

The Certification Panacea

Rigo Wenning ERCIM/W3C Legal counsel rigo.wenning@ercim.eu



Threats with daily reminder

1 société sur 2 ?

Il s'agit du nombre de sociétés victimes de cyberattaque en france en 2021

Cybersécurité en entreprise CESIN 2022

50 000€, c'est le coût médian d'une cyberattaque avec pour conséquences :





Political Pressure: The EU MUST DO something about it!







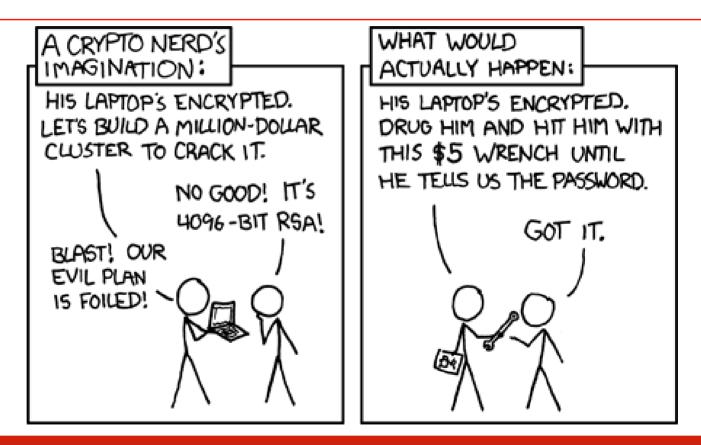
Join 2020/18 Cybersecurity Strategy

- Transport, energy and health, telecommunications, finance, security, democratic processes, space and defence are heavily reliant on network and information systems that are increasingly interconnected.
- Threat on **Critical Infrastructure**





Errors in Security



https://xkcd.com/538/



re errors Security More in Se



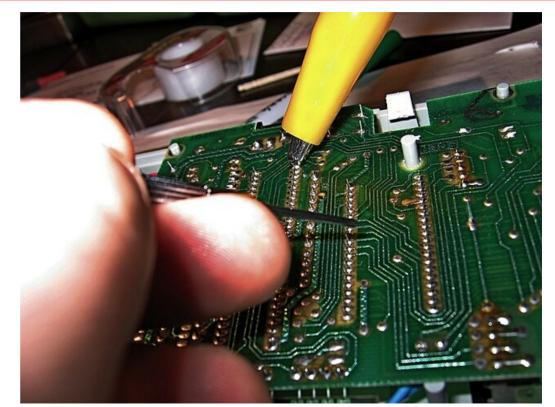
6 of 35



How we imagine we do



By elconomeno@email.com



CC bysa 2.5 Holotone at English Wikipedia



How we actually do

European Research Consortium for Informatics and Mathematics

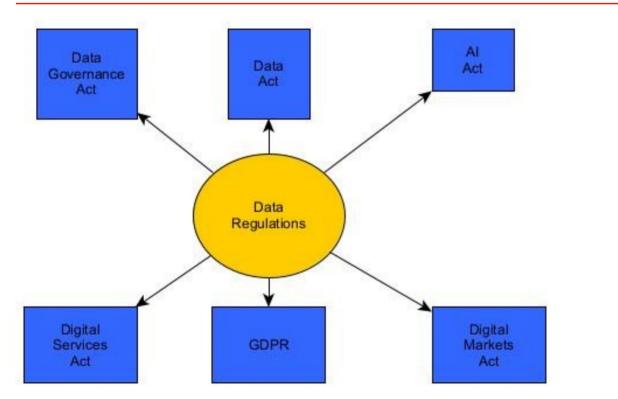


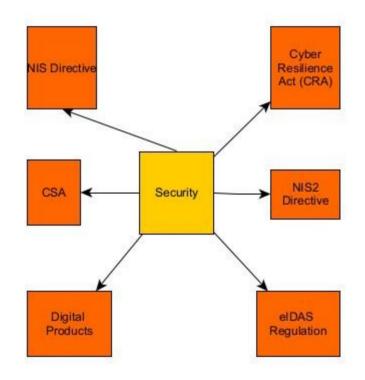


CC-BY 2.0 by Ralf Steinberger



EU covers us with Regulation







The most important:

- Cybersecurity Act (CSA) 2019/881/EU
- Proposed NIS2 Directive 2020/823/COM
- Cyber resilience Act (CRA) 2022/454/COM
- Revision of eIDAS



Wide range of national legal acts

- Telecommunications
- Energy
- Water
- National cybersecurity structures/schemes
 - (BSI, ANSSI, ACN)

- Adressing
 - Administration!!
 - Critical infrastructure
 - Now also the private sector



High variety of use cases



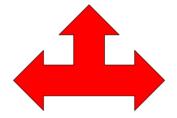
How to get from Regulation to Security?

Or how to deflect responsibility & difficulties to find consensus

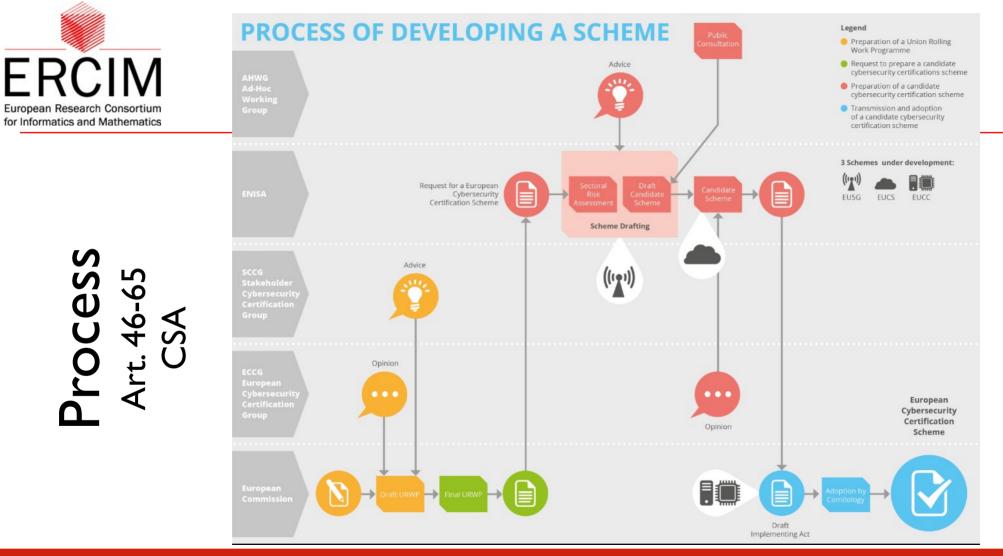


on a governmental level









SECRYPT 2023

14 of 35



Current certification schemes

- The European Cybersecurity Certification Scheme (EUCC)
- The European Certification Scheme for Cloud Services (EUCS)
- The European Cybersecurity Certification Scheme for 5G (EU5G)



European Cybersecurity Certification Scheme (EUCC)

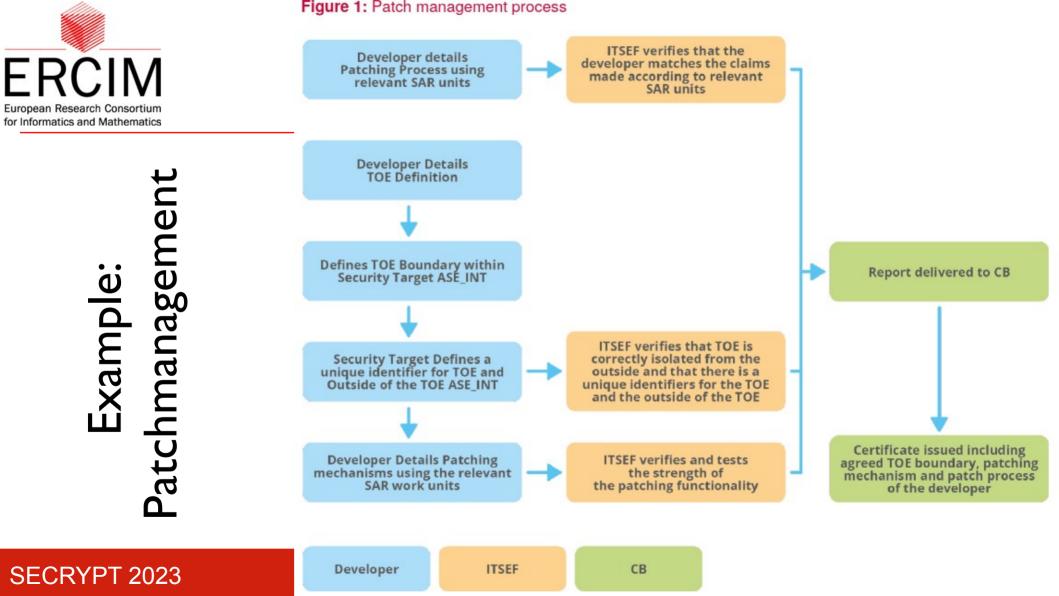
- Responsible: ENISA, Confirmation by EC via delegated ACT (not yet)
- Can develop on demand of European Cybersecurity Certification Group (ECCG)
- Must develop on demand of the EC
- Art. 50 CSA: ENISA must provide a dedicated website for certification

(https://certification.enisa.europa.eu)



EUCC

- Meta: A Schema for Certification schemes based on Common Criteria (280 pages)
- Assurance level defined in CSA (Art.52, basic, substantial, high)
- Matrix of criteria (AVA_VAN.1-5) mapping to those levels
- The EUCC Scheme shall not allow for conformity selfassessments.





Examples from EUCS

- Use standards compliant to 1025/2012/EU
 - ISO and ESOs (ETSI/CEN/CENELEC)
 - Fortunately RFC8446 (TLS)was recognized here
 - It is funny to see that the Commission Decision did not mention a version
- Format still in review
 - Machine readable?



Presumption of conformance

- Certification scheme has requirements
- Requirements can be measured
- Results can be testified and secured
- Also serves as a conformance how to
- Conformance as a major vector for market policing (see CRA)



Certification is

- Expensive (Ok, security researchers can make money)
- Burdensome
- Time consuming
- A pain

Automation is key!

The new US-EU Privacy Framework is out and requires CERTIFICATION We need data!

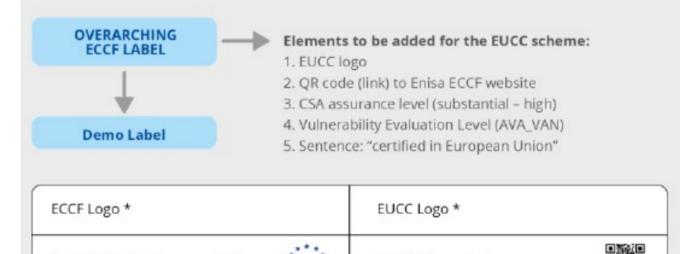
ERCIM And all I got was a bumper sticker

Certified in the European Union

CSA - Assurance Level

(substantial / high)

European Research Consortium for Informatics and Mathematics



* Logo and rules for its usage to be developed by the entity that registers the respective logo.

ECCF Enisa website

AVA_VAN

Vulnerability Evaluation Level



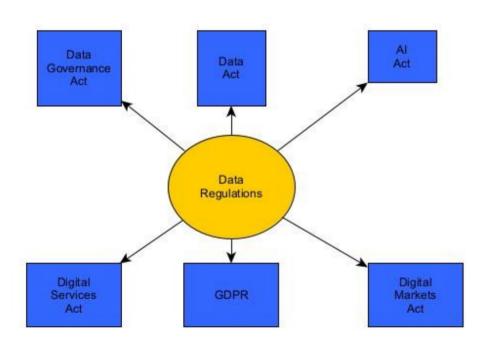
The Cost of Reading Privacy Policies Aleecia M. McDonald 2008

- Calculations: 76 days per person for reading privacy policies
- Test on 75 of the most popular websites ~ 2514 words per policy
- Reading rate: 250 words per minute
- Resulting in an average of 10 minute per policy plus 6 minute comprehension
- Average unique sites visited: 1462 sites
- McDonald calculated a cost of \$\$781 billion for the US
- This was for web, not for big data or IoT





Automation needs data

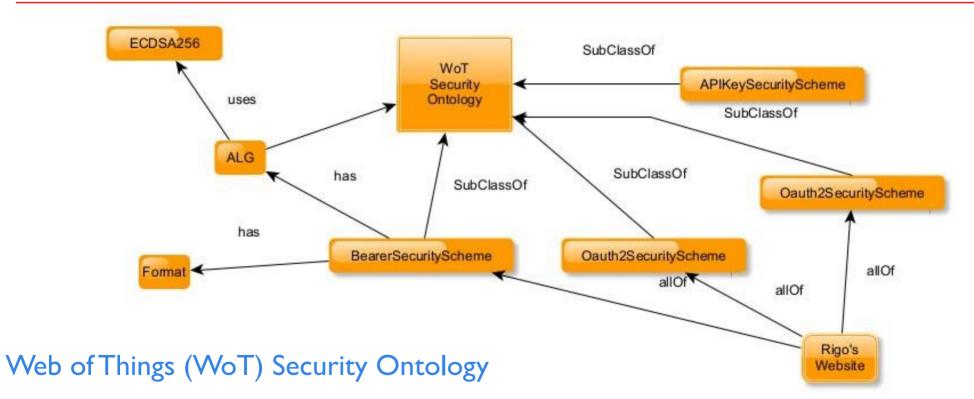


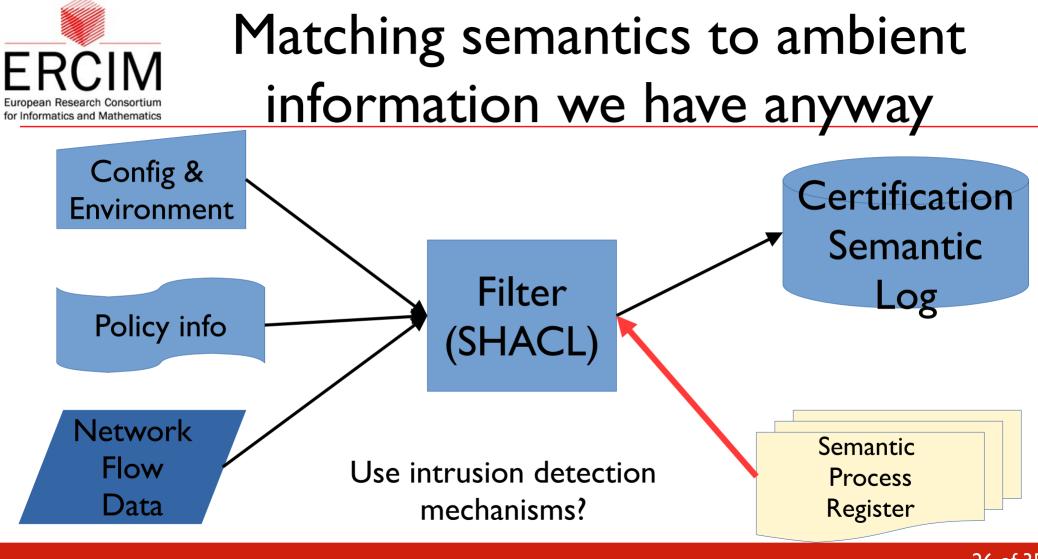
- We have data
- We need to share data
- We need to secure data
- We need agreed security semantics
- We need AI to produce the outcome

ERCIM European Research Consortium

We also need secured semantics

European Research Consortium for Informatics and Mathematics





SECRYPT 2023

26 of 35



Automation

Certification Semantic Log

Compliance Notification Stream

Administration Monster





Does a seal



(certification) Increase Security?

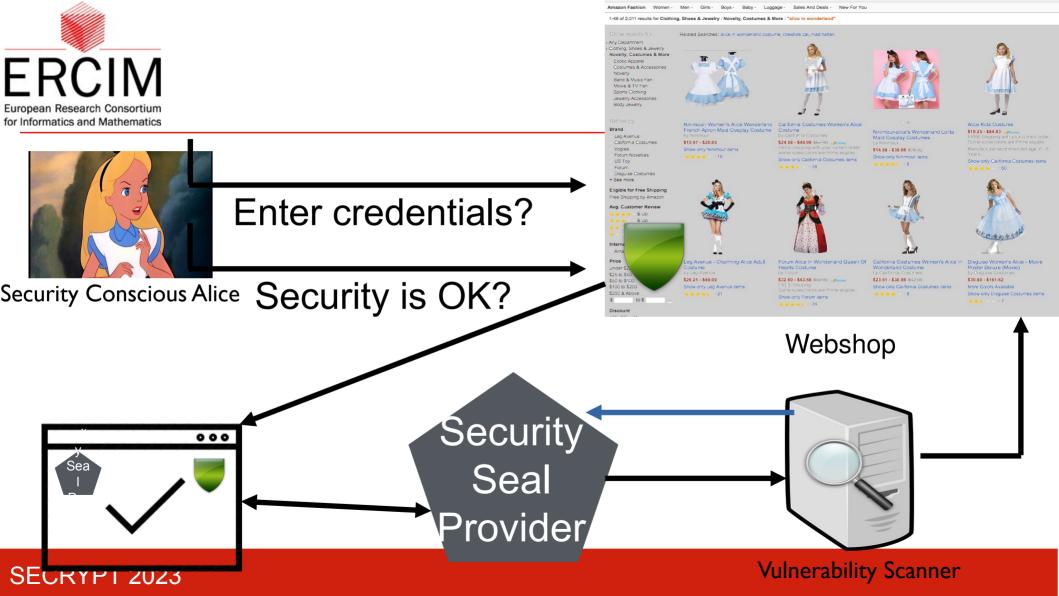
By EFF cc-by 3.0





Clubbing Seals

- Tom Van Goethem, Frank Piessens, Wouter Joosen, Nick Nikiforakis 2014
- Testing the security of webshops that have a seal
- Some shortcomings in the data analyzed
- Recklessly stealing from Nick's presentation



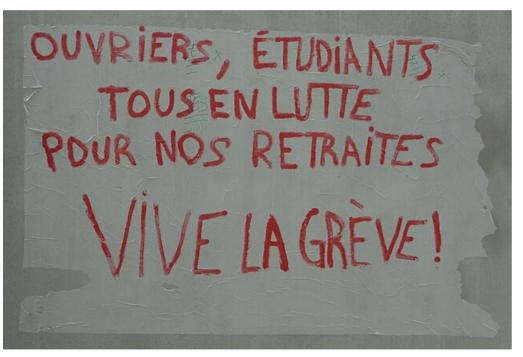
Security Mechanism	Sites w/ Seal (%)	Sites w/o Seal (%)	Significantly different (p-value)
HSTS	1.05	1.06	X (1.00)
Secure Cookies	1.83	0.42	X (0.06)
SSL Stripping	15.45	15.64	X (0.99)
X-Frame Options	3.71	5.14	✓ (0.02)
HttpOnly Cookies	42.27	29.98	✓ (<0.01)
Content-Security-Policy	0.00	0.00	– (NA)
Anti-CSRF tokens	6.39	11.89	✓ (<0.01)
X-Content-Type-Options	0.00	0.00	– (NA)
iframe sandbox	0.18	0.04	X (0.37)



Addionally: Attack vectors

- Security seals are part of an attacker's toolset
 - Attacker can evaluate if seal covers vulnerability
 - Tested sites only fixed things on the list
 - Search for the seal that does not cover vulnerability
- Improve phishing campaigns





Should we oppose Certification?

Abdoucondorcet, CC BY-SA 4.0 <https://creativecommons.org/licenses/by-sa/4.0>, via Wikimedia Commons



There is the human aspect!

- Certificaton helps to think about all aspects
- Certification is a process, not a goal
- Automation helps against bureaucracy





SECRYPT 2023

Thank you



rigo.wenning@ercim.eu @rigo@mamot.fr

