NIST Privacy Engineering Objectives and Risk Model Discussion Draft

Introduction

In April 2014, NIST held a workshop focused on advancing privacy engineering as a basis for the development of technical standards, guidelines, and best practices for the protection of individuals' privacy and civil liberties.[1] Workshop discussions assessed models provided by other disciplines such as cybersecurity and safety risk management, and whether they could be adapted to privacy. Process-oriented privacy principles (such as the Fair Information Practice Principles (FIPPs)) are an important component of an overall privacy framework, but on their own they have not achieved consistent and measurable results in privacy protection. In the security field, risk management models, along with technical standards and best practices, are key components of improving security. Similarly, the safety risk management field also has well-developed models, technical standards and best practices. To date, the privacy field has lagged behind in the development of analogous components.

The NIST series of privacy engineering workshops seeks to address these gaps and challenges. The April workshop convened a wide variety of stakeholders from across sectors and disciplines. Some key considerations that emerged from the workshop included:

1. There is a communication gap around privacy between the legal and policy, design and engineering, and product and project management teams that increases the difficulty for organizations to manage privacy concerns effectively, understand risks and implement mitigating controls before harm occurs. A contributing factor is the lack of a common vocabulary and set of tools that can be used to build consistent requirements and technical standards across organizations.
2. More development is needed of tools that measure the effectiveness of privacy practices.
3. Overall risk management should be a fundamental driver of an organization's approach to privacy.

Building off of this feedback, NIST has developed a set of privacy engineering objectives and a risk model to facilitate discussion at the next NIST privacy engineering workshop on September 15-16, 2014 in San Jose, CA.[2] The accompanying slide discussion deck defines the privacy engineering objectives and the risk model, as well as their underlying components.

Scope

NIST's privacy engineering work is focused on providing guidance to developers and designers of information systems that handle personal information. This guidance may be used to decrease risks related to privacy harms, and to make purposeful decisions about resource allocation and the effective implementation of controls. Privacy engineering as defined in this discussion draft is primarily directed at mitigating risks arising from unanticipated consequences of normal system behavior. Risks to privacy

[1] More information about the first NIST Privacy Engineering Workshop, including agenda, summary, and archived video, can be found at http://www.nist.gov/itl/csd/privacy-engineering-workshop.cfm.

[2] For the purposes of this discussion draft, the "privacy engineering objectives" are intended to function in a similar manner to the security objectives in NIST FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems." Available online at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf. In other literature, such objectives may be referred to as "quality attributes" or "system properties."

arising from malicious actors or attacks can continue to be mitigated by following standard security standards and frameworks.

In addition, this discussion draft does not describe a complete privacy risk management framework. A potential framework might include not only a set of design objectives and a risk model, but also other components such as a mapping to specific controls to mitigate identified risks. For instance, privacy controls may be derived from principles such as the FIPPs (e.g., notice and consent mechanisms or data minimization techniques), as well as achieved through security technologies such as encryption. This discussion draft covers only the foundational concepts of design objectives and a risk model. NIST will evaluate adding additional components over time, including the appropriate means of addressing controls based on feedback at the September workshop and comments.

Proposed Privacy Engineering Objectives

At the April Workshop, NIST introduced the concept of design objectives that are outcome-based and provide important measurement capabilities. In cybersecurity, the objectives Confidentiality, Integrity and Availability (CIA) have enabled organizations to make risk impact assessments about the implementation of these objectives, design system requirements for cybersecurity and evaluate and test the effectiveness of an organization's controls for achieving these objectives.[3] Ideally, systems that maintain CIA should be able to mitigate security harms; and likewise, systems that maintain privacy engineering objectives should be able to mitigate privacy harms to individuals.

NIST received positive feedback from attendees at the April Workshop about the need for such objectives, but only minimal input on their composition. Therefore, in developing the objectives, NIST staff explored current and long-standing theories on the concept of privacy such as controlling for surprises[4] and avoiding the "creepy" factor[5], self-determination and individuals' interest in controlling their information[6] and freedom from intrusion.[7] As a result, the objectives are designed as overarching system characteristics that encompass these privacy concepts and enable the mitigation of privacy harms. Optimally, they also can help demonstrate that privacy-preserving systems can have net-positive outcomes on operational purposes.

NIST proposes the following three privacy engineering objectives:

- **Predictability** is enabling reliable assumptions about the rationale for the collection of personal information and other data actions to be taken with that personal information. Predictability helps to address concerns about avoiding unpleasant surprises that create public backlash.
- **Manageability** is providing the capability for authorized modification of personal information, including alteration, deletion, or selective disclosure of personal information. Manageability can provide the technical capacity for improving choices about the handling of personal information and individuals' participation in such decisions.

[3] For definitions of CIA, see NIST FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems." Available online at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.
[4] Wilton, Peter, "Four ethical issues in online trust" Internet Society. 2014 Available online at http://www.internetsociety.org/sites/default/files/Ethical%20Data-handling%20-%20v2.0.pdf
[5] Cranor, Lorrie Faith, et al, "Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising". Carnegie Mellon University. April 2012. Available online at https://www.cylab.cmu.edu/research/techreports/2012/tr_cylab12007.html#sthash.cy91myyj.dpuf
[6] Westin, Alan, "Privacy and freedom". New York: Atheneum. 1968.
[7] Brandeis, Louis and Warren, Samuel, "The Right to Privacy," Harvard Law Review (1890)

- **Confidentiality** is preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. This definition is the same definition as the security objective Confidentiality in NIST SP 800-53 Revision 4. Confidentiality reflects the overlap between privacy and security in keeping data secure and protecting against unauthorized intrusions.

These privacy engineering objectives are not intended to define the use of specific controls or the role of actors within the system. For example, the Manageability objective requires that a system be capable of enabling authorized modification of personal information, but policy and use of a risk model should define who can make those modifications (e.g. end user individuals or administrators) and which specific control mechanisms should be deployed.

Proposed Privacy Risk Model

The risk management model in the discussion deck is focused on the privacy impact on individuals whose information is collected, used, stored, and transmitted by information systems, and how organizations can prevent adverse impact on those individuals. It provides a method for determining the allocation of resources and making informed choices about privacy in systems. The model is intended to help organizations identify where controls can be most effectively implemented and facilitate proactive steps to mitigating privacy risks.

At the April Workshop, the limits of the analogy between privacy and cybersecurity was a key topic. Of particular interest was whether or not the terminology of security "threats" and "vulnerabilities" would be appropriate for assessing privacy risk. A key distinction between privacy and security is that the functions of a system can be operating normally and still result in privacy harms to individuals, while security failures are often described as when a system has operated or been forced to operate in an abnormal manner. This departure from security calls for a different vocabulary to express privacy risk.

Another important consideration for a privacy risk model is that privacy harms may occur far outside of the system. The discussion deck illustrates how privacy harm may arise from data actions a system performs in ways that are problematic, or that contravene the privacy engineering objectives**.** Participants at the April Workshop discussed privacy harms derived from Daniel Solove's "Taxonomy of Privacy" and concerns with his classification.[8] Based on this discussion, NIST arrived at the concept of problematic data actions that diverges from Solove's classification by drawing a distinction between actions that create the opportunity for harm, and actual harms that individuals experience. This conceptual distinction enables the risk model to focus on problematic data actions as an aspect of the system that developers and designers can identify and mitigate, rather than the identification of specific harms to individuals.[9]

Finally, the privacy risk model takes context into consideration. Context is often discussed as a key privacy concern in so far as the processing of personal information in one setting can be acceptable, but

[8] Solove, Daniel J., "A Taxonomy of Privacy". University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006; GWU Law School Public Law Research Paper No. 129. Available at SSRN: http://ssrn.com/abstract=667622

[9] Harms from security breaches are generally well understood. In privacy, consensus is still being developed around what constitutes harms. However, if the privacy engineering objectives are intended to mitigate the risk of privacy harms, then the underlying harms need to be explicated in order to assess the utility of the objectives. The discussion deck includes a proposed list of privacy harms.

may be problematic in another setting.[10] Context and the types of personal information used and/or generated serve as the primary modifiers that can identify the threshold in a given system where a normal data action becomes "problematic." The discussion deck proposes a set of illustrative contextual factors to assist organizations in assessing privacy risk.[11]

Next Steps

NIST will use the following questions to facilitate discussion at the September workshop. Written comments are also welcome and may be submitted to **privacyeng@nist.gov** **until September 30, 2014**. Output from the September workshop and written comments will support the development of a draft NIST Interagency Report (NISTIR) to be released for public comment.

- **Questions specific to the Discussion Deck:**
  - Privacy Engineering (slide 4): Is this definition helpful?
  - Privacy Engineering Objectives (slides 8-10): Are these objectives actionable for organizations? Are there any gaps?
  - System Privacy Risk Model (slide 13): Is it constructive to focus on mitigating problematic data actions?
  - System Privacy Risk Equation (slide 14): Does this equation seem likely to be effective in identifying system privacy risks? If not, how should system privacy risk be identified?
  - Context (slide 16): Are these the right factors? Are there others?
  - Problematic Data Actions (slides 18-24): Are these actions functional? Are there additional ones that should be included?
  - Harms (slides 26-29): Are these harms relevant? Are there additional ones that should be included?

[10] For a foundational discussion of the importance of context to privacy, see Nissenbaum, Helen, Privacy as Contextual Integrity. Washington Law Review, Vol. 79, No. 1, 2004. Available at SSRN: http://ssrn.com/abstract=534622

[11] The definition of context and the illustrative factors have been derived from the White House's "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting innovation in the Global Digital Economy" (February 2012). Available online at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf