Privacy Resilience and Techno-Policy Standards (?)

The case of the W3C

Julien Rossi

julien.rossi@utc.fr @julienrossi







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



Topic Description

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, informationflow 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 fr 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	<u>ct</u> 9
April to June 2018 by thread	by author by subject	<u>ct</u> 50
January to March 2018 by thread	by author by subject	<u>ot</u> 31
October to December 2017 by thread	by author by subject	<u>ot</u> 23
July to September 2017 by thread	by author by subject	<u>et</u> 27
April to June 2017 by thread	by author by subject	ot 32
January to March 2017 by thread	by author by subject	ot 36

₱ #privacy	[09:27:07] [09:27:07] [09:27:23] [09:27:47] [09:27:48] [09:28:03] [09:28:04] [09:28:09] [09:28:22]	jnovak jnovak mkwst jnovak weiter *	2. Zakin sees moneill, weiler, jnovak on the speaker queues monethreshold to be a speaker queues appets scontadevent/onbeforeunlad/ sites having text and specifying who they are aspect of the lying is that websites are declaring something. once someone has said something there's a legal context acking sees weiler. inovak on the speaker queue	a a c d d
	[09:27:07] [09:27:23] [09:27:47] [09:27:48] [09:28:03] [09:28:09] [09:28:22]	jnovak mkwst jnovak weller *	Zakis sees moneill, weiler, invak on the speaker queue Sometht to fellow up on share iskat use saying regarding the user facing aspects S/onloadewent/onbeforeunload/ sites having text and specifying who they are aspect of the lying is that websites are declaring something, once someone has said something the least content, not speaker queue	a c d d
	[09:27:23] [09:27:47] [09:27:48] [09:28:03] [09:28:09] [09:28:09] [09:28:22]	jnovak mkwst jnovak weiter * Jnovak	Sometic: to follow up on what shout was saying regarding the user facing aspects s/onloadevent/onbeforewunload/ sites having text and specifying who they are aspect of the lying is that websites are declaring something. once someone has said something there's a lead context ack mon Zakim sees weller. inovak on the speaker oueue	a c d d
	[09:27:47] [09:27:48] [09:28:03] [09:28:04] [09:28:09] [09:28:22]	mkwst jnovak weiler *	aspects s/onloadevent/onbeforeunload/ sites having text and specifying who they are aspect of the lying is that websites are declaring something, once someone has said something there's a lead context ack mon Takim sees weiler, inovak on the speaker queue	d d
	[09:27:47] [09:27:48] [09:28:03] [09:28:04] [09:28:09] [09:28:22]	mkwst jnovak weiter * jnovak	s/onloadevent/onbeforeunload/ sites having text and specifying who they are aspect of the lying is that websites are declaring something. once someone has said something there's a lead context ack mon Zakim sees weller. inovak on the speaker oueue	d
	[09:27:48] [09:28:03] [09:28:04] [09:28:09] [09:28:22]	jnovak weiler * jnovak	sites having text and specifying who they are aspect of the lying is that websites are declaring something. once someone has said something there's a lead context ack mon Zakim sees weller. inovak on the speaker queue	d
	[09:28:03] [09:28:04] [09:28:09] [09:28:22]	weiler * jnovak	is that websites are declaring something, once someone has said something there's a legal context ack mon Zakim sees weiler, inovak on the speaker gueue	d
	[09:28:03] [09:28:04] [09:28:09] [09:28:22]	weiler * jnovak	there's a legal context ack mon Zakim sees weiler, inovak on the speaker queue	d
	[09:28:03] [09:29:04] [09:28:09] [09:28:22]	weiler * jnovak	ack mon Zakim sees weiler, inovak on the speaker queue	
	[09:28:04] [09:28:09] [09:28:22]	* jnovak	Zakim sees weiler, inovak on the speaker queue	d
	[09:28:09] [09:28:22]	Jnovak		
	[09:28:22]		suggestion that if a site specifies the reason for collecting data.	1
	[09:28:22]		then, that is recorded somewhere in the UA	
		inovak	similar way with DNT and TPWG have a well-known resource where that's	9
			stored as a JSON resource	h
	[09:28:40]	inovak	gives user the ability to remember why they granted permission	
	[09:28:52]	inovak	might be a way to isolate the user agent trustworthy issues	11.1
	[09:28:53]	mount		j
	[80:20:54]	*	Takim sees weiler, inovak, mkwst on the speaker queue	
	09:29:001	inovak	ack weiler:	
	[09.29.00]	*	Zakim sees weiler, inovak, mkwst on the speaker queue	
	[89.29.21]	inovak	while been weight, provide many of the provider but should more of is "how	
	(05125122)	Juoran	ran sites fail more gently"	11.
	100.20.250	dsinger	at at a second sec	
	[89:29:25]	*	Takim sees weiler, inovak, mkwst, dsinger on the speaker queue	
	[89:29:28]	inovak	accept the no and do something useful still	
	[89:29:43]	inovak	ran into a web conferencing application and if it didn't get camera	
	1001201107	Juoran	access wouldn't load	
	[69.29.52]	inovak	want to find some way to encourage sites more generally to behave	
	[05.25.52]	Juoran	hottor	
	[89:38:85]	wseltzer	ack weiler	
	[0.05.96.96]	*	Zakim sees inovak, mkwst, dsinger on the speaker queue	
	[89.30.21]	inovak	is investigated an alternative before to it you give me access to	
	(05150122)	Juoran	this data. I agree to these rules	
	182-86-981	i www.ak	ack deinger	
	[69:30:28]	Clottak *	Takin sees inovak moust on the sneaker queue	
	[89:38:48]	inovak	dsinger: requiators have a hard time regulating privacy but not broken	
	1001001107	Juoran	aranger regetators have a hard time regetating privacy but het broken	
	[09:30:52]	inovak	glazou: if you think that websites are going to avoid failing because ask	
	[05150152]	Juoran	for it	
	[89:38:58]	inovak	noing to be hard to argue for	
	[89:31:88]	inovak	if a website asks for camera, want a stream of bytes	
	[09:31:13]	inovak	if the user says no give a placeholder	
	[89:31:28]	inovak	that way no website is ever noing to fail	
	[09:31:31]	Jilovan	ack in	
	[00.31.41	*	Takin sees most on the sneaker queue	
	[60.31.32]	inovak	well are included of fail in give them comething fake	
	[00:31:58]	mover	inousk: I scree with the noint that if the user save "no" we chould	
	[05.51.50]	inter a c	rature a stream of A butes	
	[69-32-63]	wseltzer	inovak: agree that if user says no don't return broken ani but string of	
	[05152105]	HOCCLET	Ac	
	[60.32.16]	micust	That's what iOS does We return an empty array of contacts etc	
	[89:32:10]	micust	Graceful failure	
	[00:32:19]	*	usaltzer defers to must	
	[09:32:37]	mbuct	weiler. De hers comment to reimplement things to do that?	
	[89.32.50]	innwst	mkwst: yes browsers would have to do something	
	[89.32.50]	weilor	a?	
	[60.32.92]	werten	Zakim sees moust on the sneaker queue	
	[89:32 55]	inovak	a?	
	[09.32.55]	JHOVAK	Zakim sees moust on the sneaker queue	
	[09.32.03]	Wealtzer	ack mk	
	[00.33.00]	#Jettzer	Takin sees no one on the speaker out to	
	[09.33.00]	-	Lakin sees to one on the speaker preue	



```
.....
2
    donottrack.py
3
    Jonathan Mayer - jmayer@stanford.edu
4
    A proof-of-concept web proxy that adds a Do Not Track header to all requests. Not intended for regular use.
5
6
7
    v0.02 - 1/30/11
    Updated header.
8
9
    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
18
    import socket
19
    import select
20
21
    DoNotTrackHeaderName = "DNT"
    DoNotTrackHeaderValue = "1"
                                                            Cénéral
                                                                                   Modifier les préférences pour les suggestions de recherche
24
    AllowedHosts = ["127.0.0.1"]
                                                            Accueil
                                                                                   Protection contre le pistage
26
    MAX_RECV = 8192
                                                            Q Recherche
                                                                                   La protection contre le pistage bloque les traqueurs en ligne qui collectent vos données de navigation depuis
                                                                Vie privée et
                                                                                   plusieurs sites web. En savoir plus sur la protection contre le pistage et sur la protection de votre vie privée
   Christopher Soghoian
                                                                sécurité
                                                                                   Utiliser la protection contre le pistage pour bloquer les traqueurs connus
                                                                                                                                                     Exceptions...
   Sid Stamm
                                                            Compte Firefox
                                                                                      Toujours
                                                                                                                                              Modifier les listes de blocage...
   Jonathan Mayer
                                                                                   Uniquement dans les fenêtres privées
                                                                                     Jamais
   => support from the FTC in the US
                                                                                   Envoyer aux sites web un signal « Ne pas me pister » indiguant que vous ne souhaitez pas être pisté
                                                                                   En savoir plus
   (idea from around 2009)
                                                                                      Seulement lorsque la protection contre le pistage est utilisée
   (TPWG:
                        chartered
                                              between
                                                                                   Toujours
   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 and 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)
- <u>Question: is it bad for privacy?</u>

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)

« 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) « 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)

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

Basic Search Advanced Search		
Look for (Keywords):	resilient	
and/or subject 🗸 :		
O Search In all lists		
• Or enter list name(s):	public-privacy	
Search! · Reset		
Sorry, no result found.		

	W3C°	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 Mai	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 💙 :						
O 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