ITL BULLETIN FOR APRIL 2017

BUILDING THE BRIDGE BETWEEN PRIVACY AND CYBERSECURITY FOR FEDERAL SYSTEMS

Naomi Lefkovitz, Ellen Nadeau, Larry Feldman,[1] and Greg Witte,[1] Editors
Applied Cybersecurity Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

Because information technology (IT) deeply affects privacy at individual and societal levels, systems should be built in a trustworthy manner, consistent with widely recognized, high-level privacy principles — such as the Fair Information Practice Principles (FIPPs). The National Institute of Standards and Technology (NIST) regularly conducts research into technology, aiming to improve innovation and competitiveness, thereby advancing U.S. national and economic security and quality of life. Much of NIST's previous guidance into the trustworthiness of systems in various technical areas— including cybersecurity, cloud computing, big data, and cyber-physical systems— has focused on the security objectives of confidentiality, integrity, and availability (CIA). While unauthorized access to personally identifiable information (PII) is a subset of information security and a critical aspect of privacy, there is a less-developed understanding of other ways in which a system impacts individuals' privacy and how to identify and address risks that extend beyond unauthorized access. Thus, there is a need to bridge cybersecurity and privacy as two different attributes of trustworthiness.

NIST's Information Technology Laboratory has developed a new Internal Report (NISTIR) 8062, Introduction to Privacy Engineering and Risk Management in Federal Systems, building on several years' collaboration with public and private sector partners – including two public workshops and a webinar. While all organizations benefit from effective privacy engineering, NISTIR 8062 will be particularly helpful for U.S. federal agencies. Federal privacy protections have been in place for more than four decades, and the need to protect individuals' privacy remains as critical today as ever. The U.S. Office of Management and Budget's recent update to Circular No. A-130 includes a new emphasis on managing privacy risk, so federal agencies will need guidance on repeatable and measurable approaches to bridge the gap between privacy principles and effective implementation. To that end, NISTIR 8062 will:

- Lay the groundwork for future guidance on how federal agencies will be able to incorporate privacy as an attribute of trustworthy systems through the management of privacy as a collaborative, interdisciplinary engineering practice;

[1] Larry Feldman and Greg Witte are Guest Researchers from G2, Inc.

- Introduce a set of objectives for *privacy engineering* and a new model for assessing privacy risks in federal systems; and

- Provide a roadmap for evolving these preliminary concepts into actionable guidance, complementary to existing NIST guidance for information security risk management, so that agencies may more effectively meet their obligations under Circular A-130 and other relevant policies.

NISTIR 8062 is an introductory report intended to foster further discussion. To better support the operational needs of agency privacy programs, and to help develop guidance that is comprehensive enough to promote compliance with policy directives, NIST will continue to collaborate with the privacy community through open processes.

An Engineering Approach to Privacy

A significant body of work already addresses security in federal systems. Recently, the term "privacy" has begun to be added to these security documents. This addition implies that privacy shares enough characteristics with security that the guidance should be applicable to address privacy. However, even the fact that "privacy" is used as a separate term confirms that privacy has a separate meaning and brings with it issues distinct from security. That is why it is important to understand the relationship—particularly the distinctions—between information security and privacy. Doing so will improve understanding of how to apply established systems engineering and risk management processes to address privacy concerns.

As noted in Circular A-130: "Federal information is a strategic asset subject to risks that must be managed to minimize harm. Protecting an individual's privacy is of utmost importance. The Federal Government shall consider and protect an individual's privacy throughout the information life cycle. While security and privacy are independent and separate disciplines, they are closely related, and it is essential for agencies to take a coordinated approach to identifying and managing security and privacy risks and complying with applicable requirements." At the same time, throughout the Circular, there is clear recognition that privacy and security needs require separate leadership with unique skills, and that a coordinated approach does not necessarily mean an identical approach.

Public discourse on the relationship between security and privacy often includes colloquial phrases such as "Security and privacy are two sides of a coin." and "There is no privacy without security." Clearly, confidentiality of PII plays an important role in the protection of privacy. However, there are security issues unrelated to privacy (e.g., confidentiality of trade secrets), just as there are privacy issues unrelated to security. For example, some communities have responded negatively to smart meters due largely to concern that the information being collected can reveal behavior inside a person's home, and less so from concerns that the utilities cannot keep the information secure. Even actions taken to

protect PII can have privacy implications. For example, security tools, such as persistent activity monitoring, can create concerns about the degree to which that monitoring reveals information about individuals that is unrelated to cybersecurity purposes.

These cases illustrate that systems designed to achieve beneficial objectives (e.g., improved efficiency of the electrical grid and increased security) can adversely affect individuals' privacy as an unintended consequence or byproduct of the system as it is *collecting and using* information about individuals.

This byproduct risk model is conceptually distinct from the security risk model. In the security risk model, concerns focus on unauthorized activity that causes a loss of confidentiality, integrity, or availability of information or systems. In the byproduct risk model, the processing of PII is planned and permissible (i.e., authorized), but it creates implications for individuals' privacy. So, while some privacy concerns arise from unauthorized activity, privacy concerns also can arise from authorized processing of information about individuals.

Figure 1, below, shows a non-proportional representation of the relationship between the privacy and security domains.

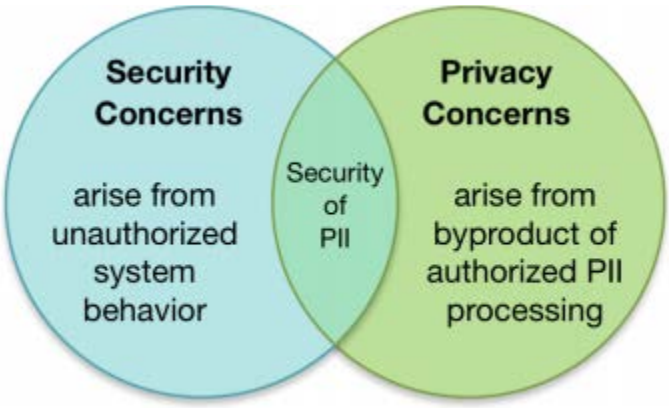

Figure 1. Relationship between Information Security and Privacy

Recognizing the boundaries and overlap between privacy and security is key to determining when existing security risk models and security-focused guidance may be applied to address privacy concerns — and where there are gaps that need to be filled to achieve an engineering approach to privacy. For instance, existing information security guidance does not address the consequences of a poor consent mechanism for use of PII, the purpose of transparency, what PII is being collected, or which changes in use of PII are permitted so long as authorized personnel are conducting the activity. Given these material distinctions in the disciplines, it should be clear that agencies will not be able to effectively manage privacy solely on the basis of managing security.

Privacy Engineering in Federal Systems

In information security, the security objectives also known as the CIA triad — confidentiality, integrity, and availability — have been used as a means of categorizing capabilities and controls to achieve security outcomes. Similarly, privacy engineering objectives could enable system designers or engineers to focus on the types of capabilities needed to demonstrate that the system meets system privacy requirements and fulfills agency privacy policies. NISTIR 8062 presents three privacy engineering objectives for this purpose:

- Predictability — enabling reliable assumptions by individuals, owners, and operators about PII and its processing by an information system;
- Manageability — providing the capability for granular administration of PII including alteration, deletion, and selective disclosure; and
- Disassociability — enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system.

These privacy engineering objectives are intended to supplement, not replace, the FIPPs.

The NISTIR describes common risk terminology from NIST guidance and adapts this terminology to provide a new privacy risk model as a first step towards developing guidance for privacy risk assessment. In information security, the risk factors include the threats to the system and the vulnerabilities that can be exploited by those threats. However, the terms “threat” and “vulnerability” fail to capture the essence of many privacy problems for individuals. Returning to the example of the smart meters, the smart meters are the part of the system collecting the information and thereby creating the problems for individuals (e.g., loss of trust; chilling effect on ordinary behavior). An information security risk model would be unlikely to perceive this behavior of the smart meter as a “threat” since the activity is an authorized part of the functioning of the system itself. While it is not inconceivable to expand a threat-based model to apply to the purposeful processing of PII, overloading this term runs the risk of causing more confusion and miscommunication than clarity, and ultimately creating more difficulties in determining meaningful privacy risk assessments and appropriate mitigations.

Therefore, rather than adding more concepts to the term “threat,” a more information-rich factor for a privacy risk model is to identify the operation that a system is performing on PII, that could cause an adverse effect or a problem for individuals — in short, a *problematic data action*.

Roadmap for Federal Guidance for Privacy Engineering and Risk Management

As described above, the purpose of NISTIR 8062 is to introduce how systems engineering and risk management could be used to develop more trustworthy systems that include privacy as an integral

attribute. However, an introduction is insufficient to provide the detailed guidance federal agencies will need to incorporate these processes into their privacy programs and to meet their responsibilities under OMB Circular A-130.

NIST already has developed extensive guidance for federal agencies on information security risk management, including the establishment of the Risk Management Framework (RMF). With respect to privacy programs, this guidance is appropriate for addressing risks to individuals arising from unauthorized access to their information. As NISTIR 8062 notes, however, such guidance is not as well-suited for addressing risk that may arise from the authorized processing of PII. Collaborating through open processes, NIST intends to expand its guidance to enable agencies to apply the privacy risk model and the privacy engineering objectives to existing engineering and risk management practices. The goal of this expanded guidance is to enable greater consistency in achieving privacy-positive outcomes for their systems. In addition, this expanded guidance will help agencies to better integrate the NIST RMF into agencies' privacy programs.

NIST will continue to collaborate with agencies to identify additional work products that can help understand and define the roles, tasks, and technical processes in privacy engineering and risk management. This guidance should shed light on how privacy engineering objectives and a privacy risk model can complement the FIPPs and the use of Privacy Impact Assessments (PIAs) to continually improve privacy programs. Over time, NIST anticipates that agencies will have a complete set of tools to enable privacy to achieve parity with other considerations in agencies' enterprise risk management processes.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov