From STPA*-Sec to STPA-Priv: Leveraging STPA for Privacy Engineering

Stuart Shapiro

Principal Cyber Security and Privacy Engineer

The MITRE Corporation

March 23, 2016

*System-Theoretic Process Analysis

MITRE

Overview

- The Move Toward Privacy Engineering
- The Nature of Privacy Risk Management
- Privacy Controls versus Security Controls
- Framing Privacy in Terms of Constraints
- Modifying STPA-Sec for Privacy

The Move Toward Privacy Engineering (1/2)

- **Getting Privacy into Socio-Technical Systems**
  - Privacy impact assessments (PIAs)
    - Description vs. assessment
  - Privacy enhancing technologies (PETs)
    - Architectural vs. point control
  - Privacy by Design (PbD)
    - Principle vs. practice
  - Privacy engineering
    - Conventional vs. privacy-specific techniques

The Move Toward Privacy Engineering (2/2)

- **Some General Techniques for Privacy Engineering**

	Analytical	Instrumental
Programmatic	Data Classification	Systems Engineering Life Cycle
Technical	Failure Mode and Effects Analysis	Data Flow Diagrams

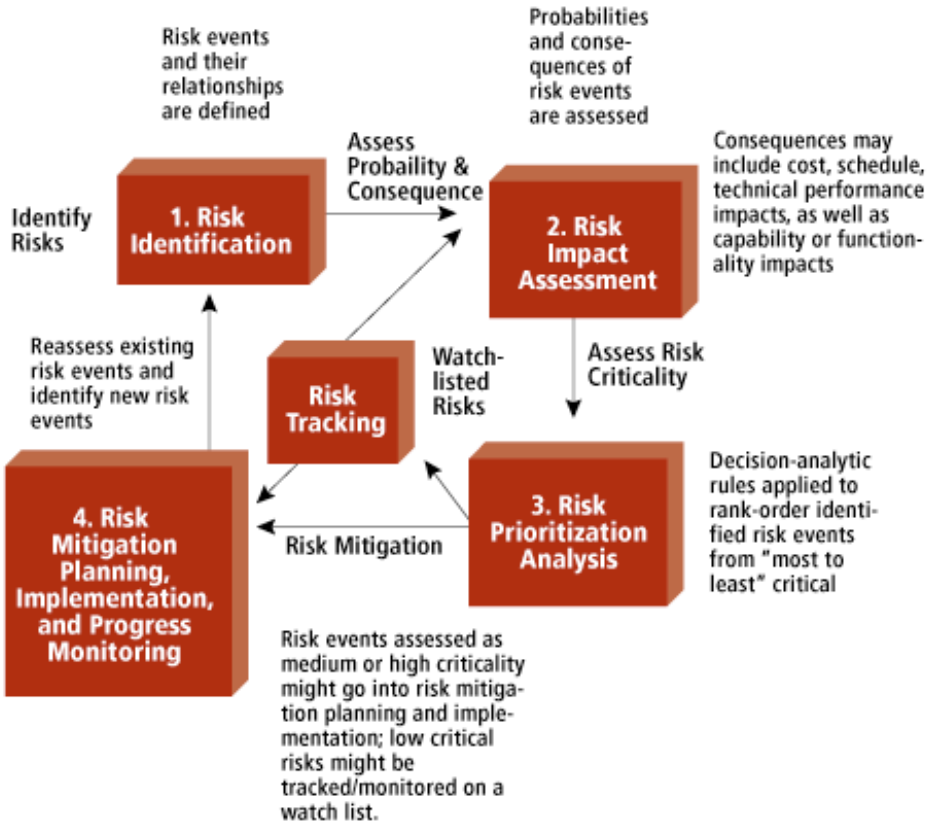
- **Some Privacy Engineering Techniques**

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

MITRE

The Nature of Privacy Risk Management (1/2)

- **Risk management in the systems engineering life cycle**



Garvey, P.R., 2008, *Analytical Methods for Risk Management: A Systems Engineering Perspective,* Chapman-Hall/CRC-Press, Taylor & Francis Group (UK), Boca Raton, London, New York, ISBN: 1584886374.

MITRE

The Nature of Privacy Risk Management (2/2)

- **Risk models: threats, vulnerabilities, consequences**
  - Cyber security: C-I-A
- **Some privacy risk models**
  - Fair Information Practice Principles
  - Calo's dichotomy
  - Solove's taxonomy
  - LINDDUN (also method)
  - Contextual integrity
  - NIST Privacy Risk Management Framework
- **Hybrid models possible**
- **Dominant [problematic] characteristics of current praxis**
  - FIPPs (What)
  - PIA (How)
  - Conducted at (often post-design) SELC milestone (When)
- **The problem with probabilistic approaches**

Privacy Controls vs. Security Controls (1/2)

- **NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations,* long governed U.S. government computer security controls**
- **NIST SP 800-53r4, *Security and Privacy Controls for Federal Information Systems and Organizations,* includes privacy controls**
- **Appendix F, Security Control Catalog**

Access Control	Media Protection
Awareness and Training	Physical and Environmental Protection
Audit and Accountability	Planning
Security Assessment and Authorization	Personnel Security
Configuration Management	Risk Assessment
Contingency Planning	System and Services Acquisition
Identification and Authentication	System and Communications Protection
Incident Response	System and Information Integrity
Maintenance	Program Management

  - The organization vs. the system

Privacy Controls vs. Security Controls (2/2)

- **Appendix J, Privacy Control Catalog**

Authority and Purpose	Accountability, Audit, and Risk Management
Data Quality and Integrity	Data Minimization and Retention
Individual Participation and Redress	Security
Transparency	Use Limitation

  - The organization…
    - Implicates management and operational elements only
- **Must deliberately work to bring in technical elements**

Framing Privacy in Terms of Constraints (1/2)

- **Focus on system writ large sets the stage for bringing in technical control elements**
- **Desired/undesired system behaviors dependent on risk model and context**
  - Implications of model granularity
  - Contrast, for example, FIPPs with Calo's dichotomy

- **Transparency**
- **Individual Participation**
- **Purpose Specification**
- **Data Minimization**
- **Use Limitation**
- **Data Quality and Integrity**
- **Security**
- **Accountability and Auditing**

- **Subjective privacy harm**
  - Perception of unwanted surveillance
- **Objective privacy harm**
  - Forced or unanticipated use of personal information

Framing Privacy in Terms of Constraints (2/2)

- **Consequences**
  - Directly informed by most privacy risk models
  - Goals vs. anti-goals
- **Vulnerabilities**
  - May be covered by the risk model (e.g., contextual integrity), in which case directly situate in terms of the system
  - If risk model does not cover vulnerabilities but does cover consequences, use anti-goals to elucidate vulnerabilities
  - If risk model only covers threats (e.g., CNIL Methodology for Privacy Risk Management)
    - Elucidate consquences to elucidate vulnerabilities?
- **Constraints**
  - May intrinsically conflict with functional requirements
  - Must capture residual risk

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

Summary

- **The move toward privacy engineering requires more privacy-specific technical analytical methods**
- **Privacy risk management needs**
  - More effective risk analysis techniques
    - For complex socio-technical systems
    - That don't rely upon arbitrary quantification
  - More effective integration of the technical elements of risk controls
- **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
- **Paper with example at 2nd International Workshop on Privacy Engineering in May**

Questions?

- **Contact information**

Stuart Shapiro

sshapiro@mitre.org

+1-781-271-4676

MITRE