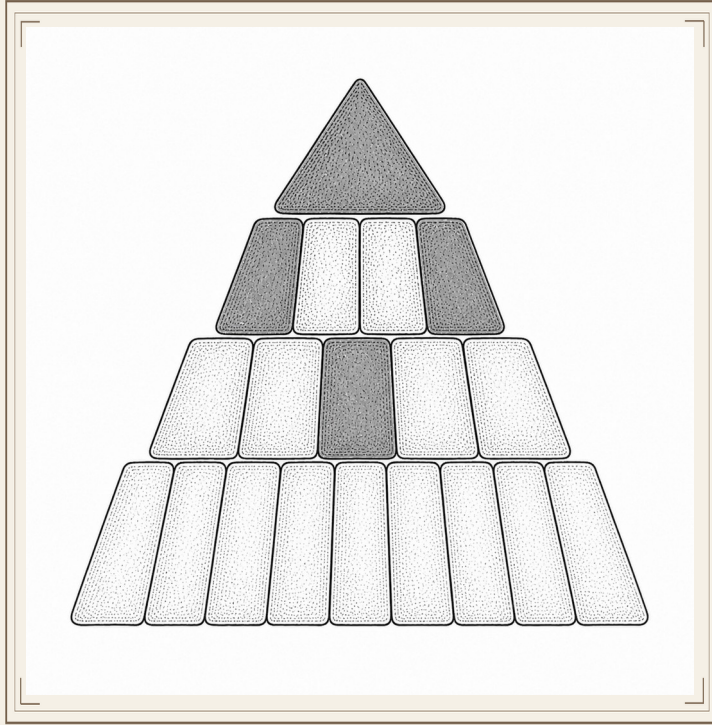


Fig. 2 — Illustration of modular software

- Software is modular: Just like modern industry
- It consists of commercial modules and non-commercial / OSS modules
- OSS allows for reuse of existing modules
- Consequently, 94% of all software contains OSS software

What are the Effects of This?

- OSS typically operates on shoestring budget
- Self-exploitation is the norm
- Calls for sponsors go unanswered
- Social contract is implied, but commercial integrators fail to fulfill their obligations

They Privatize the Profit and Socialize the Costs!

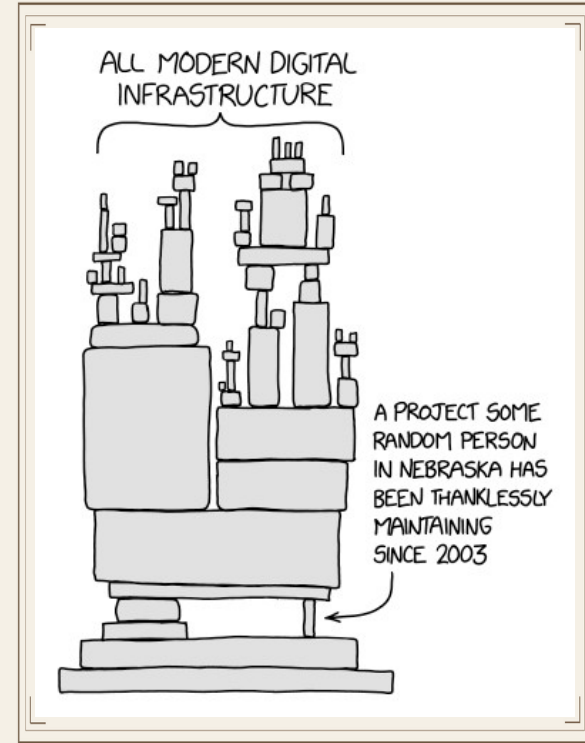


Fig. 3 — *xkcd.org* - 2347

OWASP CRS AS EXAMPLE

What is a WAF? What is OWASP CRS? How does it look like?

What is a WAF?

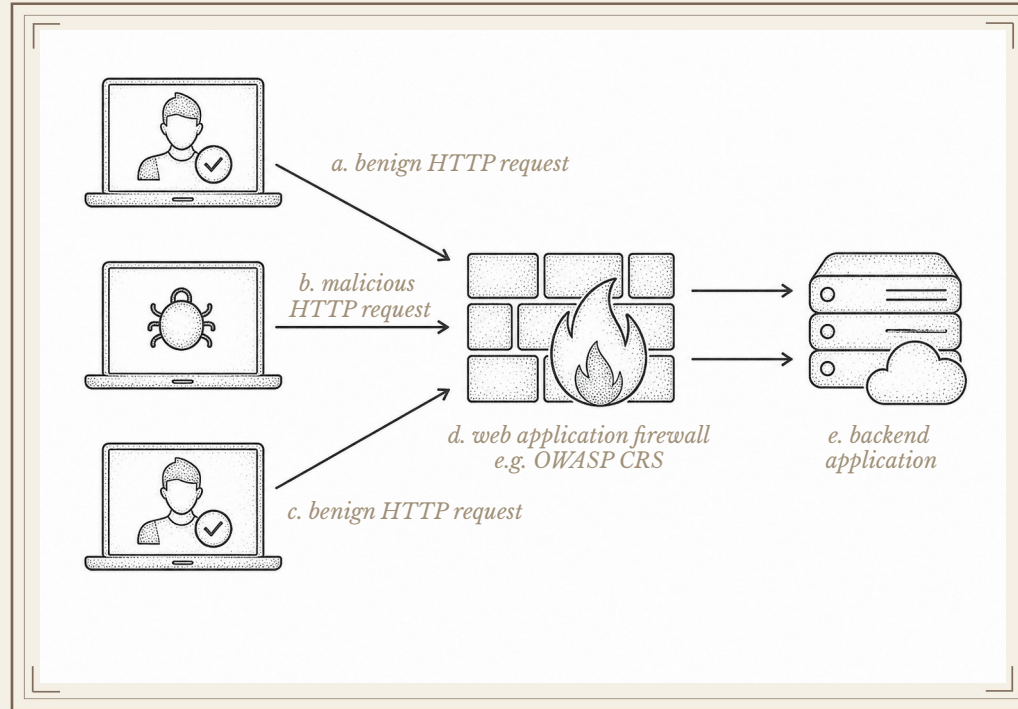


Fig. 4 — Scheme of a Web Application Firewall (WAF)

OWASP CRS as an Example

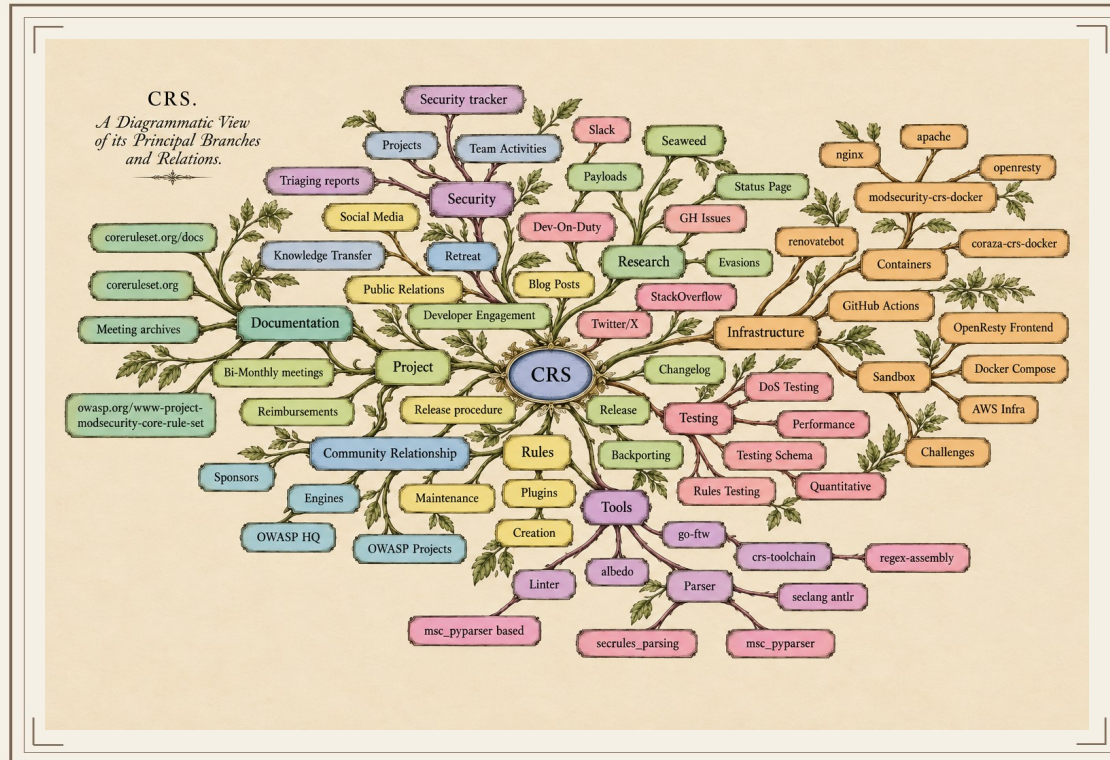


Fig. 5 — OWASP CRS – Overview of Project Activities

Who Uses and Profits from OWASP CRS

- **Google Cloud Armor** - Thank you for sponsoring!
- Microsoft Azure (*"We ran out of money!"*)
- Cloudflare (*Foulplay in public calls*)
- Akamai (*Instructed employee to cease communication*)
- Swiss AdNovum (*Never even returned calls*)
- ...



Ursus arctos

AI CHANGES EVERYTHING

The raise of AI Security Research – What this means for OSS projects?

The Rise of AI Security Research



Rhododendron ferrugineum

- 2025 brought a lot of poor AI generated bug reports – a big nuisance
- 2026 brought an avalanche of viable AI bug reports (and sometimes fixes)

What does this mean for OSS projects?

- Struggling to keep up, many quote mental load
- Developer resources are burnt
- Reviewers are becoming the bottle neck
- There is a danger that malicious actors could be allowed to join projects (e.g. posing as volunteer reviewers)
- Non-security minded projects might just give up on security completely

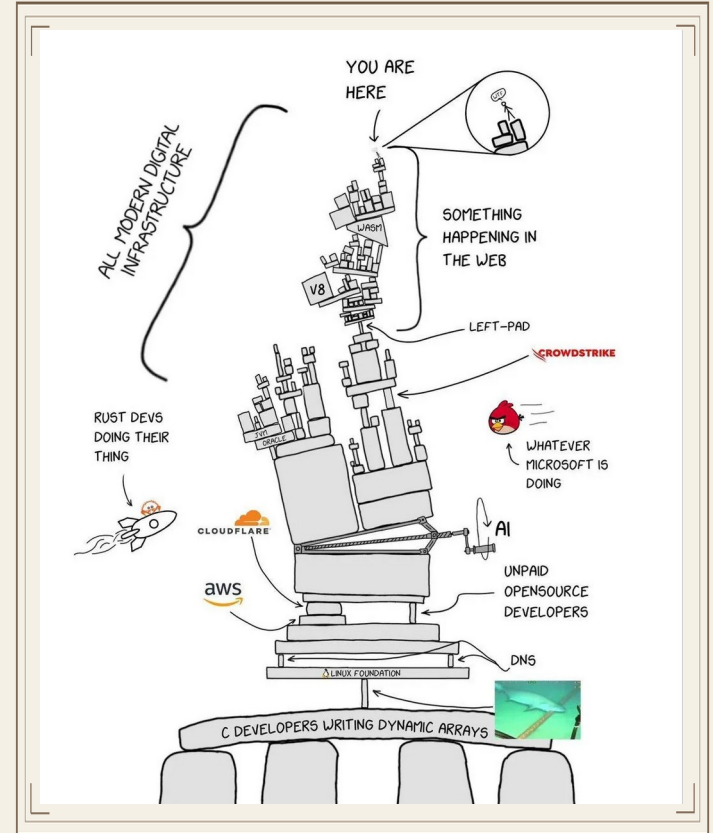


Fig. 6 — xkcd 2347 remix
reddit.com

CHAPTER IV

A CALL TO ACTION

Building on the base of the EU Cyber Resilience Act (CRA)

EU Cyber Resilience Act

Open-source software stewards shall put in place and document in a verifiable manner a cybersecurity policy to foster the development of a secure product with digital elements as well as an effective handling of vulnerabilities by the developers of that product.

– EU CRA, Article 24, Obligations of open-source software stewards

- EU CRA secures products with digital elements
- Commercial integrators of OSS are classified as OSS stewards
- OSS stewards are obliged to provide security for their products with digital elements
- They need to inform OSS projects about security issues

This should result in communication between integrators and their OSS supply chain.

Call to Action

- We need policies that help finance critical open source projects
- We need businesses to help maintain their supply chain
- We need to implement Cyber Resilience Act in a way that gives Open Source projects real leverage and real support



Arnica montana

Governments should



Dactylis glomerata

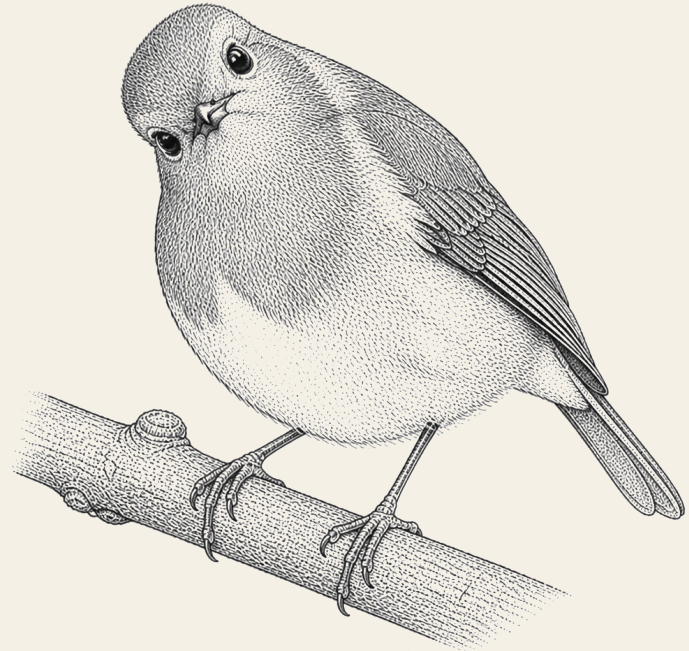
- coordinate with other governments about critical OSS
- fund open source development
- invite private sector via public / private partnerships
- create tenders demanding commitment to OSS support
- Introduce laws like Swiss EMBAG

Questions?

Dr Christian Folini

<https://christian-folini.ch>

christian.folini@netnea.com



Erithacus rubecula