IPEN - The Internet Privacy Engineering Network

Workshop:

Engineering Privacy into Internet Services and Applications

Date: Friday, 26 September 2014
9:00 – 17:00

Venue: Berlin State Parliament, Berlin, DE
Niederkirchnerstr. 5, 10111 Berlin-Mitte, near tube station Potsdamer Platz

Organisers: Co-hosted by EAID, EDPS, Berlin BDI, OWASP Top 10 Privacy Risks Project, ULD, CNIL, IE DPC, CBP NL, ICO, Oxford Internet Institute, University College London

Draft Agenda

9:00 - 9:30 **Registration**

9:30 - 10:00 **Opening keynotes:**

Ralf Wieland, President of Berlin Parliament (Abgeordnetenhaus)

Peter Hustinx, European Data Protection Supervisor

Dr. Alexander Dix, Berlin Data Protection Commissioner

10:00 - 11:00 **Session 1: Exploring the existing initiatives & tools and identifying the technical gaps.**

Moderator: Achim Klabunde (EDPS)

Panellists: Florian Stahl & Stefan Burgmair (OWASP), Hannes Tschofenig, (ARM), Jens Kubieziel (Tor), Rob van Eijk (CBP NL), Dr. Joss Wright (OII), Stéphane Petitcolas (CNIL)

There are a number of examples of existing tools and developing initiatives for better technical support of privacy, as well as the IETF efforts to consider privacy in the design of internet protocols. OWASP Top 10 Privacy Risks Project has collected information on where privacy issues need to be addressed.

The panellists will briefly present existing initiatives and tools for privacy aware development and on-going projects, then will discuss what is covered by the existing tools, and where the gaps still need to be filled.

11:00 - 11:15 **Coffee**

11:15 - 11:30 **Keynote presentation: Peter Schaar (EAID)**

11:30 - 12:30 Session 2: Use Cases – How can we identify and address privacy gaps?

Moderator: Marit Hansen (ULD)

Panellists: Dr. Stephen Farrell (Trinity College Dublin), Dr. George Danezis (University College London), Ultan O'Carroll (IE DPC), Massimo Attoresi (EDPS), Dr. Jaap-Henk Hoepman (Radboud University Nijmegen)

Despite the preoccupation of users to protect their privacy, it appears that the use of available privacy options and tools is less than could be expected. Some of the reasons are technological: complexity, usability issues, missing transparency, lack of user control. But is user friendly design and implementation the only problem? Are existing privacy features actually providing what users need? Are they sufficient to make apps and services compliant with data protection obligations? This session will discuss fall short of users' needs and expectations and which privacy controls and features will need to be developed and integrated in new tools and services.

12:30 - 13:30 Lunch

13:30 - 16:00 Session 3: Approaches to engineering privacy

Moderators: Achim Klabunde (EDPS), Marit Hansen (ULD), Dr Simon Rice (ICO)

In three subsequent conversations, participants will discuss the approach to engineering privacy from different angles. Each conversation will be kicked off by two short presentations which present two distinct perspectives on the subject of the discussion. Practical use cases may be used to illustrate the approaches.

First conversation:

- **Hannes Tschofenig**: Privacy considerations for Internet protocols
- **Rob van Eijk**: Privacy risk assessment as an engineering tool

PRIVACY CONSIDERATIONS

Privacy considerations are a form of guidance to increase awareness of privacy related design choices. We will explore to what extent there is a gap between the perspectives on privacy considerations of data protection authorities and the standards community. We will look at both perspectives. The design of a protocol is very different from the assessment of the legal compliance of (components of) an information system. Therefore, these perspectives may very well contradict.

On the one hand, from a standards community perspective, privacy considerations are a design issue. The aim is to make designers, implementers and users of technical protocols and specifications aware of privacy related design choices. The privacy considerations for e.g., (internet) protocols and API's are rooted in a tradition of security considerations.

On the other hand, from a data protection perspective, privacy considerations are a policy issue. Under the European Commission's proposed Data Protection Regulation, a Data Protection Impact Assessment (DPIA) would become mandatory. The purpose of a DPIA is identifying and mitigating all types of privacy risks, e.g., not limited the impact of eavesdropping or data breaches.

Second conversation:

- **Frank Dawson**: Privacy Engineering & Assurance as an Emerging Engineering Discipline
- **Ultan O'Carroll**: Integrating privacy requirements in the systems engineering process

PRIVACY ENGINEERING PROCESS

The Privacy Engineering & Assurance discipline provides a systematic and engineering compatible approach to implementing privacy. It also integrates a code of ethics and professional practice. The discipline needs to be supported by professional certification and educational academic curriculums that provide a source for needed software engineering resources.

On the other hand, developers are already working in a defined environment of procedures, constraints and non-functional requirements. Developers, therefore, have to trigger an incremental transformation which they can start now by adapting their use of tools and experience to drive an effective "bottom up" approach to engineering privacy.

Third conversation:

- **Dr. George Danezis**: Real life demands and constraints for a developer
- **Stéphane Petitcolas**: Real life data protection requirements

REAL LIFE CONDITIONS

Engineering Privacy has to be integrated within the overall engineering process, and is subject to its technical and budgetary constraints and trade-offs. Those include conflicting requirements between privacy, integrity and functional requirements; the availability, usability and maturity of privacy-friendly, privacy-enhancing solutions; and the integration of 3rd party components, or architectures that may be unaware of privacy considerations. In this session, we will discuss examples of projects and strategies that can achieve a high degree of privacy protection while minimizing engineering risk.

Use Case Examples:

- Integration of 3rd party services in web sites
- Transparent Privacy Settings
- Tools against digital trails
- Tools for mobile tracking
- Password registration
- Policy-Aware Web
- Secure transfer

16:00 - 16:45 Conclusions: Where to go from here?

17:00 Closing remarks

An after-party for participants may be arranged in the evening after the workshop.

For more information about this Workshop, please see the Practical Information document.

To register for this event, please fill out the Registration Form and return to ipen@edps.europa.eu

Confirmed speakers:

Keynotes presented by:

- **Ralf Wieland, Präsident des Abgeordnetenhauses von Berlin**
- **Peter Hustinx, European Data Protection Supervisor**
- **Dr. Alexander Dix, Berlin Commissioner for Freedom of Information and Data Protection**
- **Peter Schaar, Chairman of the European Academy for Freedom of Information and Data Protection (EAID), former German Federal Commissioner for Freedom of Information and Data Protection**

Panellists:

- **Florian Stahl, OWASP Top 10 Privacy Risks Project**
- **Stefan Burgmair, OWASP Top 10 Privacy Risks Project**
- **Dr. George Danezis, University College London**
- **Dr. Joss Wright, Research Fellow at the Oxford Internet Institute, University of Oxford**
- **Dr. Stephen Farrell, Trinity College Dublin**
- **Dr. Jaap-Henk Hoepman, Privacy & Identity Lab /Radboud University Nijmegen**
- **Hannes Tschofenig, ARM, Ltd.**
- **Jens Kubieziel, Tor**
- **Frank Dawson, Nokia**
- **Marit Hansen, Marit Hansen, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)**
- **Ultan O'Carroll, Office of the Irish Data Protection Commissioner**
- **Rob van Eijk, College Bescherming Persoonsgegevens (CBP)**
- **Achim Klabunde, Head of IT Policy, European Data Protection Supervisor (EDPS)**
- **Massimo Attoresi, European Data Protection Supervisor (EDPS)**
- **Dr. Simon Rice (ICO)**
- **Stéphane Petitcolas (CNIL)**

Possible Use Cases for Break-Out Groups in Session 3:

- **Integration of 3rd party services in web sites**: (**#3rdpartytools**)

  Integrating third parties services may potentially expose web visitors to tracking based on scripts, cookies or other devices. Visitors' personal data is disclosed to third parties with which visitors often have no connection, no knowledge nor any *willingness to allow them processing. Web site operators run the risk of non-compliance with data protection legislation and of losing the trust of their users. Therefore, some users are likely to stop visiting the site or to use content blocking tools that would (if widely adopted) reduce the website revenues.*

Is it possible to integrate third party elements into web sites in a way that respects the visitor' rights to privacy and data protection? How can the web site operator ensure that visitors receive meaningful information the data processing by third parties and have effective ways to give or withhold consent to such processing?

- **Transparent Privacy Settings**: (**#privacysettings**)

  Users are confronted with a huge variety of functions and measures which collect and process personal data for different purposes. The descriptions in complex privacy policies often are not fully clear. Even when privacy settings can be chosen by the users, their meaning may be different from what the users expect. In many situations, users may be confronted with several such mechanisms at the same time, e.g., when browsing web pages with 3rd party elements, often from several parties such as ad brokers. Additionally, some systems may even be incompatible with each other, e.g., when opting out of one system requires permitting third-party cookies.

  Is it possible to develop an effective and efficient system of privacy information and choices that gives the users meaningful control over the processing of their data? Can that work on mobiles?

- **Tools against digital trails: (#mobiletracking)**

  Smart phones have many ways of tracking the moves of their users. Traces can also increasingly be linked across different devices. There is scientific proof that even seemingly anonymous data (e.g., location information of cell phones) can be traced back (i.e., be de-anonymised) if the database and the timeframe are sufficiently broad. However, location aware services are so attractive and convenient that users accept the tracking mechanisms, often unaware of the volume of data they disclose.

  How could tracking be limited to what is absolutely necessary for a service? Can the storage of data be limited in time? Is it possible to aggregate data at a low level of the network to avoid the building up of too big data sets? Can the purpose limitation for location data be technically supported?

- **Password registration**: (**#passwordregistration**)

  Even though publications about data breaches and password theft seem to become more and more frequent, we may still be seeing only the tip of the iceberg. Choosing strong passwords, changing them frequently and not reusing passwords across several services are recommended measures, but put big strain on human memory. Cross-service credentials may be an option, but they come with other privacy issues, disclosing much to the main provider.

  Is there a way to maintain a multitude of strong and diverse passwords in a secure manner? Are any existing tools reliable and recommendable? What would be needed for a reliable secure password registrations system? Or is the 'forgotten password' email request still the best approach?

- **Policy Aware Web: (#policyawareweb)**

  Personal data (and any other information), once published online, will very likely remain publicly available. Even if they are deleted on the original website, they may have been linked to or mirrored on other sites before deletion. Restrictions on the use of the information given at its original source will not be copied with the information, e.g., when a photo is copied from one social network from another, it may become more public than intended and chosen by the original publisher. There is no simple technical tool available at present which could ensure the systematic deletion of data on the web (i.e, which could teach the Web how to forget).

  The concept of the Policy Aware Web combines several existing technologies, namely structured data, identity management, access control, and sticky policies (i.e., use policies that travel with the data itself). Tools for controlling the availability of (personal) data on the web based on limiting contents exposure on a website either through the application of (automatic) deletion mechanisms or via the implementation of search preference signalling protocols. Can this concept help to improve privacy on the web and how could that work?

- **Secure transfer: (#securetransfer)**

  Sending unencrypted data can compromise the privacy of users. Personal data should be secured during transfer through unsecured networks (e.g., internet GSM/UMTS, public WLAN, etc.).

  User-friendly, secure, efficient, interoperable seem to be mutually contradicting objectives. Is it possible to establish a broadly usable system for (nearly) everybody with today's toolkits?

- **Other subjects:**

  Participants are invited to present other ideas.

iD Datenschutz und Informationsfreiheit in Berlin

EAID

ULD

An Coimisinéir Cosanta Sonraí Data Protection Commissioner

COLLEGE BESCHERMING PERSOONSGEGEVENS

UCL

ico. Information Commissioner's Office

European Data Protection Supervisor