Privacy Resilience and Techno-Policy Standards (?)

The case of the W3C

Julien Rossi

julien.rossi@utc.fr
@julienrossi

utc
SORBONNE UNIVERSITES

COS TECH
Connaissance Organisation et Systèmes TECHniques
UTC EA 2223

UNIVERSITÉ RENNES 2

Can privacy resilience be a property of the information and communication systems we use? And if so, then how?


European Commission
RESEARCH & INNOVATION
Search
Participant Portal
European Commission > Research & Innovation > Participant Portal > Opportunities
HOME
FUNDING OPPORTUNITIES
HOW TO PARTICIPATE
PROJECTS & RESULTS
EXPERTS
SUPPORT
LOGIN
REGISTER
EU Programmes 2014-2020
Search Topics
Updates
Calls
H2020
3rd Health Programme
Asylum, Migration and Integration Fund
TOPIC : Building blocks for resilience in evolving ICT systems
Topic identifier: SU-ICT-02-2020
Publication date: 27 October 2017
Focus area: Boosting the effectiveness of the Security Union (SU)
Types of action: RIA Research and Innovation action
DeadlineModel: single-stage
Planned opening date: 25 July 2019
Deadline: 19 November 2019 17:00:00
Time Zone : (Brussels time)

Topic Description

- Less

Specific Challenge:

Algorithms, software and hardware systems must be designed having security, privacy, data protection and accountability in mind from their design phase in a measurable manner. Relevant challenges include: (a) to develop mechanisms that measure the performance of ICT systems with regards to cybersecurity and privacy and (b) to enhance control and trust of the consumer of digital products and services with innovative tools aiming to ensure the accountability of the security and privacy levels in the algorithms, in the software, and ultimately in the ICT systems, products and services across the supply chain.

Scope:

Proposals are invited against at least one of the following three subtopics:

a) Cybersecurity/privacy audit, certification and standardisation

Innovative approaches to (i) design and develop automated security validation and testing, exploiting the knowledge of architecture, code, and development environments (e.g. white box) (ii) design and develop automated security verification at code level, focusing on scalable taint analysis, information-flow analysis, control-flow integrity, security policy, and considering the relation to secure development lifecycles, (iii) develop mechanisms, key performance indicators and measures that ease the process of certification at the level of services and (iv) develop mechanisms to better audit and analyse open source and/or open license software, and ICT systems with respect to cybersecurity and digital privacy.

b) Trusted supply chains of ICT systems

Innovative approaches to (i) develop advanced, evidence based, dynamic methods and tools for better forecasting, detecting and preventing propagated vulnerabilities, (ii) estimate both dynamically and accurately supply chain cyber security and privacy risks, (iii) design and develop security, privacy and accountability measures and mitigation strategies for all entities involved in the supply chain, (iv) design and develop techniques, methods and tools to better audit complex algorithms (e.g. search engines), interconnected ICT components/systems (v) devise methods to develop resilient systems out of potentially insecure components and (vi) devise security assurance methodologies and metrics to define security claims for composed systems and certification methods, allowing harmonisation and mutual recognition based on evidence and not only on trust.

The trusted supply chain for ICT systems/components should be considered by proposals in its entirety, in particular by addressing the IoT ecosystems/devices that are part of the supply chain.

“Standards intersect with the public interest both because of the critical nature of interoperability in public infrastructures and because they can be enactments of governance themselves.” (DeNardis, 2014, p. 76-77)

Nick Doty & Deirdre Mulligan (2013) : “techno-policy standards”

Standardising body	Documents produced
IETF	RFC 1087 – Ethics and the Internet RFC 6973 – Privacy Considerations for Internet Protocols RFC 7258 – Pervasive Monitoring Is an Attack RFC 3041 – Privacy Extensions for Stateless Address Autoconfiguration in IPv6 (draft) RFC 4941 – Privacy Extensions for Stateless Address Autoconfiguration in IPv6 (draft)
W3C	TAG Self-Review Questionnaire PING Fingerprinting Guidance TPWG DNT (Tracking Compliance & Scope) (Tracking Preference Expression) P3P

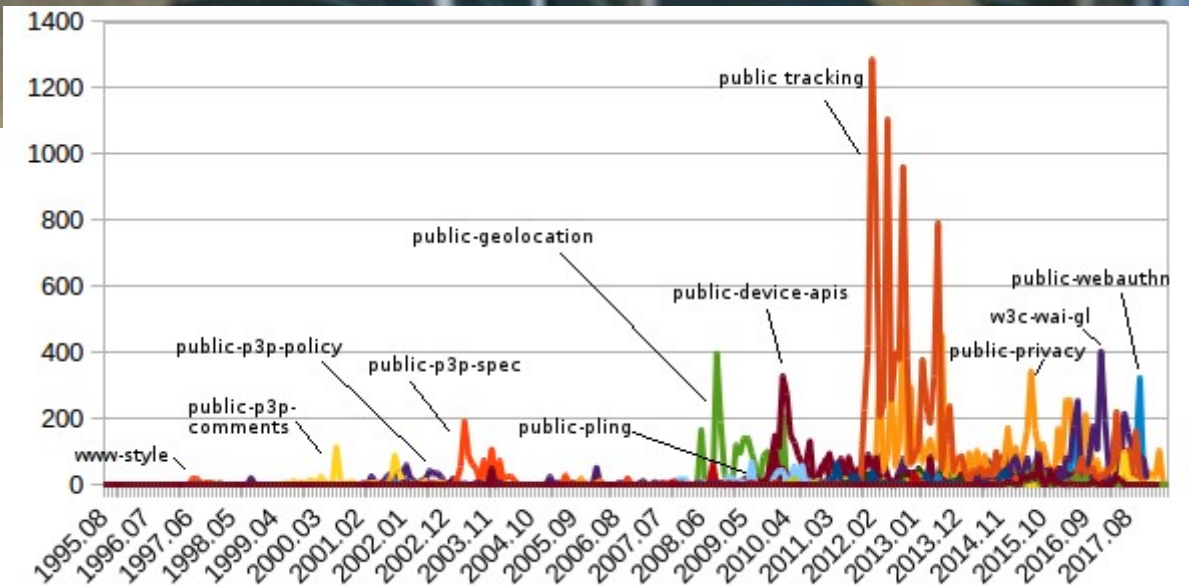
public-privacy@w3.org Mail Archives

Privacy at W3C.

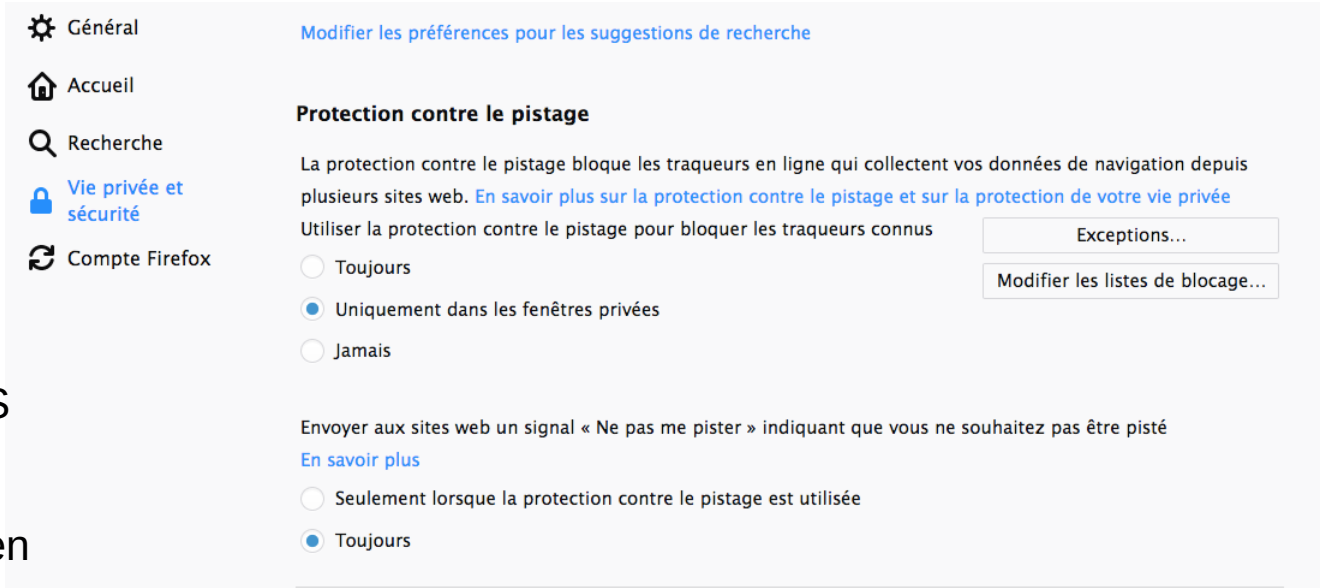
About this list: [Indices by calendar periods] [Latest messages] [Mailbox fo
Mail actions: [mail a new topic] [subscribe to this list][unsubscribe from thi
Help: [How to use the archives] [Search in the archives]

Search this list for [ ] Search

period	re-sorted			messages
July to September 2018	by thread	by author	by subject	9
April to June 2018	by thread	by author	by subject	50
January to March 2018	by thread	by author	by subject	31
October to December 2017	by thread	by author	by subject	23
July to September 2017	by thread	by author	by subject	27
April to June 2017	by thread	by author	by subject	32
January to March 2017	by thread	by author	by subject	36



```
"""
donottrack.py
Jonathan Mayer - jmayer@stanford.edu

A proof-of-concept web proxy that adds a Do Not Track header to all requests.  Not intended for regular use.

v0.02 - 1/30/11
Updated header.

v0.01 - 10/5/10
Sloppy HTTP 1.0 support.  Apologies for any Python faux pas; this is my first foray into the language.
Acknowledgement: Architecture follows Suzuki Hisao's TinyHTTPProxy, http://www.okisoft.co.jp/esc/python/proxy/.
"""

import BaseHTTPServer
import SocketServer
import urlparse
import socket
import select

DoNotTrackHeaderName = "DNT"
DoNotTrackHeaderValue = "1"

AllowedHosts = ["127.0.0.1"]

MAX_RECV = 8192
```



Christopher Soghoian
Sid Stamm
Jonathan Mayer

=> support from the FTC in the US

(idea from around 2009)
(TPWG: chartered between September 2011 and Sept. 2018

Video downloaded from: https://gizmodo.com/heres-the-crazy-wing-bending-airbus-does-to-stress-test-1750425092

Resilience

"Resilience [...] is defined as the ability of the ***system*** to **withstand a major disruption within acceptable degradation parameters <u>and</u> to recover within an acceptable time** and composite costs and risks" (Haimes 2009, 498)

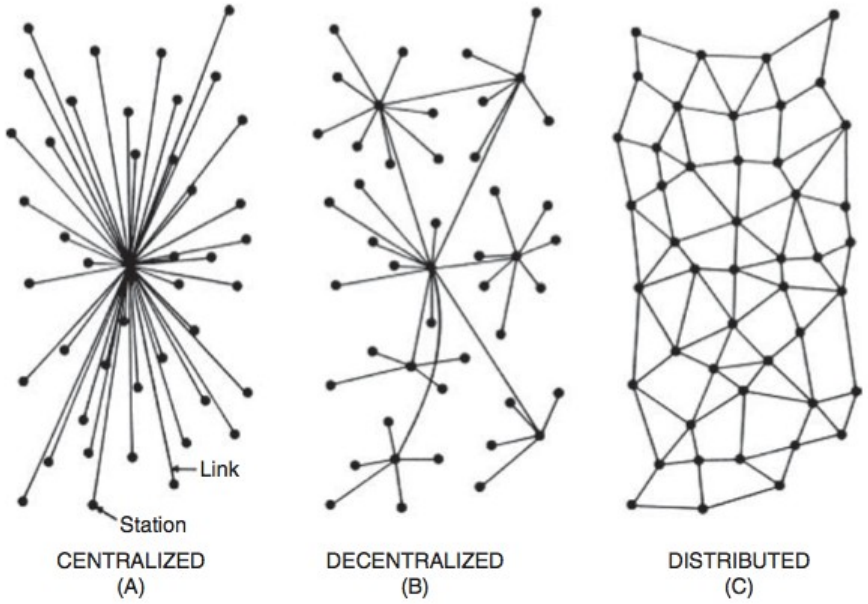


Figure 1.1. Baran's diagrammatic categorization of communications networks: Centralized, decentralized, and distributed networks

Bing, Jon. 2009. « Building Cyberspace: A Brief History of Internet ». Dans : Bygrave LA, Bing J (éd.). Internet governance: infrastructure and institutions. Oxford ; New York : Oxford University Press, p.10

Paul Baran, 'On Distributed Communications—I. Introduction to Distributed Communi- cations Networks', Memorandum RM-3420-PR (Santa Monica: Rand Corporation, 1964), 9.

Resilience

"Resilience [...] is defined as the ability of the ***system*** to **withstand a major disruption within acceptable degradation parameters <u>and</u> to recover within an acceptable time** and composite costs and risks" (Haimes 2009, 498)

"*What I'm trying to pick out with this term is, firstly, a thoroughly heterogeneous ensemble consisting of discourses, institutions,* ***architectural forms****, regulatory decisions, laws, administrative measures, scientific statements, philosophical, moral and philanthropic propositions – in short, the said as much as the unsaid. Such are the elements of the apparatus. The apparatus itself is the system of relations that can be established between these elements*" (Foucault, 1980, p. 194)

Techno-policy standards + users = resilience?

ClientHints

- A new way of getting information about a device
- You get the same information as was already available through various API’s
- But instead of the process going through API’s, it would go into HTTP request headers
- It is discussed by IETF’s HTTP WG, and supported by Google (among others)
- Question: is it bad for privacy?

From the Security Considerations

Implementers ought to consider both user and server controlled mechanisms and policies to control which Client Hints header fields are advertised:

- Implementers SHOULD restrict delivery of some or all Client Hints header fields to the opt-in origin only, unless the opt-in origin has explicitly delegated permission to another origin to request Client Hints header fields.
- Implementers MAY provide user choice mechanisms so that users may balance privacy concerns with bandwidth limitations. However, implementers should also be aware that explaining the privacy implications of passive fingerprinting to users may be challenging.
- Implementations specific to certain use cases or threat models MAY avoid transmitting some or all of Client Hints header fields. For example, avoid transmission of header fields that can carry higher risks of linkability.

Implementers SHOULD support Client Hints opt-in mechanisms and MUST clear persisted opt-in preferences when any one of site data, browsing history, browsing cache, or similar, are cleared.

« Let's focus on providing consumers with greater transparency and control over online data collection and usage » (J.C. Cannon, Microsoft, e-mail on 23 Oct. 2011)

« The way I see it is: privacy and security are both attributes of the system. And security is a tendency for a system to do what it's designed to do. […] Privacy is a little different because this one is user-centric. So regardless of whoever created the system, the question is: does the system do what its users expect with the data? » (Sid Stamm, interview)

« So there is a form of definition, […] I think: user control. And so there has been a lot of focus on things like: talking about permissions, consent, in the web model, having a user agent... The idea is supposed to be that you have this piece of software that is working on your behalf, that you have this control over » (anonymous interview with a PING member)

« Rather than seeing DNT as a “kill switch”, providing user control1 over a powerful process designed to influence their behavior and decision-making is a business practice that should benefit everyone » (Jeffrey Chester, e-mail, 1 Dec. 2011)

Mailing-lists Search service

Search among 1,844,212 messages in the W3C Mailing-List archives

Basic Search | Advanced Search

Look for (Keywords): resilient

and/or subject :

Search in all lists

Or enter list name(s): public-privacy

Search! · Reset

Sorry, no result found.

Mailing-lists Search service

Search among 1,844,212 messages in the W3C Mailing-List archives

Basic Search | Advanced Search

Look for (Keywords): resilience

and/or subject :

Search in all lists

Or enter list name(s): public-privacy

Search! · Reset

Sorry, no result found.

Mailing-lists Search service

Search among 1,844,212 messages in the W3C Mailing-List archives

Basic Search | Advanced Search

Look for (Keywords): resilient

and/or subject :

Search in all lists

Or enter list name(s): public-tracking

Search! · Reset

Sorry, no result found.

ePrivacy Regulation proposal

Article 9

Consent

1.The definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply.

2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet.

3.End-users who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.

Conclusion?

- Techno-policy standards (at least those developed by W3C groups) are not meant with resilience in mind
- They do not create privacy resilience as a property of the technical architecture either
- Can they capacitate individual resilient behaviours?

Roadmap & recommandations

- We need to map out standards and privacy resilient uses (and privacy preserving uses in general)
- For example:
  - Ability to deny (ex: OTR chat systems)
  - Ability to prove (promises made by servers can be proven through logs)
  - Ability to legally protect (eg: the ePrivacy Regulation; eg: if robots.txt had a legal status)
  - Ability to express (eg: DNT TPE, P3P…)
  - … ?

What about collective resilience?

- Reaction to surveillance stress
- The role of privacy ~~resilience~~ against surveillance stress
- The role of fora like W3C PING and W3C TPWG and IRTF HRCIP as (would-be) factors of resilience