Privacy Risk Analysis Based on System Control Structures

Adapting System-Theoretic Process Analysis

(STPA) for Privacy Engineering

Julie Snyder

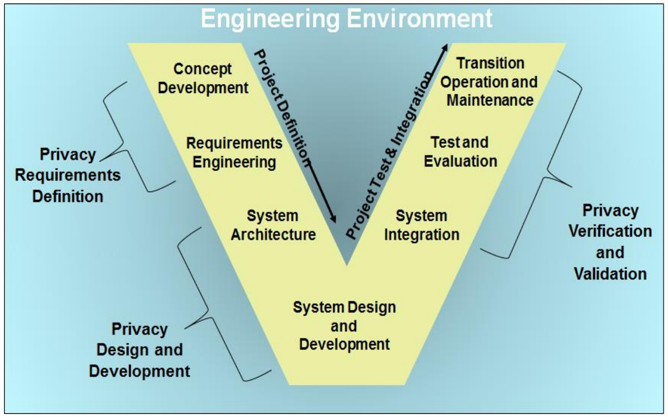
May 26, 2016

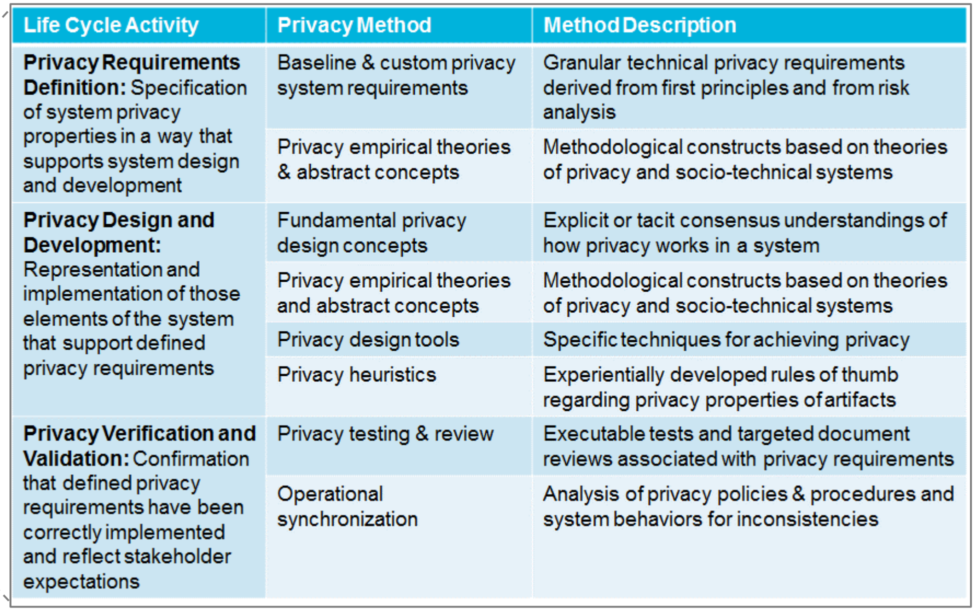
MITRE

Approved for Public Release; Distribution Unlimited. Case Numbers 14-2545, 16-0355 and 16-0887

Privacy Engineering Spans the Systems Engineering Life Cycle

- **A full spectrum of methods is needed**


Engineering Environment
Concept Development
Requirements Engineering
System Architecture
System Design and Development
System Integration
Test and Evaluation
Transition Operation and Maintenance
Project Definition
Project Test & Integration
Privacy Requirements Definition
Privacy Design and Development
Privacy Verification and Validation



Life Cycle Activity	Privacy Method	Method Description
Privacy Requirements Definition: Specification of system privacy properties in a way that supports system design and development	Baseline & custom privacy system requirements	Granular technical privacy requirements derived from first principles and from risk analysis
	Privacy empirical theories & abstract concepts	Methodological constructs based on theories of privacy and socio-technical systems
Privacy Design and Development: Representation and implementation of those elements of the system that support defined privacy requirements	Fundamental privacy design concepts	Explicit or tacit consensus understandings of how privacy works in a system
	Privacy empirical theories and abstract concepts	Methodological constructs based on theories of privacy and socio-technical systems
	Privacy design tools	Specific techniques for achieving privacy
	Privacy heuristics	Experientially developed rules of thumb regarding privacy properties of artifacts
Privacy Verification and Validation: Confirmation that defined privacy requirements have been correctly implemented and reflect stakeholder expectations	Privacy testing & review	Executable tests and targeted document reviews associated with privacy requirements
	Operational synchronization	Analysis of privacy policies & procedures and system behaviors for inconsistencies

- **STPA-Priv is one specific method for one specific task: privacy risk analysis**

The Nature of Privacy Risk Management

- **Multiple risk models (as opposed to security)**
  - Fair Information Practice Principles
  - Calo’s dichotomy
  - Solove’s taxonomy
  - LINDDUN (also method)
  - Contextual integrity
  - NIST Privacy Risk Management Framework
- **Current praxis is dominated by programmatic approaches**
  - FIPPs and PIA
- **The problem with probabilistic approaches…**

Dealing with Quality Attributes of Complex Socio-Technical Systems

- **Complexity and tight coupling (Perrow)**
- **Emergent properties**
  - Unforeseen interactions
- **Human cognitive limitations**
- **Accident impact breadth and depth**

- **A safety engineering response that leverages systems theory**
  - System-Theoretic Accident Model and Processes (STAMP)
  - System-Theoretic Process Analysis (STPA)
  - Has been shown to
    - Identify the same hazards as traditional techniques plus others those techniques missed
    - Operate more efficiently than traditional techniques

STAMP

- **Frames safety in terms of constraints on system behavior rather than prevention of events and event chains**
- **Constraints are enforced by controls**
  - Hierarchical
  - Closed loop (adaptive feedback)
  - Development vs. operations
- **Controls employ process models**
- **Accidents occur when the controller process model diverges from the process being controlled, resulting in**
  - Incorrect control action
  - Missing control action
  - Control action applied at the wrong time
  - Incorrect duration of control action

STPA-Sec

- **Variant of STPA aimed at cyber security**

1. **Identify losses to be considered**
   - C-I-A
2. **Identify system vulnerabilities that can lead to losses**
   - Anti-goals
3. **Specify system functional control structure**
   - Constraints derived from vulnerabilities
4. **Identify insecure control actions**
   - Potential insecure control actions by constraint and insecure control action type
   - Causal scenarios for insecure control actions

Modifying STPA-Sec for Privacy (1/2)

- **“Loss” is a less generally useful term in the context of privacy risk than in the context of safety and security risk**
  - STPA-Priv refers to “adverse consequences” rather than “losses”
- **Adverse consequences are dependent on the risk model**
  - Explicitly force choice of defined privacy risk model for determining adverse consequences
    - STPA-Priv refers to privacy “frameworks” for the sake of familiarity and in recognition of the incompleteness of most privacy risk models
- **Some privacy controls can be open-loop controls**
  - E.g., privacy policy + implicit consent

Modifying STPA-Sec for Privacy (2/2)

1. **Identify potential adverse privacy consequences to be considered, as denoted by a selected framework**
2. **Identify vulnerabilities that can lead to adverse privacy consequences in the context of the system**
3. **Specify system privacy constraints and functional control structure, including open-loop privacy controls**
4. **Identify privacy-compromising control actions**

Smart TV Example

- **Based on an actual smart TV**
- **Feature enables TV to recognize on-screen content**
- **Enabled by default**
- **Collects “viewing data” from TVs located within the U.S. related to publicly available content**
  - Service provider
  - Date and time
  - Programs and commercials viewed
- **Viewing data are claimed to be anonymous and are combined with IP address and demographic information obtained from third parties to deliver ads to known devices that share the TV’s IP address**
- **Aggregate data are shared with media and data analytics companies**

1. Identify potential adverse privacy consequences to be considered, as denoted by a selected framework

- **Calo's subjective/objective privacy harms**
  - Subjective privacy harm: Perception of unwanted surveillance
  - Objective privacy harm: Forced or unanticipated use of personal (i.e., specifically related to a person) information

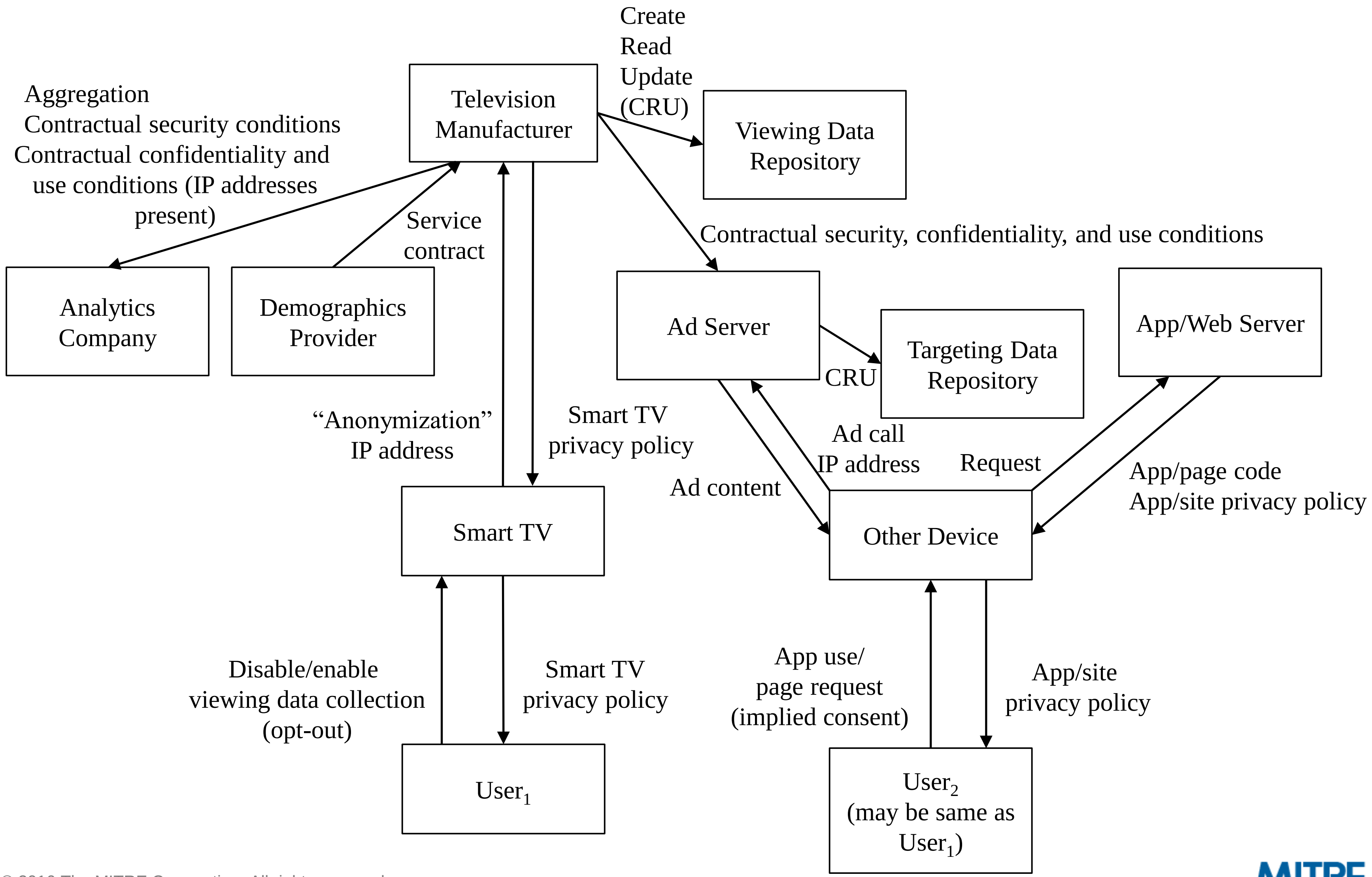
2. Identify vulnerabilities that can lead to adverse privacy consequences in the context of the system

- **User of device associated with the same IP address as the television may perceive unwanted surveillance based on the ads delivered, even if not responsible for program choices.**
- **User does not realize prior to use how viewing data are being collected, retained, combined with other information, and used to serve ads and for other analytics.**
- **User wants to opt out of collection of viewing data but cannot determine how to disable collection.**

3. Specify system privacy constraints and functional control structure, including open-loop privacy controls (1/2)

- **User of device associated with the same IP address as the television must not perceive unwanted surveillance based on the ads delivered.**
- **User must understand what and how data are being collected and used and actual practices must be consistent with that understanding.**
- **User must be able to determine how to disable collection of viewing data and to carry out those instructions.**

3. Specify system privacy constraints and functional control structure, including open-loop privacy controls (2/2)


Television Manufacturer
Create
Read
Update
(CRU)
Viewing Data Repository
Aggregation
Contractual security conditions
Contractual confidentiality and use conditions (IP addresses present)
Service contract
Analytics Company
Demographics Provider
Contractual security, confidentiality, and use conditions
Ad Server
CRU
Targeting Data Repository
App/Web Server
"Anonymization" IP address
Smart TV privacy policy
Ad call
IP address
Request
Ad content
App/page code
App/site privacy policy
Smart TV
Other Device
Disable/enable viewing data collection (opt-out)
Smart TV privacy policy
App use/ page request (implied consent)
App/site privacy policy
User$_1$
User$_2$ (may be same as User$_1$)

MITRE

4. Identify privacy-compromising control actions (1/2)

Privacy Constraint	Incorrect control action	Control action not provided	Control action provided too soon or too late	Control action applied too long or not long enough
User of device associated with the same IP address as the television must not perceive unwanted surveillance based on the ads delivered.	Transmission of viewing data from TV outside the U.S. enabled	Privacy information not provided to user in the context of the device User is not empowered to disable collection of viewing data		
User must understand what and how data are being collected and used and actual practices must be consistent with that understanding.	Transmission of viewing data from TV outside the U.S. enabled Privacy information unclear Micro-level data can be inferred from aggregate data Micro-level data can be associated with identifying information	Privacy information not read Data are not deleted or are deleted inconsistently from the viewing and targeting data repositories	Privacy information not communicated prior to TV use	
User must be able to determine how to disable collection of viewing data and to carry out those instructions.	Instructions and/or control for disabling collection of viewing data not readily accessible	User is not empowered to disable collection of viewing data		

4. Identify privacy-compromising control actions (2/2)

Problematic Control Action	Causal Scenarios
Transmission of viewing data from TV outside the U.S. enabled	VPN use results in TV outside the U.S. being associated with a U.S. IP address
Privacy information not provided to user in the context of the device	User of device has not reviewed privacy policy on TV and experiences ads that appear to reflect viewing habits
User is not empowered to disable collection of viewing data	User makes use of the TV but does not have the authority to disable collection of viewing data due to their position or role (e.g., a child or visitor in a home)
Privacy information unclear	Privacy policy provides information that is too general or too detailed to understand Privacy policy is poorly written for a general reader
Micro-level data can be inferred from aggregate data	Data are aggregated in such a way as to enable data associated with specific smart TVs to be recovered by analytics firms
Micro-level data can be associated with identifying information	As multiple sets of “anonymous” data are combined, it becomes possible to link data to specific individuals or households via quasi-identifiers
Privacy information not read	User ignores privacy policy when presented
Data are not deleted or are deleted inconsistently from the viewing and targeting data repositories	No explicit retention policy exists for data in the viewing and targeting data repositories; retention policy is implicit based on how information categories are defined in the privacy policy
Privacy information not communicated prior to TV use	Privacy policy is not presented to all individual users upon initial use
Instructions and/or control for disabling collection of viewing data not readily accessible	User can’t find or can’t remember where to find instructions and/or control for disabling collection of viewing data User has difficulty following instructions for disabling collection of viewing data

Conclusion

- **The move toward privacy engineering requires more and better privacy-specific risk analysis methods (among others)**
  - For complex socio-technical systems
  - That don’t rely upon arbitrary quantification
- **STPA-Priv can help address this need by adapting STPA-Sec to accommodate**
  - The variety of privacy risk models
  - The open-loop nature of some privacy controls
- **Further developing this method requires refining the method and road-testing it with real-world projects**

Questions?

Contact information:

Stuart Shapiro
sshapiro@mitre.org
+1-781-271-4676

Julie Snyder
jsnyder@mitre.org
+1-703-983-4104

Additional Material

Characterizing Privacy Engineering Techniques (with examples)

	Analytical	Instrumental
Programmatic	Privacy Impact Assessment	FIPPs
Technical	CNIL Methodology for Privacy Risk Management	Secure Multi-Party Computation