Technologies for cloud services that protect privacy, data integrity and digital identity by design

DG CONNECT, Unit "Cloud and Software": Consultation on Cloud Computing Research Innovation Challenges for WP 2018-2020

Contribution by
Cédric Thomas, OW2 and Caleb James Delisle, XWiki
November 2016
Outline

► Context
  ► Why we should consider protecting privacy, data and digital identity by design

► Technologies
  ► Three key technology areas that deserve EU attention – and money ;)

► Work programme
  ► Not only technologies but also people...
Context: The Human Factor

- Irrationality
- Information asymmetry
- Public Regulation?
- Change agents
User behavior is plagued by...

Irrationality

- “I've hacked your accounts, I know where you are.”
- “Many recipients just went on surfing”

▶ Do not count on users doing what is in their best interest.
▶ Users, consumers are often irrational
  ▶ Even professional buyers
▶ Think: drinking, smoking, driving, eating, buying, etc.
Information asymmetry

...works in favor of vendors

- Vendors have more information
  - If cheating is possible they will
  - Also called “Market imperfection”
- Think: second hand car, pharmaceutical, financial products...
  - “Basically the result of this is that users will adopt whatever technology is put in front of them because they don't know its full costs and therefore it is society's obligation to help protect them?”

https://commons.wikimedia.org/wiki/File:Kovacs_special_1968.JPG
https://www.flickr.com/photos/127619525@N05/15075074577
https://pixabay.com/fr/d-affaires-hommes-d-affaires-1320058/

(cc) 2016, Cedric Thomas, Caleb James Delisle
Public regulation?

“However, we do not believe that a stand-alone cloud regulatory framework is necessary to address these concerns. (...) Customer education is the single most important element of a program to drive cloud confidence.”
Silicon Valley did begin as an open and agile culture of hackers and tinkerers based around UC Berkeley and Stanford.

Every attempt at replicating Silicon Valley so far has failed, every time we try to emulate what it is today without recognizing where it began.

An "intolerant minority" (only 3-4%) can dictate the preferences of an entire population (Nassim Taleb)

The intolerant minority of privacy and security conscious individuals and businesses will shift the market
Technologies: Back to (Internet) Basics

End-to-End Encryption
Zero-Knowledge Cloud Services
Protocol-Based Architectures
End-to-End Encryption

Definition

Encryption which protects messages from all of the intermediary servers between their origin and their destination.

Relevance

20 years ago, HTTPS was considered by the US government to be a munition, now it is a basic pillar of e-commerce.

E2EE will be a key enabler of new services and new architectures.

Challenges

Multi-party key agreements
Proxy recryption

https://www.flickr.com/photos/111692634@N04/11406975556 - www.bluecoat.com/
https://www.flickr.com/photos/ideonexus/5175383269
Zero-Knowledge Cloud Services

Definition

Zero Knowledge Cloud Services are services which use End to End Encryption to make themselves **blind to the data which they host**

Relevance

Zero Knowledge Cloud Services can uniquely provide the benefits of the Cloud with the auditable security of the client side (cryptographic) software

Challenges

- Operations on hosted data
- Homomorphic encryption
- Order preserving encryption
- Substitution cyphers

Protocol-Based Architectures

**Definition**

- Protocol-Based Architecture are **distributed** with no dependence on a central server.

**Relevance**

- Protocol-Based Architecture is about avoiding value capture by monopoly-oriented platforms and building the next generation internet services (incl. IoT) around open protocols implementing the peer-to-peer paradigm.

**Challenges**

- Blockchain processing issues
- Self hosting paradigm
- Modeling, code-ification of trust
- Protocol standardisation
Work programme: Technologies and People

Perspectives
“Technology” objective
“People” objective
Perspectives

“By design” perspective

“Users are irrational; Expertise asymmetry works in favor of vendors; Public regulation will not be accepted; Privacy and security should be enabled by design.”

“Activist” perspective

“Rent-based monopolies didn't create Silicon Valley; The future is bottom-up, participatory and open source; Encryption is critical to business; A healthy active minority will shift the market.”
“Technology” objective

“By design” perspective:

“Users are irrational; Expertise asymmetry works in favor of vendors; Public regulation will not be accepted; Privacy and security should be enabled by design.”

Help develop technologies for cloud services that protect privacy, data integrity and digital identity by design:

- Protocol-Based Architectures
- End-to-End Encryption
- Zero-Knowledge Cloud Services
“People” objective

“Activist” perspective:

“Rent-based monopolies didn't create Silicon Valley; The future is bottom-up, participatory and open source; Encryption is critical to business; A healthy active minority will shift the market.”

Foster through research grants and other means a European hacker scene to rival the hacker/geek scene which lead to Silicon Valley.

Facilitate agile transfers between European hacker communities and startups and SMEs

Support developers' communities, OW2! ;)

Support hacker-oriented events, hackathons, etc.
Thank you

And now let's talk Q&A Disagreements Complements Feedback etc.