INFORMATION TECHNOLOGY LABORATORY

National Institute of Standards and Technology

Information Technology Laboratory

Cybersecurity and Privacy for the Internet of Things

Program Overview

James A. St. Pierre
Deputy Director, ITL

June 2017

The Internet of Things (IoT)

- The IoT has the potential for enormous societal benefits

  in health, safety, energy, security, productivity, environment …

- There is no widely accepted definition of IoT – Gartner states: *"IoT is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment"*

NIST Information Technology Lab
IOT Research

NIST Information Technology Laboratory has extensive expertise related to IoT

Examples of research areas include:

- ***Security and Privacy***
- ***Networking***
- ***Data Analytics***
- ***Timing***

Our "Cybersecurity for IoT" Program builds on the decades of cybersecurity research and experience on the technological underpinnings of the IoT

Image source: http://techliquids.com/the-importance-of-digital-trust-amidst-decreasing-loyalty/

INFORMATION TECHNOLOGY LABORATORY

ITL Cybersecurity for IOT Program

- Program purpose
  - Cultivate trust in IoT through:
    - Definitions, guidance, and best practice documentation
    - Research, producing IoT reference data and enabling software tools
    - Coordination of standards within and across sectors in the digital economy;
- Stakeholders
  - Government
  - Industry
  - Academia
  - Standards Development Organizations
  - (International Focus)

NIST IoT Cybersecurity and Privacy Activities

Existing IoT security-related efforts at NIST

- **IoT-Specific**
  - Lightweight Encryption
  - Network of Things
  - Vehicle-to-vehicle transportation
  - Cybersecurity for Smart Grid Systems
  - Cybersecurity for Cyber Physical Systems
  - BLE Bluetooth
- **Directly Supporting IoT**
  - Wireless Medical Infusion Pumps
  - RFID Security Guidelines
  - Guide to Industrial Control Systems (ICS) Security
  - Security for Time
  - Supply Chain Risk Management
  - Blockchain
  - Hardware Roots of Trust
  - Galois IoT authentication & PDS Pilot
  - Cloud security
- **Indirectly Supporting IoT**
  - Cybersecurity Framework
  - CSF Profile for Manufacturing
  - National Vulnerability Database
  - Security of Interactive and Automated Access Management Using Secure Shell (SSH)
  - Digital Identity Guidelines
  - Security Content Automation Protocol (SCAP) Standards and Guidelines
  - Software Assessment Management Standards and Guidelines
  - Cyber Threat Information Sharing
  - Privacy Engineering and Risk Management

IoT security-specific work

Status	Effort	Additional Comments
Document	Lightweight Encryption (NIST IR 8114)	Need to identify the classes of IoT devices that can't do full-strength crypto.
Document	Network of Things (NIST SP 800-183)	Provides a model and terminology for describing IoTs. Opportunity to map the model to lower-level architectures and designs.
In Progress	Vehicle-to-vehicle transportation	Participating in international standard development for vehicle cybersecurity, consulting domestically on automotive security, and developing CSF profile for transportation.
Document	Cybersecurity for Smart Grid Systems (NIST IR 7628 Rev 1)	Possible explosive growth in numbers of sensors and actuators, with security requirements. Opportunity to map to IoT models (like SP 800-183)
Document	Cybersecurity for Cyber Physical Systems (framework document)	Opportunity to map to IoT models (like SP 800-183)
Document	BLE Bluetooth (SP 800-121)	Protecting IoT communication.

Directly supporting IoT security

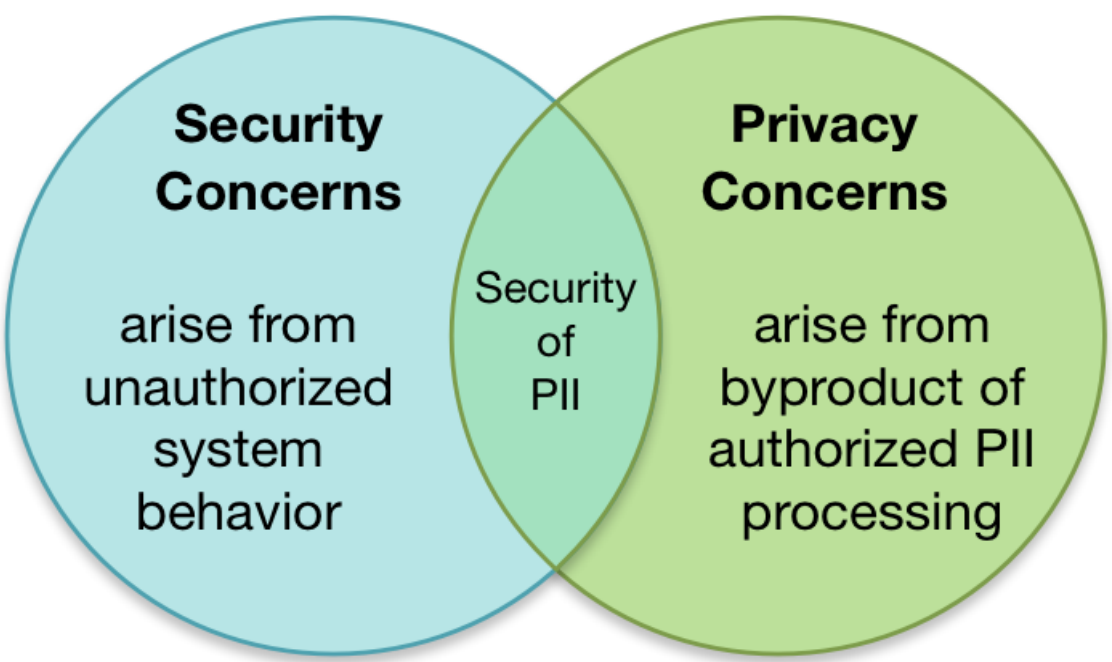
Status	Effort	Additional Comments
In Progress	NCCoE - Wireless Medical Infusion Pumps	Working with industry partners to develop implementation guidance for wireless medical infusion pumps use case (http://nccoe.nist.gov/projects/use_cases/medical_devices).
Document	RFID Security Guidelines (NIST SP 800-98)	Information disclosure issue; impoverished version of an IoT
Document	Guide to Industrial Control Systems (ICS) Security (NIST SP 800-82)	Overlay for 800-53 for control system environments, taking into account their specialized challenges.
Document	Supply Chain Risk Management (NIST SP 800-161)	Supply chain risk management practices
In Progress	Blockchain	How do fundamental blockchain features and resource requirements relate to IoT? (e.g. “proof of work”)
Document	Hardware Roots of Trust (NIST SP 800-147)	Assured boot and state attestation.
In Progress	Galois IoT authentication & PDS Pilot	Pilot deploying strong authentication for IoT-connected smart building. Enables access to IoT devices and sharing device data across organizational entities.
Document	Cloud security (NIST SP 800-144)	Cloud definition.

Indirectly supporting IoT security and privacy

Status	Effort	Additional Comments
Document, and Web resources	Cybersecurity Framework (nist.gov/cyberframework)	Approach for managing and reducing cybersecurity risk.
Document	CSF Profile for Manufacturing (white paper)	Profile maps manufacturing processes to the cybersecurity framework. Multi-laboratory effort within NIST.
Web	National Vulnerability Database (nvd.nist.gov)	A resource for cataloging IoT vulnerabilities.
Document	Security of Interactive and Automated Access Management Using Secure Shell (SSH) (NIST IR 7966)	Essential utility for management of distributed devices.
Document	Security Systems Engineering (NIST SP 800-160)	Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems
Document	Security Content Automation Protocol (SCAP) Standards and Guidelines (NIST SP 800-126 R2)	Specifications for representing security configuration and vulnerability information.
Document	Software Assessment Management Standards and Guidelines (IR 8060)	Maintain an inventory of installed software (and maybe hardware) for an organization. SWID tag.
Document	Cyber Threat Information Sharing (SP 800-150)	Guidance for organizations generating and/or consuming cyber threat information, data formats
Document	Introduction to Privacy Engineering and Risk Management for Federal	Report introducing concepts for privacy engineering and risk management in systems.

Privacy

Information Security and Privacy: Boundaries and Overlap



11

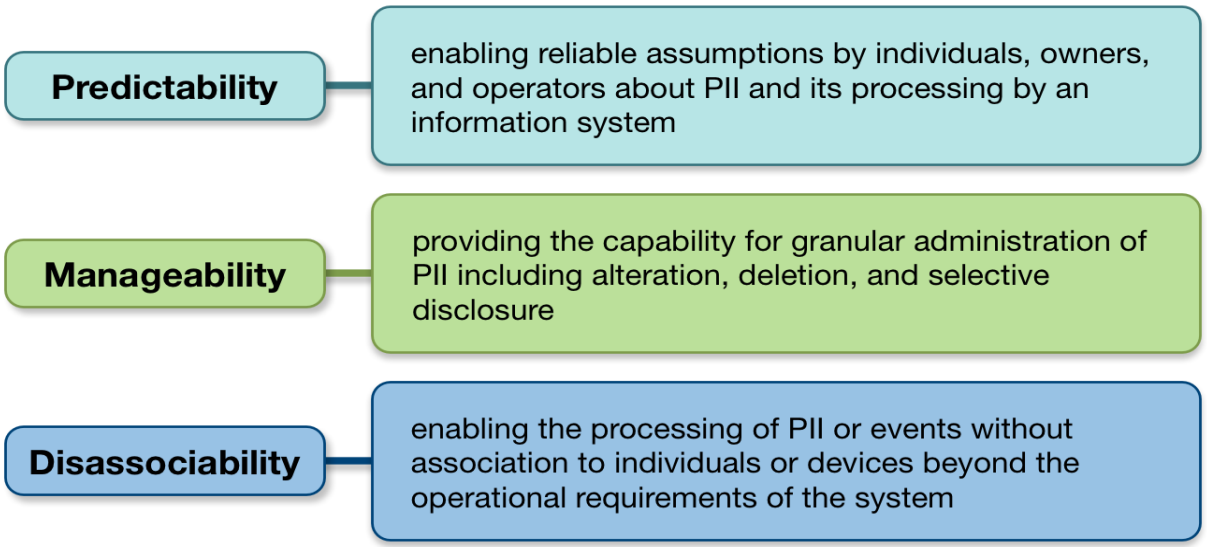
NIST Working Definition of Privacy Engineering

A specialty discipline of systems engineering focused on achieving freedom from conditions that can create problems for individuals with unacceptable consequences that arise from the system as it processes personally identifiable information (PII).

12

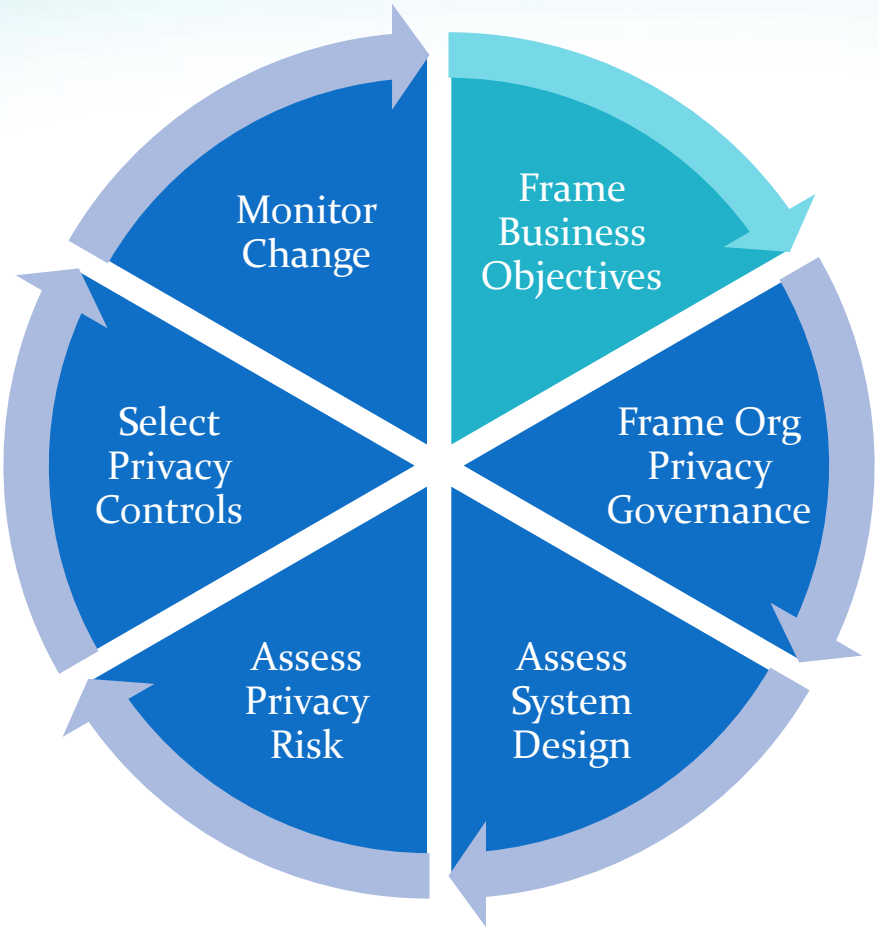
NIST Privacy Engineering Objectives

- Design characteristics or properties of the system
- Support policy through mapping of system capabilities
- Support control mapping



13

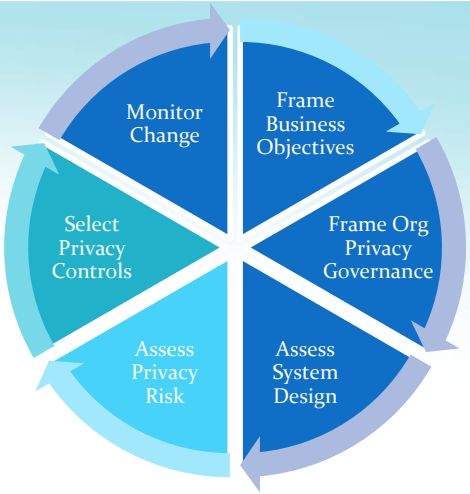
Privacy Risk Assessment Methodology



14

Select Privacy Controls

Data Actions	Potential Problems for Individuals	Potential Controls	Considerations
Collection from the Social Media Site	Stigmatization: Information is revealed about the individual that they would prefer not to disclose.	1. Configure API to enable more granular retrieval of information, pull full name and email only; enable capability to pull profile photograph if future proofing requires it. 2. Inform users of collection. 3. Delete unneeded information after collection.	1. Significantly reduces collection of information, possibly decreasing risk across the system. Would potentially lower risk of stigmatization, power imbalance, and loss of trust problems. 2. Users may be informed of specific information collected in this data action, but that may not improve risk across the system as they are unable to prevent the revelation of information. 3. Unclear how users will understand the process. Leverages appropriate disposal controls. Decreases risk of stigmatization, but not necessarily power imbalance or loss of trust. Compare potential failure rate for API
	Power Imbalance: People must provide extensive information, giving the acquirer an unfair advantage.		
	Loss of Trust: Individuals lose trust in ACME due to a breach in expectations about the handling of personal information.		



Data Actions	Potential Problems for Individuals	Selected Controls	Rationale	Residual Risks
Collection from the Social Media Site	Stigmatization: Information is revealed about the individual that they would prefer not to disclose.	1. Change API call to only pull full name and email; consider change to pull profile photograph if future proofing requires it. 2. Inform users of information that is collected and why at time of collection.	1. Significantly reduces collection of information, possibly decreasing risk across the system. Would potentially lower risk of stigmatization, power imbalance, and loss of trust problems. 2. Meets transparency requirement. Easy to implement.	
	Power Imbalance: People must provide extensive information, giving the acquirer an unfair advantage.			
	Loss of Trust: Individuals lose trust in ACME due to a breach in expectations about the handling of personal information.			

15

Resources

Jim St.Pierre – jimstp@nist.gov

NIST Cybersecurity for IOT website:
https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

NIST Privacy Engineering Website:
https://www.nist.gov/programs-projects/privacy-engineering

NIST-IR 8062 "An Introduction to Privacy Engineering and Risk Management in Federal Systems "
https://doi.org/10.6028/NIST.IR.8062

16