From Privacy-Enabling Technology to Privacy-Enabled Architecture

Stuart Shapiro

The MITRE Corporation

August 20, 2008

MITRE

Move Toward Comprehensive Risk Management

- PII breaches and breach notification requirements
  - Both private and public sector
    - OMB guidelines on incident handling, including reporting, risk-based assessment, and notification, 2006
    - OMB directive to minimize use of Social Security Numbers and personally identifiable information (PII) generally, 2007
  - Monetary cost
  - Public trust
- Convergence of enterprise information risk
  - Infosec
  - Privacy
  - Intellectual property

From Enhancing to Enabling

- Searches for practical privacy *enhancing* technologies produce tools that are overwhelmingly
  - Intended to be used by individuals, not enterprises
  - Aimed at preventing the collection of PII in the first place
- Enterprises, on the other hand, need to *manage* PII throughout the information life cycle: collection, processing, use, disclosure, retention, destruction
  - Need technologies to support PII-related business processes
- Effective support of PII-related enterprise business processes may or may not require privacy-specific technologies
  - Deployment/configuration of other technologies in ways that support privacy
  - Note sample technologies mentioned in ISE Privacy Guidelines
- Privacy-*enabling* technologies include enterprise-oriented tools and those that are not privacy-specific

From Technologies to Business Processes

- PETs by themselves don't necessarily help if they don't support relevant business processes
- PET and business process categorization enable appropriate mappings
- 70/20/10 heuristic
  - 70% of PII-related enterprise business processes are common across organizations
  - 20% of PII-related enterprise business processes are specific to the *type* of organization
  - 10% of PII-related enterprise business processes are specific to the *individual* organization
  - Specialization may involve additional high-level processes and/or additional sub-processes
  - Concept is more important than the specific numbers

Constructing a Mapping

- Direct
  - PETs to business processes
- Indirect
  - Use cases to business processes
  - PETs to use cases
  - Use cases can identify and thereby target critical business processes
- Sanity check: Do PETs in the same category map to the same business processes or use cases?
  - *Purpose of categorization is to facilitate technology selection and deployment*

Moving Beyond Point Solutions

- Architectures serve as broad templates that carry with them certain desirable properties
  - System
  - Enterprise
- Given that privacy is a desirable property, can we identify/develop architecture(s) that by their nature support privacy?
  - Support PII-related business processes through appropriate use of privacy-enabling technologies
- Privacy-enabled architecture (PEA)
  - Systematic deployment, configuration, and coordination of privacy controls so as to comprehensively address privacy risk
  - Controls should map to business processes as well as risks

Privacy-Enabled Architecture (PEA): Two Approaches

- Technological pointillism
  - Systematic deployment of point solutions so as to provide comprehensive privacy risk management at the system or enterprise level
  - E.g., adaptation of U.S. National Institute of Standards and Technology (NIST) computer security guidance
    - System category > confidentiality/integrity/availability impact levels > control sets
- Technological palette
  - Seamlessly embedding privacy-enabling technologies within system or enterprise design so as to achieve comprehensive privacy risk management
  - Analogy with service-oriented architecture (SOA)
    - Focus on business processes
    - Loose coupling of services and specific technologies
  - E.g., dynamic data desensitization

Conclusion

- Enterprises require PETs that are oriented toward data stewards rather than data subjects
- Relevant commercial tools can act as privacy-*enabling* technologies, even if not explicitly designed or intended to support privacy
- Mapping PETs to business processes, either directly or via use cases, is essential to deployment
- Ultimately, individual PETs are a means to the larger goal of privacy-enabled architecture

Questions

- Half truths
- Quarter truths
- Total evasions

Contact information:

Stuart Shapiro
Principal Information Privacy and Security Engineer
The MITRE Corporation
sshapiro@mitre.org
781-271-4676