Privacy Harm Analysis

Sourya Joyee De

06 April 2016

Talk Plan

1. Background
2. Motivation
3. A Case Study in Smart Grids
4. Main Components of the Analysis
    - Risk sources, privacy weaknesses, feared events, harms
5. From Privacy Weaknesses to Privacy Harms: Harm Trees
6. Risk Assessment based on Harm Trees
    - Input/output likelihoods; Rules for likelihood computation; Example computation of risk
7. Conclusions based on Risk Assessment
8. Summary of Our Contributions
9. Other works

Background

PIA: "a process whereby the potential impacts and implications of proposals that involve potential privacy-invasiveness are surfaced and examined" (Clarke'98)

- At present, Privacy Impact Assessments (PIA) lack in technical details and rigour
  - PIA $=$ PRA $+$ organizational aspects ...
- Lack of agreement on important terminologies and notions
- No detailed end-to-end guidelines to apply PRA for practical scenarios

Article 33 of the EU Regulation mandates data controllers to carry out PIA

Steps of a PIA (by PIAF Consortium) I

1. Determine whether a PIA is necessary
2. Identify the PIA team and set its terms of references, resources, time frame
3. Prepare a PIA plan
4. Agree on a budget for the PIA
5. Describe the proposed project to be assessed
6. Identify stakeholders
7. Analyze information flows and other privacy impacts
8. Consult stakeholders

Steps of a PIA (by PIAF Consortium) II

9. Check that the project complies with legislation
10. Identify risks and possible solutions
11. Formulate recommendations
12. Prepare and publish the PIA report
13. Implement the recommendations
14. Third-party review and audit of the PIA
15. Update the PIA if there is a change in the project
16. Embed privacy awareness throughout the organization and ensure accountability

Our Approach: The Big Picture

- Propose a comprehensive PRA methodology: PRIAM.
  - Components: data, system, stakeholders, risk sources, privacy weaknesses, feared events, privacy harms
  - Attributes and categories of components
  - Linking attributes and categories to determine risk level
- Apply on different use cases
- Propose counter-measures

Motivation

- Energy consumption data may reveal detailed information about consumer's personal life.
- EG2's DPIA template is not clear about assessment of impacts of feared events. It does not provide sufficient idea about impacts specific to smart grid.
- Establishment of link among harms, feared events and privacy weaknesses.
  - *Legal scholars only discuss harms*
  - *Technical works only discuss feared events/ threats/ vulnerabilities*

A Case Study on Smart Grids: System Overview

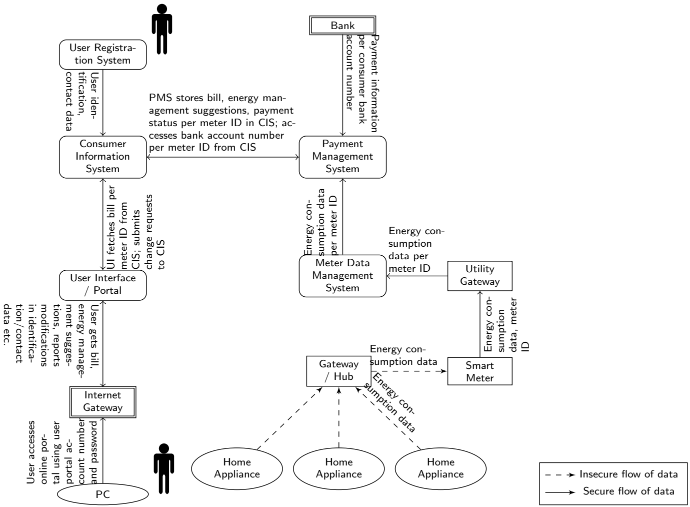

User Registration System
User identification, contact data
Bank
Payment information per consumer bank account number
PMS stores bill, energy management suggestions, payment status per meter ID in CIS; accesses bank account number per meter ID from CIS
Consumer Information System
Payment Management System
UI fetches bill per meter ID from CIS; submits change requests to CIS
Energy consumption data per meter ID
Energy consumption data per meter ID
User Interface / Portal
Meter Data Management System
Utility Gateway
User gets bill, energy management suggestions, reports modifications in identification/contact data etc.
Energy consumption data, meter ID
Energy consumption data
Gateway / Hub
Smart Meter
Energy consumption data
Internet Gateway
User accesses online portal using user portal account number and password
Home Appliance
Home Appliance
Home Appliance
PC
Insecure flow of data
Secure flow of data

Figure: Data flow diagram of a smart grid system

Main Components: Risk Sources

- Any entity (individual or organization) which may process (legally or illegally) data belonging to a data subject and whose actions may directly or indirectly, *intentionally or unintentionally* lead to privacy harms.

- Often referred to as *adversary* or *attacker* in the literature.

- The term "risk sources" is less security connotated and is not limited to malicious actors.

- Examples: MDMS, CIS, PMS administrators, the utility provider, consumers, service technicians, operators or other employees, hackers

Main Components: Privacy Weaknesses

- A weakness in the data protection mechanisms (whether technical, organizational or legal) of a system or lack thereof.
- Can be found out from a description of existing legal, organizational and technical controls
- Must consider privacy weaknesses in the design and in the implementation of the system

Examples

Code	Privacy weaknesses
V.1	Security vulnerability in PMS
V.2	Security vulnerability in MDMS
V.3	Security vulnerability in CIS
V.4	Functional errors in PMS
V.5	Functional errors in MDMS
V.6	Functional errors in CIS
V.7	Unencrypted energy consumption (per meter ID) data processing
V.8	Unencrypted billing related data processing
V.9	Unencrypted consumer identification and contact data processing
V.10	Unencrypted transmission of energy consumption data from home appliance to smart meter
V.11	Non-enforcement of data minimization
V.12	No opt-outs for consumers for high volume/precision data collection
V.13	Not assigning capabilities to consumers to challenge erroneous data about themselves
V.14	Insufficient system audit

Table: Some privacy weaknesses in a smart grid system

Main Components: Feared Events

- An event of the system that occurs as a result of the exploitation of one or more privacy weaknesses and that may lead to privacy harms.
- Intermediate technical event between privacy weaknesses and harms

Examples

Code	Feared events	Relevant scenarios
FE.1	Excessive collection of energy consumption data	Collection of energy consumption data more frequently than billing period without consumer consent
FE.2	Use of energy consumption data for unauthorized purpose	Develop detailed consumer profiles, monitoring and restricting energy usage
FE.3	Data inference from energy consumption data	Inferring about a person's lifestyle or habits from his energy consumption
FE.4	Retaining billing related data more than required	Not deleting energy management suggestions long after consumer stops using utility provider's service, not deleting bills even after 5 years
FE.5	Retaining energy consumption data more than required	Ineffective deletion of energy consumption data from utility gateway
FE.6	Retaining contact and identification data more than required	Not deleting e-mail address, DoB even after consumer stops using utility provider's service
FE.7	Unauthorized access to identification / contact data	Hacker gets access to identification / contact data
FE.8	Unauthorized access to billing related data	One consumer gets access to another's billing data
FE.9	Unauthorized access to energy consumption data	Service technician gets access to energy consumption data
FE.10	Use of identification / contact data for unauthorized purposes	Targeted advertising

Table: Feared events in a smart grid system

Main Components: Privacy Harms

- The negative impact on a data subject, or a group of data subjects, or the society as a whole, from the standpoint of physical, mental, or financial well-being or reputation, dignity, freedom, acceptance in society, self-actualization, domestic life, freedom of expression, or any fundamental right, resulting from one or more feared events.
- Useful inputs to establish a list of harms are:
  - previous privacy breaches, case law, recommendations, points of view of stakeholders

Examples

Harms	Information revealed by smart meters	Pattern	Granularity
Burglary, profile based discrimination	When are you usually away from home?	High/ low power usage during the day	Hour/ minute
Burglary	Have you been away from home for some time?	High/ low power usage during the day	Day/ hour
Kidnapping, stalking, child abuse	Do you leave a child alone at home? How often and how long?	Single person power usage or simultaneous power usage at distinct areas of the house during the day	Minute/ second
Burglary, kidnapping, stalking, profile based discrimination	Is your home protected by an electronic alarm system?	Appliance activity matching alarm system signature	Minute/ second
Profile based discrimination, Burglary	Do you own a lot of expensive gadgets?	Appliance activity matching signature of expensive gadgets	Minute/ second
Consumer profiling	Did you watch the game last night?	Appliance activity matching the game showtime	Hour/ minute
Burglary, stalking	Are you living alone at home right now?	Single person power usage or simultaneous power usage at distinct areas of the house during the day	Day/ hour
Profile based discrimination	Do you stay at home all day watching TV or in front of the computer?	Appliance activity matching signature of TV, computer	Hour/ minute
Profile based discrimination, targeted advertising	Do you cook often or prefer to eat outside?	High/ low power events around meal times for microwave, cook tops etc.	Hour/ minute

Table: Information Revealed by Smart Meters

Types of Privacy Harms in Smart Grids

- *Financial harms*: Burglars come to know when the occupants are not at home or if the home security system is inactive or not installed inferred from energy consumption data.
- *Psychological harms*: A potential employer may decline a job offer to a consumer because of alleged unhealthy lifestyle inferred from his energy consumption data.
- *Harms to reputation or dignity*: Exposure of a consumer's lifestyle may cause him embarrassment.
- *Social harms*: Remote switching off of energy supply during periods of high demand may deprive consumers of utilities essential for leading a normal life.

Attributes of Privacy Harms

1. *Victims of harms*
   - individual consumers or their family members (e.g., burglary);
   - specific section of consumers based on age (e.g., targeted advertising), gender (e.g., stalking of females), religion, ethnicity, profession, industry etc.;
   - society (e.g., government surveillance).
2. *Intensity*: a composite representation of the significance of the impact on the victims.
   - duration of the harm (from short time to irreversible),
   - extent of the damage, etc.

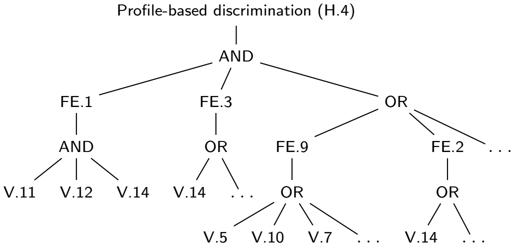
These attributes are used to compute severity of harms.

Examples

Code	Harm	Types	Victims
H.1	Kidnapping of a child	Psychological, financial	Age group
H.2	Burglary	Financial, psychological	Consumer, family
H.3	Restriction of energy usage	Psychological	Society
H.4	Profile-based discrimination	Psychological, financial	Consumers, family

Table: Examples of harms and their attribute values in a smart grid system

From Privacy Weaknesses to Privacy Harms: Harm Trees



Profile-based discrimination (H.4)

AND

FE.1

FE.3

OR

AND

OR

FE.9

FE.2

. . .

V.11

V.12

V.14

V.14

. . .

OR

OR

V.5

V.10

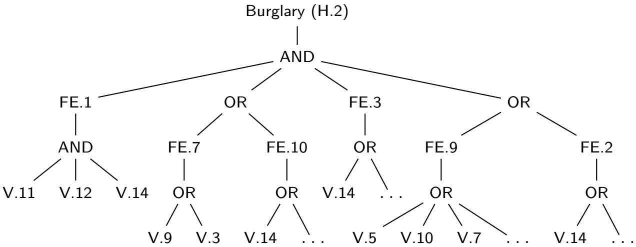
V.7

. . .

V.14

. . .

Figure: Harm tree for profile-based discrimination (H.4)



Burglary (H.2)

AND

FE.1

OR

FE.3

OR

AND

FE.7

FE.10

OR

FE.9

FE.2

V.11

V.12

V.14

OR

OR

V.14

. . .

OR

OR

V.9

V.3

V.14

. . .

V.5

V.10

V.7

. . .

V.14

. . .

Figure: Harm tree for burglary (H.2)

Risk Assessment based on Harm Trees

Risk level: (severity, likelihood)

- Severity is computed from harm attributes
- Likelihood is computed based on:
  - Harm trees
  - Scales for input/output likelihoods
  - Rules for likelihood computation

Scale for input/ output likelihoods

We use the following symbolic values for input and output likelihood (probability) values (p):

- *Negligible (N)* for $p \leq 0.01\%$
- *Limited (L)* for $0.01\% < p \leq 0.1\%$
- *Intermediate (I)* for $0.1\% < p \leq 1\%$
- *Significant (S)* for $1\% < p \leq 10\%$
- *Maximum (M)* for $p > 10\%$

Rules for likelihood computations

P_i is the likelihood of ith child node:

R1. AND node with independent child nodes: $\prod_i P_i$.

R2. AND node with dependent child nodes: $Min_i(P_i)$, i.e., minimum of the likelihoods of child nodes.;

R3. OR node with independent but not mutually exclusive child nodes: $1 - \prod_i (1 - P_i)$.

R4. OR node with mutually exclusive child nodes: $\sum_i P_i$.

R5. OR node with dependent child nodes: $Max_i(P_i)$, i.e., maximum of the likelihoods of child nodes.

The rules are applied bottom-up to the bounds of the intervals associated with the child nodes.

Example risk level computation

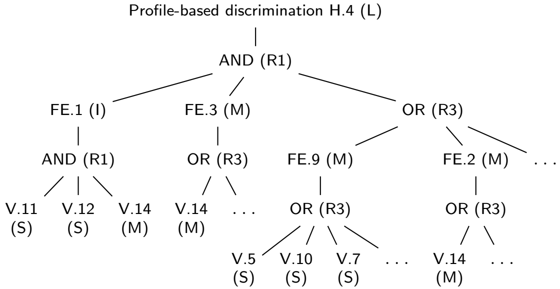


Figure: Example computation of likelihood of profile-based discrimination (H.4) using harm trees

Risk level for profile-based discrimination: *(high, limited)*
Similarly, risk level for burglary: *(moderate, negligible)*

Conclusions based on Risk Assessment

1. Based on the risk levels, risk due to profile-based discrimination should be primary target for mitigation.
2. Based on harm trees, V.14 is the most common privacy weakness, meaning that strong efforts should be put into accountability measures (especially auditing).
   - The above conclusions depend on initial assumptions.
3. Accountability: keeping track of all assumptions and choices made.

Summary of Our Contributions

1. Suitable assumptions about the smart grid system design focusing on the energy management and billing sub-systems.
2. Definition of *harms*, *feared events*, *privacy weaknesses* and *risk sources*.
3. Instantiation of *attributes of harms* for the smart grid scenario.
4. Establishment of *harm trees*.
5. Illustration of usage of harm trees for *risk assessment*, identifying risks need to be mitigated and selecting privacy weaknesses to be countered first for smart grids.

(accepted at IWPE'16)

Other Works

1. PRIAM: Privacy risk assessment methodology
   - Emphasis on classes and attributes of risk sources, privacy weaknesses, feared events, harms
   - Focus on factors that determine classes and attributes
   - Sample measurement scales
   - Application on fitness tracking systems

   (submitted to DBSec'16)

2. Counter-measure selection

Thank you!