Design and analysis of technical systems for humans

Introductory talk

Victor Morel
https://victor-morel.net/

Chalmers University of Technology

morelv@chalmers.se

CHALMERS
UNIVERSITY OF TECHNOLOGY

WASP WALLENBERG AI, AUTONOMOUS SYSTEMS AND SOFTWARE PROGRAM

6^{th} October 2022

Goals of this presentation

Introduce myself to iSec

- Where I was / What I did
- What are my interests / What could be my input

Present my past work

- PhD thesis: Enhancing information and consent in the IoT
- A standard for consent in the IoT
- Recent paper on cookie paywalls

Expose my perspectives

- For the CyberSecIT project
- In line with my research interests

Outline

Sweden: there and back again

Master thesis in Uppsala

Generating co-evolutionary polarized opinion networks

PhD in France

Inria - Privatics (Lyon), Enhancing information and consent in the IoT

Back to Sweden

For *kannelbullar*? ~~For *kannelbullar*?~~ For a postdoc at iSec

Kanelbullar by hepp, CC-BY 2.0

Title explained - *Design and analysis of technical systems for humans*

Design?

- Not just as in *interface design*
- More like *conception* of systems

Analysis?

- Technical analysis
- Network and data science background

Humans?

- Often the weak link of technical systems
- Providing a technical interpretation of legal requirements

Blending law, design/HCI, and computer science

Law because

Privacy is also a legal topic

Design/HCI because

Research is needed on both *architectures* and *interfaces* of systems

Computer science because

I am still a computer scientist

The combination of the three...

... results in promising research
... tailored to a *human* society

SoK: Three facets of privacy policies, Morel and Pardo, 2020

Research interests

Outline

Past, present, future

Past

PhD work at Inria

Present (recent past)

Short postdoc in Austria

Future

Perspectives on the CyberSecIT project

Outline

The Internet of Things

- Growing infrastructure
- Numerous devices, various uses
- Limited capacities and interfaces
- Different types of data collected

Privacy concerns in the IoT

Personal data collection

→ Risks of surveillance and abuse of targeted advertising

→ Specific issues raised with the IoT

→ Difficult to comply with regulations

General Data Protection Regulation

GDPR

- Most recent legal framework for personal data protection in Europe
- Extra-territorial scope: impact outside Europe as well
- Introduces rights for data subjects
- And obligations for data controllers

Key ideas

- Bundle of principles (Art. 5)
  - Fair and transparent processing
  - Purpose limitation
  - Data minimization ...
- Content of information (Art. 13/14)
- Conditions for consent (Art. 7, 4(11))

Research question and global approach

It is possible to design a generic framework to communicate information and manage consent in the Internet of Things?

TL;DR: yes.

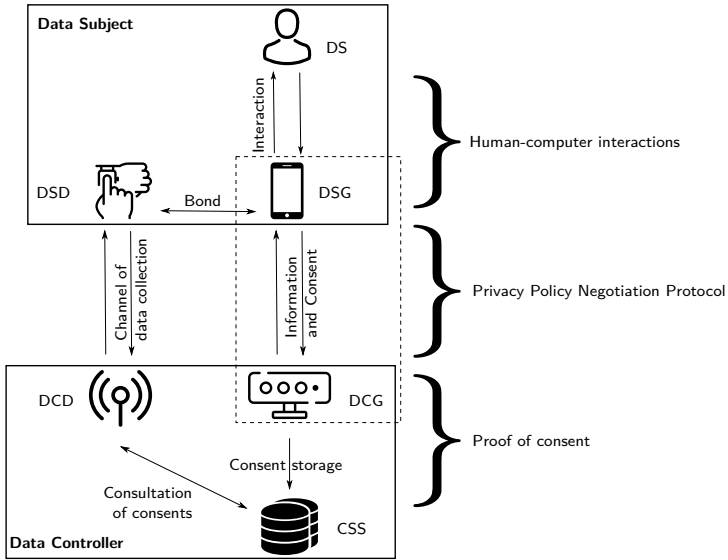
Global approach

- Machine-readable privacy policies for information and consent
- Controller privacy policies for commitment
- Data subject privacy policies to define choices

A Generic Information and Consent Framework for the IoT, Cunche, Métayer, and Morel, 2019

Outline

A generic framework for information and consent in the IoT



Explanatory diagram of the framework

ColoT: a proof of concept

ColoT - A Consent and Information assistant for the IoT

A mobile app

- Designed for Android
- Works with a gateway device (ESP32)
- Implements:
  - Information through different channels
  - P2P consent management via BLE
  - Proof of consent
- Video time!

Colot: a consent and information assistant for the iot, Cunche, Métayer, and Morel, 2020

Outline

Engaging with other disciplines working on consent

Willfulness to engage with:

Viennese croissants?

Law

Consent is notably a legal issue

Design

Dark patterns

Cognitive science

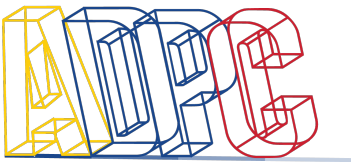
User-centered perception

Interdisciplinary paper

On DPCCMs (ADPC & GPC)

Data Protection and Consenting Communication Mechanisms, Human et al., 2022

ADPC-IoT



An alternative to cookie banners

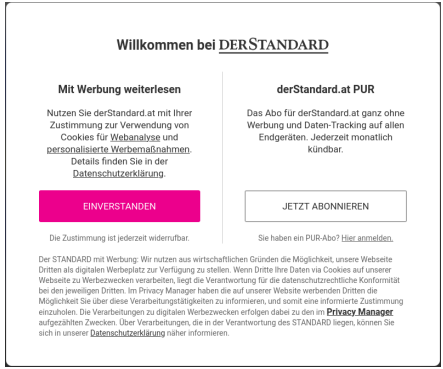
In partnership with the Austrian NGO

Porting ADPC to the IoT

Towards standardization of consent

Outline

Cookies?



More like cookie paywalls!

→ **Overlooked by academia**

Your Consent Is Worth 75 Euros A Year, Morel et al., 2022

Methodology and findings

Description

- Manual annotation of top Central Europe websites (Tranco list)
- Presence and type of wall, category of website, general info (price etc)

Measurement

- 61 of the 2800 websites studied use paywalls (2.72%), and 13 cookie paywalls (0.66%)
- Most cookie paywalls consist of news websites

Legal analysis of both cookie walls and paywalls

Divergent positions on cookie walls and paywalls from EU DPAs

Updated classification

Hard, *soft* **and** *metered paywall*, **registration wall**, **cookie wall**, and **cookie paywall**

Future work on cookie paywalls

We also found out that cookie paywalls:

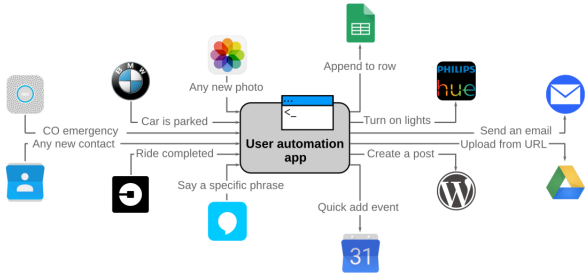
- They do not track visitors prior to interaction
- Websites present different versions → personalized pricing?

Different presentations on Chrome and Firefox

→ Requires *large scale analysis* **and** *automated tracking detection*

Outline

Overview of CyberSecIT



Two key challenges for security and privacy in IoT app platforms

- Automation → securing software from malicious attackers
- Autonomy → securing machine-learning for IoT apps

WP2: Usable privacy-enhancing permission management

High-level goal

To develop usable UI techniques and prototypes, supported by machine learning

Task 2.1

Privacy Profiles for IoT application permissions (relates to consent)

Task 2.2

ML-supported usable and privacy-compliant permission management

Task 2.3

Usable UIs for permission management

Outline

User studies

How to build privacy profiles?

- By conducting user studies (surveys)
- With focus on legal, cross-cultural, and gender aspects
- Using vignette studies

Example of a vignette

Consider that you exercising using a *fitness device* that collects your *HeartRateVariability* to *assess your sport performance*. This data will be stored for a year on the servers of *Fitbits*, a private company.

Research questions

→ What are the privacy preferences and expectations in Trigger-App Platforms with respect to privacy permissions and privacy notifications?

→ What is the influence of the legal framework in these preferences and expectations?

Outline

Summary

What was this presentation about? Mostly pastries! 🥐

But also consent and human factors:

- A technical interpretation of GDPR requirements
- Interdisciplinary view on consent management
- Cookie paywalls
- User studies for the CyberSecIT project

Grab a coffee? (With pastries *naturligtvis*)

Bibliography

- Cunche, Mathieu, Daniel Le Métayer, and Victor Morel (2020). "CoIoT: a Consent and Information assistant for the IoT". In: *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 334–336.
- Cunche, Mathieu, Daniel Le Métayer, and Victor Morel (2019). "A Generic Information and Consent Framework for the IoT". en. In: p. 9. URL: https://hal.inria.fr/hal-02166181.
- Human, Soheil et al. (2022). "Data Protection and Consenting Communication Mechanisms: Current Open Proposals and Challenges". In: *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, pp. 231–239.
- Morel, Victor and Raúl Pardo (Aug. 2020). "SoK: Three Facets of Privacy Policies". en. In: *WPES*. DOI: 10.1145/3411497.3420216. URL: https://hal.inria.fr/hal-02267641 (visited on 09/25/2019).
- Morel, Victor et al. (2022). "Your Consent Is Worth 75 Euros A Year–Measurement and Lawfulness of Cookie Paywalls". In: *arXiv preprint arXiv:2209.09946*.