Designing Privacy into Systems

(and what is the role of organizations developing standards)

Hannes Tschofenig (IAB)
Jon Peterson (IAB)
Bernard Aboba (IAB)
Karen Solins (MIT CFP PrivSec)

“Privacy”

- In the context of this presentation the term “privacy” refers to the privacy principles regulators & others have created, such as the “Fair Information Practices”* developed by the OECD.

(*)Organization for Economic Cooperation and Development, "*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*", http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html, 1980.

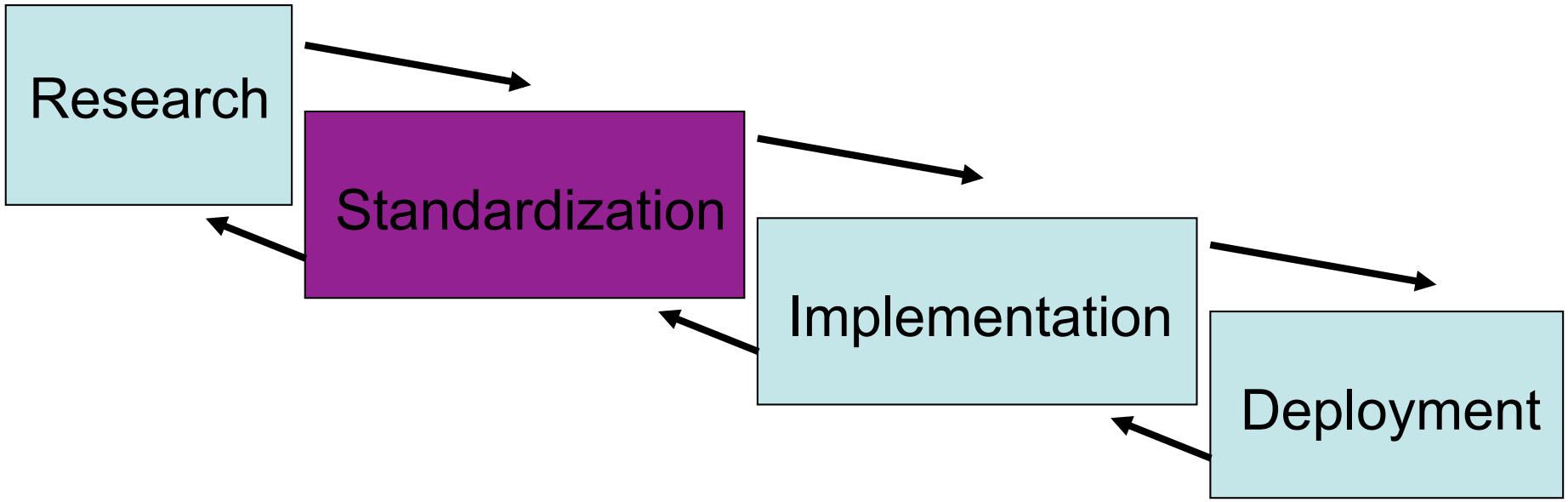
Intro

- Judging from the previous work the IETF applies a hybrid between “privacy by design” and “privacy by policy”.
- “Privacy by design” is a concept more understandable to engineers.

How do systems get developed?

- Basic approaches:
  - Developed by standards organization
  - Proprietary system
  - Built on top of standards
- Need for standards is higher in lower layers of the protocol stack
- Level of necessary interoperability quite low at the application layer
  - And seems to get lower and lower.
- The IETF has intentionally gotten itself “out-of-the-business” at the application layer.
  - Good for ensuring high speed of innovation.
  - We develop generic solutions rather than point solutions. Example: Transport of all sorts of data over HTTP rather than describing how to carry specific health data over HTTP, financial data over SIP, etc.

Scope of work at SDOs



- Quite often (in the IETF at least) we see implementation and deployment before protocols (and architectures) get standardized.

*: Graph ignores all possible feedback loops.

Challenges

- In the IETF success of a protocol is also defined in terms of deployment.
  - Standardizing something that is already deployed leads to an “immediate reward”.
  - Typically a good mixture of standardize before deployment and standardize the deployed system is utilized.
- When something is deployed then it is obviously difficult to introduce major changes in standardization.
  - Not only a problem for privacy properties of the system but for anything else.
- Too theoretical design might lead to lack of deployment.
- Main question: How far to push certain properties without negatively impacting deployment?
- Implementation and deployment are often not part of the work in SDOs.
  - From the experience in security these are the areas where lots of mistakes are being made.
  - Fixing them is often not “exciting enough” for researchers and standards professionals.
- What is done in deployment is often very difficult to learn
  - Many reasons, including business secrets, no incentives to disclose, lack of communication with those who deploy systems.

Example: SIP: Session Recording, End-to-End Security, and Media Security

- SIP is a protocol for session establishment and maintenance. It is heavily used in the voice over IP environment.
- Privacy was not an explicit design criteria but a number of privacy extensions were developed as an add-on.
- With the huge market interest in these systems business requirements (for extended functionality of intermediaries) and business/regulatory requirements came along.
- Examples of challenges:
  - End-to-End identity solutions experienced problems with middleboxes destroying end-to-end properties
  - End-to-End media security got into conflicts with what certain telecommunication operators thought would be required by regulators.
  - Session recording of media due to quality control, etc.
  - Some of these requirements are in conflict with core values of the IETF, including the “IETF Policy on Wiretapping” RFC 2804.
- How to tackle these conflicting requirements?

What can be done by groups like W3C and IETF?

- Terminology
  - A recent attempt: http://tools.ietf.org/html/draft-hansen-privacy-terminology-00
- Education and awareness building among their engineers
- Guidelines how to consider privacy as one design factor in protocol design and the development of architecture
  - Largely to make privacy aspects explicit.
  - Follows the model of writing “security considerations sections”
- Establish review teams to ensure high quality of documents
  - Requires a certain organizational model to ensure that minimum requirements are met.
- Try to develop a similar view among major SDOs to avoid forum shopping.
- Identify implementation and research challenges
- Education towards regulatory groups (IAB, ISOC, W3C TAG) about what technology can do
- Regulators could help to increase transparency