Using Game Theory to analyze Risk to Privacy

Lisa Rajbhandari

Einar A. Snekkenes

Agenda

- Introduction
- Background
- Issues focused on this paper
- Why Game Theory?
- A privacy scenario
- Limitations
- Conclusion

Introduction

- Right to privacy
- Identity information used widely
- Might be misused, stolen or lost
- Increase risk to privacy -
  - Information being used as a Commodity
  - Identity theft, online frauds
  - Tracking , profiling of individuals

Aim

- Like all other risks, privacy risks must be managed.
- Identification and understanding of risk.
- Perform risk analysis and evaluation.
- Suitable method ?

Background

Game Theory

- Branch of mathematics
- John von Neumann and Oskar Morgenstern (1944)
- John Nash – ‘Nash Equilibrium’
- Technique of studying situations of interdependence or strategic interactions among rational players [Watson].
- Used in many fields.

[Watson] Joel Watson. Strategy : An Introduction to Game Theory. W. W. Norton & Company, 2nd edition, 2008.

Probabilistic Risk Analysis (PRA)

- Risk level- estimated by studying
  - the likelihood and consequences of an event
  - probabilities in a qualitative \quantitative scale.

- ‘One-person game’ [Ronald]

- Challenges: [Bier]
  - Subjective judgement
  - Human error and performance

[Ronald] Ronald D. Fricker, J.: Game theory in an age of terrorism: How can statisticians contribute? (http://faculty.nps.edu/) Department of Operations Research, Naval Postgraduate School.
[Bier] V.M. Bier. Challenges to the acceptance of probabilistic risk analysis. Risk Analysis, 19:703{710, 1999.

Comparison

Risk Analysis	PRA	Game Theory
Collect data	Ask for subjective probability or historical data	Ask for preferences
Compute risk	Compute risk (eg. Expected value)	Compute probability and outcome (eg. Nash Equilibrium)
Decide what to do	Decide what to do	Decide what to do

Table 1. Comparison of general Risk Analysis steps: Using PRA and Game Theory

Issues focused on this paper

- Suitability of game theory for privacy risk analysis

- How are the utilities of the players calculated?

Why Game Theory?

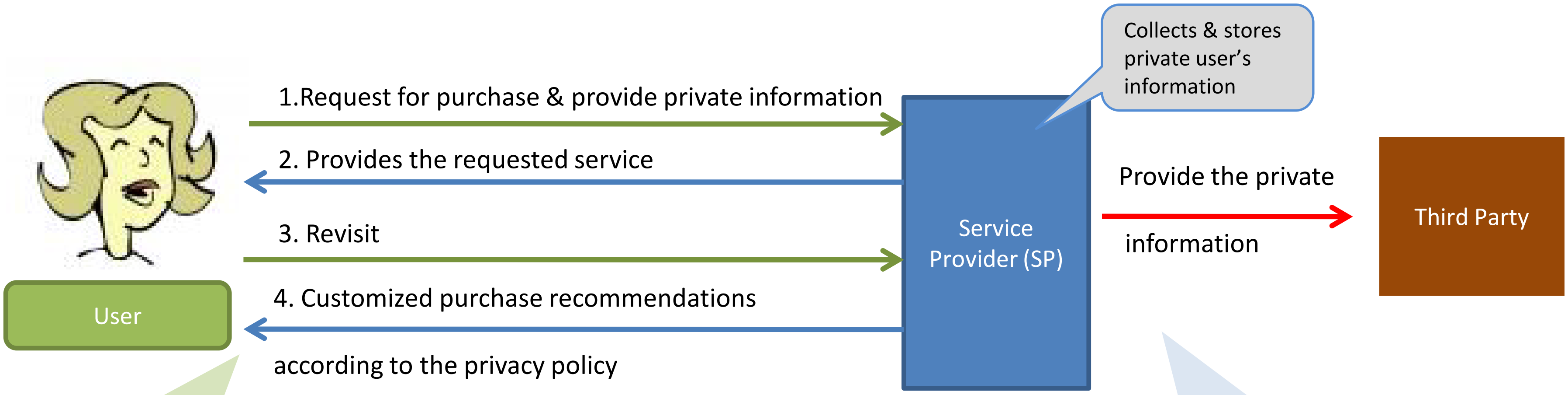
- In a game theoretic setting,
  - Situation in a form of a game.
  - Benefits are based on outcomes.
  - Incentives of the players are taken into account.

Image taken from: http://www.sxc.hu/pic/m/s/st/stelogic/905072_poker_chips_cards_and_dice_1.jpg

Why Game Theory?

- Risk analysis can be based
  - On outcomes which the subjects can provide rather than subjective probability.
  - Settings where no actuarial data is available.

A privacy scenario



Collects & stores private user's information

1.Request for purchase & provide private information

2. Provides the requested service

3. Revisit

4. Customized purchase recommendations according to the privacy policy

User

Service Provider (SP)

Provide the private information

Third Party

Recommendations 'hit'-
User-saves additional time
SP- additional sales

- Tempting for the SP to breach the agreed privacy policy.
- User-incurs additional cost (time wasting activities).

Assumptions

- Game of complete information.
- The players are intelligent and rational.
- They have common knowledge about the game being played.
- They have their best interest to optimize their utilities.

Privacy Scenario (Normal form)

User(U) \ Service Provider (SP)	Exploit (E)	Non-Exploit (NE)
Provide(P) Genuine data	a_{11}, b_{11}	a_{12}, b_{12}
Not Provide(NP) Fake data	a_{21}, b_{21}	a_{22}, b_{22}

Survey Results

- User - Survey data
- SP - Assumed values
- Utilities - Hours saved or lost.

	For User		For SP	
User provides information	Genuine	Fake	Genuine	Fake
SP usage according to policy	1	0,2	1	-0,01
SP usage in breach of policy	-0,9	-0,01	0,5	-0,2

Game Solution

	For User		For SP	
User provides information	Genuine	Fake	Genuine	Fake
SP usage according to policy	1	0,2	1	-0,01
SP usage in breach of policy	-0,9	-0,01	0,5	-0,2

Service Provider (SP)

User(U)

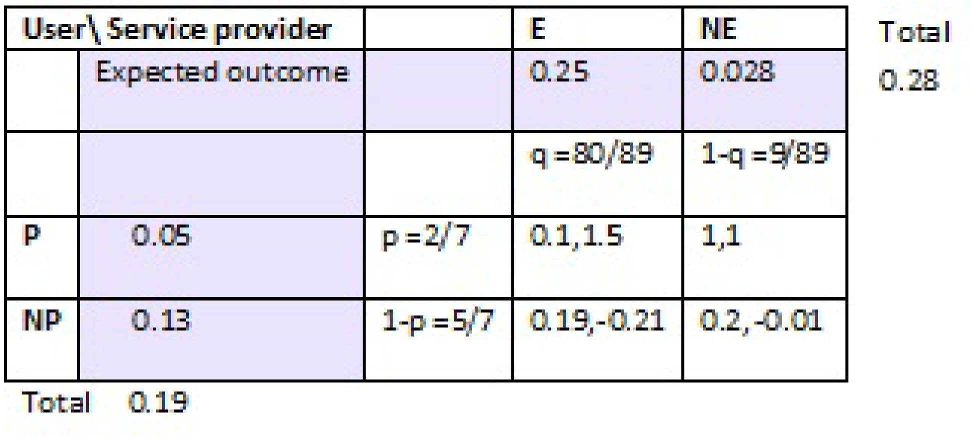
		q Exploit(E)	1-q NotExploit(NE)
p	Provide(P)	0.1 , **1.5**	1 , **1**
1-p	NotProvide(NP)	0.19, -0.21	0.2, -0.01

Fig: Normal form representation

- No pure strategy Nash Equilibrium
- Obtain mixed strategy Nash Equilibrium

$(0 \leq p \leq 1)$ $(0 \leq q \leq 1)$

Mixed strategy NE and Expected outcome



User\ Service provider			E	NE	Total
	Expected outcome		0.25	0.028	0.28
			q =80/89	1-q =9/89	
P	0.05	p =2/7	0.1,1.5	1,1	
NP	0.13	1-p =5/7	0.19,-0.21	0.2,-0.01	
Total	0.19				

Limitations

1. Small survey.

2. In real world situation - partial information.

Conclusion

- Preferences of the subjects vary highly.
- Assigning an appropriate utility.
- Risk analysis can be based on the outcomes.
- Apply the standard risk analysis techniques.

Thank you !