

A Reference Model for Privacy Protection in Social Networking Service

Xiaoguang Deng^a, Caue Bernardi Bispo^b and Yong Zeng^{a*}

^a *Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Canada*

^b *Electrical Engineering Department, University of São Paulo, São Paulo, Brazil*

Abstract Social media has become a popular means of communication thanks to the advancement of computer network and web technology. Social networking service (SNS) provides a virtual platform for users to realize their personal/professional purposes. Users have a great motivation to share their personal updates in social media in order to maintain their contacts. In the meantime, users have a strong need to protect their privacy in order to prevent all kinds of frauds from attackers. In the existing literature, many research efforts address privacy protection issues by employing computer security technology. To our best knowledge, it is the lack of a framework to propose a holistic framework of privacy protection encompassing other factors, such as user's behaviour, SNS provider's security policy, and information management strategy. In this background, this paper aims to derive a reference model for privacy protection in social networking service by using Environment-Based Design (EBD) methodology. A systematic SNS environment analysis is conducted to identify the major challenges and to organize coherent solutions.

Keywords: Privacy protection, social networking service, environment-based design (EBD) methodology, recursive object model (ROM)

1. Introduction

Over the last one and a half decade, social media has become a popular mode of communication. As Boyd & Ellison defined, social media (also called social network sites) is a web-based service that allows individuals to create a public or semi-public profile within a bounded system (Boyd & Ellison, 2007). The users can benefit from social networking service (SNS) for diverse personal/professional purposes, e.g. maintenance and development of social linkage, interest sharing, event promotion, job hunting/recruiting, business marketing, canvassing etc.

According the analysis following similar procedure in (Zeng *et al.*, 2012) based on environment-based design (EBD) methodology (Zeng, 2004; Zeng, 2011), the evolution of SNS can be roughly divided into three generations (Boyd & Ellison, 2007; nextMEDIA, 2010): group-based, link-based and specification-based. The evolution analysis using EBD methodology is shown in Fig. 1.

A group-based service aims to provide a connection of group in which the members have common interests. The first notable group-based social media was SixDegrees.com, launched in 1997. It allowed users to create their profiles and share their friends' lists without any permission. However, due to the restriction of computer network infrastructure and applications, users had very few controls over the network except viewing and chatting. The second wave of SNS began in 2002, which was marked by the first successful link-based SNS provider Friendster. Its purpose was to establish an online network of

* Corresponding author. Email: zeng@ciise.concordia.ca Tel: (+1)514-8482424 ext. 5801.

friends to match the loving couples (Goldberg, 2007). Since 2003, a number of link-based social network sites have been created (Boyd, 2006), such as MySpace (2003), LinkedIn (2003), Facebook (2004), CouchSurfing (2004), Flickr (2004), Orkut (2004) and YouTube (2005). Link-based sites have since become the mainstream of social media, as a global network cross the boundaries of nations, cultures and interests.

The group - and link-based social network has a horizontal structure. Those kinds of networks spread quickly and widely and contain large-scale information of a broad audience. However, the unstructured massive data transaction may overwhelm users with information overflow. In this context, SNS have a new trend from horizontal structure to vertical structure. Vertical SNS can be divided into two categories: personal-based and professional-based. Personal-based vertical SNS satisfies different personal interests (Boyd & Ellison, 2007), such as intention-centered (e.g. ASmallWorld, BeautifulPeople), activity-centered (e.g. Couchsurfing), and affiliation-focused (e.g. MyChurch). In the meantime, a number of industry-based vertical social network sites have been largely launched since 2005, such as Spiceworks (IT service), Wave (accounting), Practice fusion (health), Github (software), and ResearchGate (research). With a relatively niche scale, on the one hand, users of vertical SNS share their updates in order to actively get involved in the community, on the other hand, such information sharing contains huge amount of user privacy, which may include personal information, know-how expertise and intellectual property. Therefore, privacy protection becomes a critical issue in the new generation of SNS.

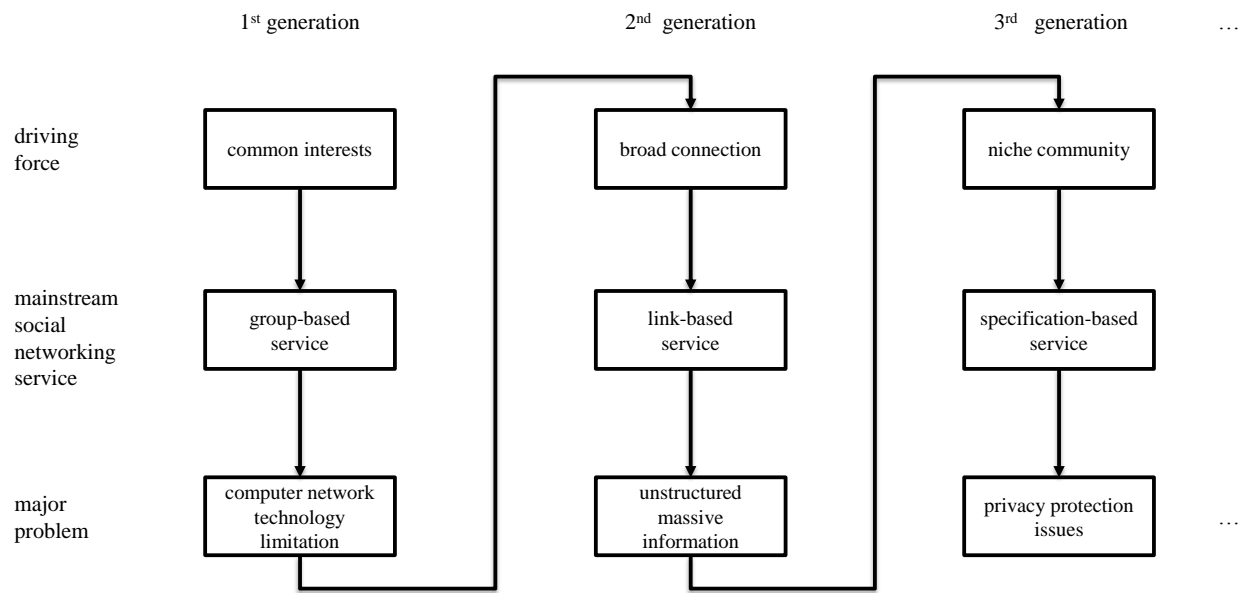


Fig. 1. Evolution analysis of social networking service (SNS) using EBD methodology.

Many existing literature emphasizes on employing computer security technologies for privacy protection in social media, like access control (Shehab *et al.*, 2012), secure multi-party computation (Li *et al.*, 2011), privacy-preserving location-based services (Puttaswamy & Zhao, 2010), data generalization (Tang & Yang, 2012), and data sanitization and anonymization (Zheleva *et al.*, 2012) etc.

To the authors' best knowledge, it is still the lack of a holistic framework to organize the scattered research ideas and results arisen from multiple factors, such as user behaviour, security policy, information management, security and privacy technology. In this context, this paper aims to propose a reference model to guide users to systematically prevent privacy leakage. Environment-Based Design (EBD) methodology, which has a strong ability of deriving step-by-step a conceptual model based on a complete environment analysis, is adopted to conduct this research.

This paper will be organized as follows. Section 2 will give a brief presentation of EBD methodology. Section 3 will focus on a systematic environment analysis of social networking service, and Section 4 aims to identify the critical challenges of privacy protection in SNS. Section 5 will deliver the reference models of privacy protection. A case study will be illustrated in Section 6. The conclusion will be given in Section 7.

2. Methodology: Environment-Based Design



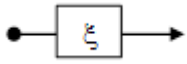
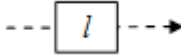
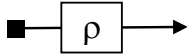
Environment-Based Design (EBD) is a design methodology proposed by Dr. Yong Zeng (Zeng, 2004; Zeng, 2011). EBD consists of three activities: environment analysis, conflict identification, and solution generation. These three activities work simultaneously to refine design requirements, analyse the problems, and generate the solutions.

In the SNS context, environment analysis refers to understanding the state of the art of social networking service. Conflict identification aims to identify the major challenges of privacy protection in a SNS environment. Solution generation will propose a reference model for user's privacy protection by addressing the identified challenges.

One of the significant strengths of EBD is the accommodation of semantic analysis throughout the entire design process. A semantic modelling tool, called Recursive Object Model (Zeng, 2008), is used to represent and deal with linguistic information in a design, which provides designers guidance to accumulate the necessary and sufficient information (Wang et al., 2013).

ROM refines representation of environment structure by including three types of relations: constraint, connection, and predicate; and two kinds of objects: primitive and compound objects. Table 1 shows the graphic symbols and their descriptions in ROM.

Table 1. Representation of recursive object model (Zeng, 2014)

	Type	Symbol	Description
Object	Object		Everything in the universe is an object
	Compound Object		It is an object that includes at least two objects in it.
Relation	Constraint Relation		It is a descriptive, limiting, or particularizing relation of one object to another.
	Connection Relation		It is to connect two objects that do not constrain each other.
	Predicate Relation		It describes an act of an object on another or that describes the states of an object.

3. Environment Analysis

In this section, the complex environment of social networking service (SNS) will be analysed. Firstly, we summarize and express the corresponding design problem from a sentence as follows:

“Derive a reference model to protect user's privacy in social networking service (SNS).”

The problem description can be transformed into the following Recursive Object Model (Zeng, 2008) diagram (shown in Fig. 2).

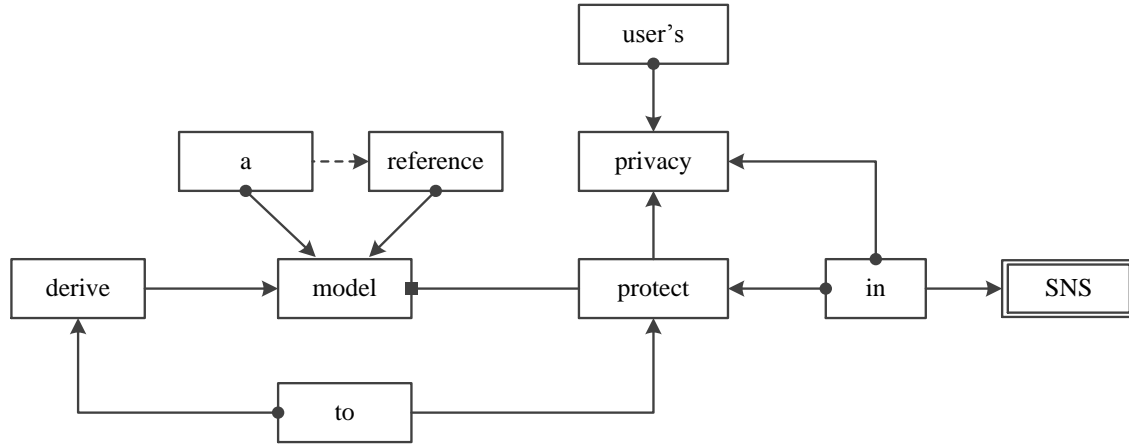


Fig. 2. Initial ROM diagram for problem description.

The initial ROM diagram can be simplified and transferred into a Product-Environment System (PES). In design perspective, the “product” component is “reference model”, which represents the main product to be designed. The environment components are “user’s privacy” and “social networking service”. The major interaction is “protect”, which occurs between “product” (reference model) and its environment components (user’s privacy). Mathematically, PES can be represented in Eq. (1).

$$\begin{aligned}
 S &= \text{reference} * \text{model}, \\
 E &= (\text{in} \otimes \text{SNS}) * (\text{user}'s * \text{privacy}), \\
 I &= (\text{reference} * \text{model}) \otimes \text{protect} \otimes (\text{in} \otimes \text{SNS}) * (\text{user}'s * \text{privacy}), \\
 &\text{where } \otimes (\text{interaction}), \text{ and } * (\text{constraint}).
 \end{aligned} \tag{1}$$

Based on PES given in Eq. (1), necessary information is required to understand the environment and thus to realize the product (“reference model”) to serve its environment. Question-asking is one of the most effective ways to elicit the relevant information. According to EBD’s question asking rules (Wang & Zeng, 2009; Zeng, 2014), a set of generic questions are asked and their answers are shown in Table 2. The answers issued from existing literatures.

Accordingly, the description of design problems can be updated as below.

“Propose a framework to understand and represent the relationships of the concepts in social networking service (SNS), as well as to develop standards and specifications to protect user’s personal information in such environment in order to prevent different kinds of frauds.”

Schematically, the product-environment system (PES) is updated and simplified in Fig. 3, and mathematically, Eq. (1) can be updated as Eq. (2). And the five updated interactions are shown in Table 3.

Next, two domain questions will be asked in Table 4 and Table 5 to elicit natural, built and human environment components regarding life-cycle perspective of privacy protection along with data sharing workflow in social media (Chen & Zeng, 2006).

Table 2. Generic question-asking

Question	Description
Why to propose a reference model to protect privacy in SNS?	In order to help user prevent the frauds from SNS (FCAC, 2013).
What do you mean “social networking service”?	A web-based service that allows individuals to build social relations among people who share interests, activities, backgrounds or real-life connections (Boyd & Ellison, 2007).
What is “privacy”?	The ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively (Falahi et al., 2010) .
What is “user’s privacy”?	It refers to user’s personal information (Gross & Acquisti, 2005).
What is “user privacy” in SNS?	It refers to user’s personal information implied in social networking service (Gross & Acquisti, 2005).
What is a “model”?	A model in science is anything used as a representation of an object, law, theory or event used as a tool for scientific understanding (Wartofsky, 1979).
What is a “reference model”?	A framework is to help understanding the significant relationships among the entities of an environment, and to develop consistent standards or specifications supporting that environment (OASIS, 2006).
How to protect user’s privacy in SNS?	unknown.

$S = \text{framework},$

$E = E_1 \cup E_2 \cup E_3 \cup E_4 \cup E_5 \cup E_6,$

$E_1 = ((in \otimes SNS) * \text{concept}) * \text{relationships},$

$E_2 = \text{standards},$

$E_3 = \text{specifications},$

(2)

$E_4 = (in \otimes SNS) * (\text{personal} * \text{information}),$

$E_5 = \text{frauds},$

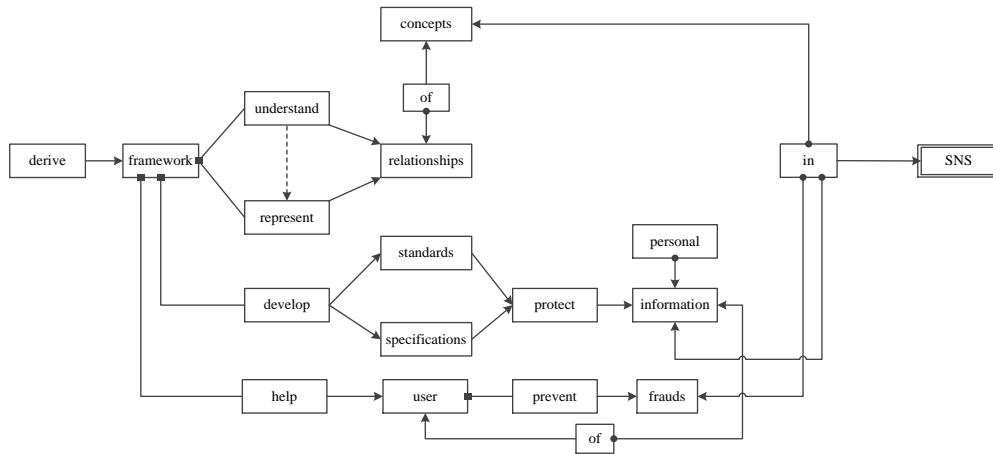
$E_6 = (in \otimes SNS) * \text{users},$

$I = I_1 \cup I_2 \cup I_3 \cup I_4 \cup I_5 \cup I_6,$

where \otimes (interaction), $*$ (constraint), and \cup (union).

Table 3. Interactions in PES (generic questions)

Interaction	Description	Formal representation
I_1	framework understands relationships of concepts in SNS	$I_1 = \text{framework} \otimes \text{understand} \otimes ((\text{in} \otimes \text{SNS}) * \text{concept}) * \text{relationships}$
I_2	framework represents relationships of concepts in SNS	$I_2 = \text{framework} \otimes \text{represent} \otimes ((\text{in} \otimes \text{SNS}) * \text{concept}) * \text{relationships}$
I_3	framework develops standards and specifications	$I_3 = \text{framework} \otimes \text{develop} \otimes (\text{standards} \wedge \text{specifications})$
I_4	standards and specifications protect personal information in SNS	$I_4 = (\text{standards} \wedge \text{specifications}) \otimes \text{protect} \otimes ((\text{in} \otimes \text{SNS}) \wedge (\text{personal})) * \text{information}$
I_5	framework helps users	$I_5 = \text{framework} \otimes \text{help} \otimes \text{users}$
I_6	users prevent frauds in SNS	$I_6 = \text{users} \otimes \text{prevent} \otimes (\text{in} \otimes \text{SNS}) * \text{frauds}$

**Fig. 3. PES after generic questions-asking.****Table 4. Domain specific questions**

#	Domain specific questions	Answers
1	What is the lifecycle of “privacy protection in SNS”?	Privacy protection goes throughout the whole workflow of data sharing in SNSs, including login registration, profile edition, status updates, community development etc. The personal information refers to user login information, user’s private information, user’s recent updates, and contacts’ sharing information respectively.
2	What are the natural, built and human components for privacy protection in SNS?	In this case, natural environment is not available, and the relevant human/built environment components are shown in Table 5.

After domain question asking, PES will be divided into two levels (represented in Eq. (3)) regarding environment component E_4 , which means the content of “private information leakage” refers to leakage of “user’s login information”, “user’s private information”, “user’s recent updates”, and “contacts’ sharing information” respectively along with the activities in social media. The updated ROM-based PES after domain question-asking is shown in Fig. 4.

Table 5. Workflow of data sharing in social media (domain questions)

Activity	Human	Built	
		Infrastructure	Information content
Login registration	user, SNS provider	telecommunication protocols, computer network and web technology, social network website etc.	login information: user name, ID, passwords etc.
Profile edition	user, SNS provider		personal information: name, nickname, gender, age, profession, address etc.
Status sharing	user, SNS provider		recent updates: message, photo, video etc.
Community development	user, user’s friend, SNS provider		contact’s sharing information: friends’ name, nickname, profession, affiliation etc.

Frist level

$$E = E_1 \cup E_2 \cup E_3 \cup E_4 \cup E_5 \cup E_6,$$

Second level

$$E_4 = E_{4,1} \cup E_{4,2} \cup E_{4,3} \cup E_{4,4}$$

$$E_{4,1} = (in \otimes login\ registration) * (login * information), \quad (3)$$

$$E_{4,2} = (in \otimes profile\ edition) * (personal * information),$$

$$E_{4,3} = (in \otimes status\ updates) * (recent * updates),$$

$$E_{4,4} = (in \otimes community\ development) * (contact * information),$$

where \otimes (interaction), $*$ (constraint), \cup (union).

4. Challenge Identification

Based on analysis above, this section attempts to identify the major challenges (conflicts) for user’s privacy protection in social media. First, a performance network will be established in order to show the dependence relations between the interactions. The representation of dependence relations is presented in Eq.(4).

$$I_{ij} = \begin{cases} 1 & \text{interaction } I_i \text{ has dependance relations on interaction } I_j \\ 0 & \text{otherwise} \end{cases} \quad (4)$$

The matrix of dependence relations is shown in Table 6. In EBD (Zeng, 2014), a performance is defined as the relations of interactions. The performance network is mathematically presented in Eq. (5), and schematically illustrated as an interaction map (shown in Fig. 5). The ROM-based performance network is presented in Fig. 6.

In EBD (Zeng, 2014), a conflict is defined as a lack of the available resources to meet a request of actions and properties. We defined two kinds of conflicts: active and reactive. An active conflict appears when it has absence of necessary action to trigger current interaction, whereas a reactive conflict occurs when two interactions cannot be accommodated simultaneously by a resource. In order to obtain the active/reactive conflict, in our study, two questions concerning triggered actions and accommodated resources are asked for each interaction (shown in Table 7).

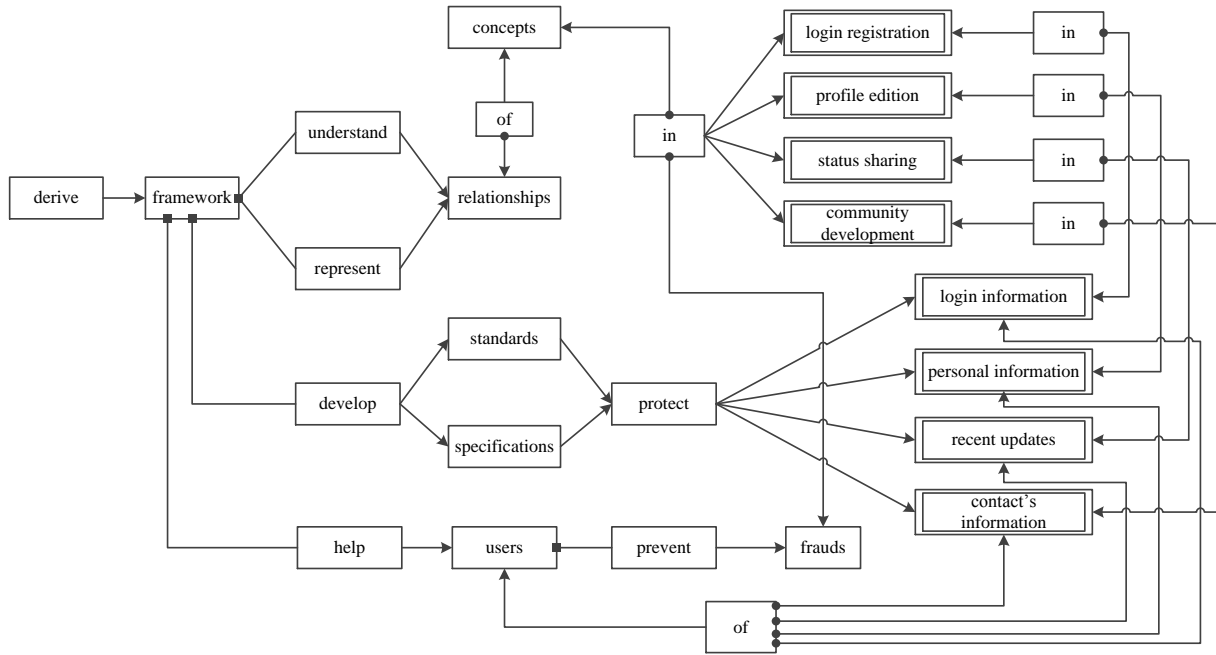


Fig. 4. PES after domain specific questions-asking.

$$P = P_{12} \cup P_{13} \cup P_{23} \cup P_{34} \cup P_{45} \cup P_{56},$$

$$P_{12} = (to \otimes I_2) * I_1,$$

$$P_{13} = (to \otimes I_3) * I_1,$$

$$P_{23} = (to \otimes I_3) * I_2,$$

$$P_{34} = (to \otimes I_4) * I_3,$$

$$P_{45} = (to \otimes I_5) * I_4,$$

$$P_{56} = (to \otimes I_6) * I_5,$$

\otimes interaction.

(5)

Table 6. Dependence relations between interactions

	I ₁	I ₂	I ₃	I ₄	I ₅	I ₆
I ₁						
I ₂	1					
I ₃	1	1				
I ₄			1			
I ₅				1		
I ₆					1	

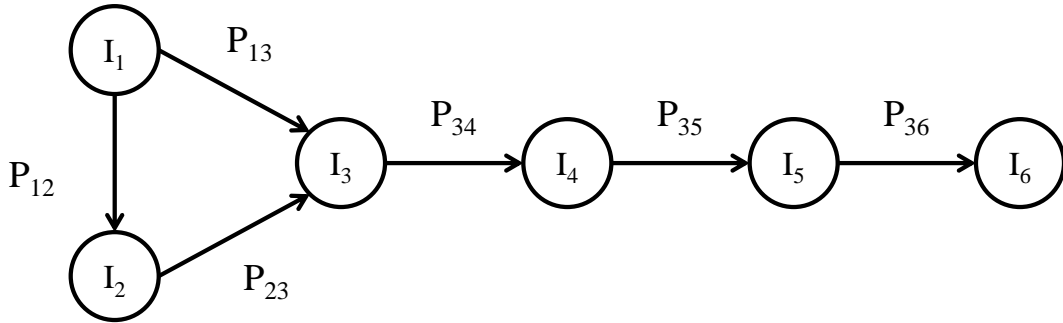


Fig. 5. Interaction map.

Since we are in the early stage of conceptual design, it assumes that we do not have any available action to trigger any interaction, and it has no overlap of resources to accommodate the interactions. Thus, we have only active conflicts C₁-C₆ at this stage related to the interactions. According to the logic of design (Zeng & Cheng, 1991), in contrast with performance analysis as a deductive process (“evaluation operator”), conflict identification is an adductive process (“synthesis operator”). Therefore, the dependence of conflicts is opposite as that of interactions. The conflict map is shown in Fig. 7. According to EBD rule, C₆, which has no incoming edge, is the critical conflict (root conflict), which is privileged to be addressed in the next section.

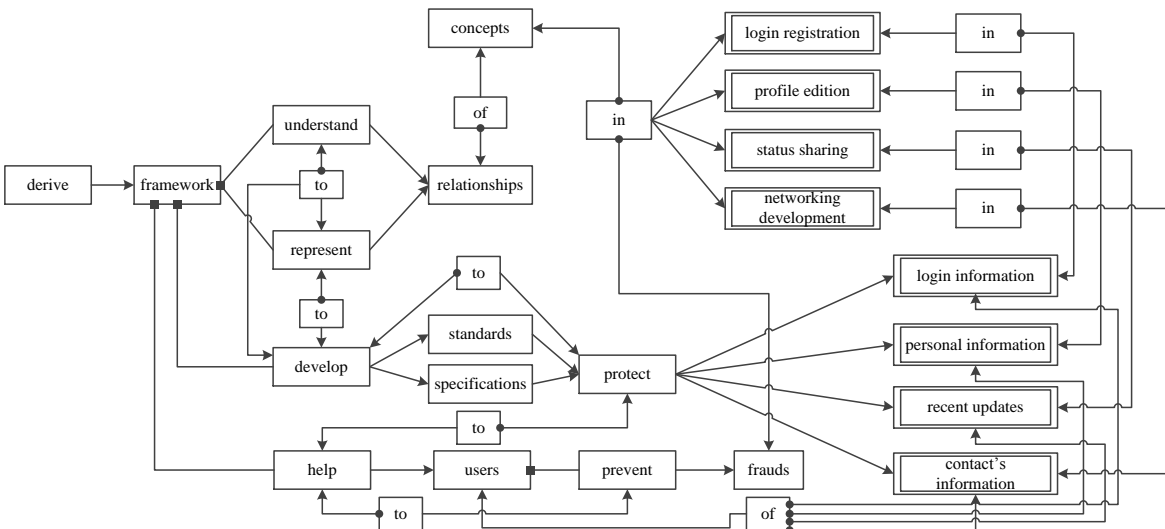


Fig. 6. ROM-based performance network.

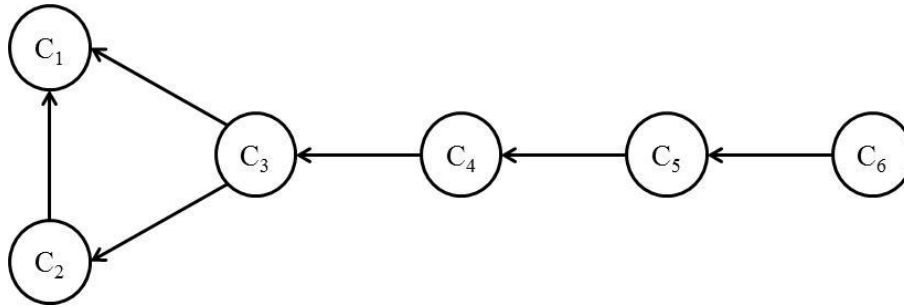


Fig. 7. Conflict map.

Table 7. Questions to elicit active/reactive conflicts

Interaction	Question	Answers
I ₁	What trigger framework to understand the relationships of concepts in SNS?	to identify the concepts in SNS
	What resources are needed to accommodate framework to understand the relationships of concepts in SNS?	literatures, bibliographies, references, open source information about SNS
I ₂	What trigger framework to represent the relationships of concepts in SNS?	to understand their relationships
	What resources are needed to represent framework to understand the relationships of concepts in SNS?	structural information and data of concepts
I ₃	What trigger framework to develop standards and specifications?	to identify the standards and specifications
	What resources are needed to develop standards and specifications?	stakeholder agreement, frauds understanding, support of policy
I ₄	What trigger standards and specifications to protect leakage of private information in SNS?	to follow the standards and specifications
	What resources are needed to protect leakage of private information in SNS?	guideline, policy, IT infrastructure
I ₅	What trigger framework to help the users?	to use the framework
	What resources are needed to help the users?	understanding of users' needs and behaviour
I ₆	What trigger users to prevent frauds?	to identify and avoid the frauds
	What resources are needed to help users to prevent frauds in SNS?	SNS provider's security policy, computer security technology

5. Reference Model Generation

5.1. Environment decomposition

The corresponding environment components related to conflict C_6 are $(in \otimes E_4) * E_5$, and $E_4 = E_{41} \cup E_{42} \cup E_{43} \cup E_{44}$. According to EBD solution strategy, we will decompose the related environment components in order to find out the knowledge of interaction related to each environment component. The decomposition procedure is represented as Eq. (6).

$$\begin{aligned} E_{1_6} &= (for \otimes E_4) * E_5 = (for \otimes (E_{41} \cup E_{42} \cup E_{43} \cup E_{44})) * E_5, \\ (\oplus E_{1_6}) &= \oplus((for \otimes E_4) * E_5) \\ &= \oplus((for \otimes E_{41}) * E_5) \cup (for \otimes E_{42}) * E_5 \cup (for \otimes E_{43}) * E_5 \cup (for \otimes E_{44}) * E_5 \end{aligned}$$

$$\text{denote } EE_1 = (for \otimes E_{41}) * E_5, EE_2 = (for \otimes E_{42}) * E_5, EE_3 = (for \otimes E_{43}) * E_5, EE_4 = (for \otimes E_{44}) * E_5$$

$$\begin{aligned} (\oplus E_{1_6}) &= \oplus(EE_1 \cup EE_2 \cup EE_3 \cup EE_4) \\ &= EE_1 \cup EE_2 \cup EE_3 \cup EE_4 \cup (EE_1 \otimes EE_1) \cup (EE_2 \otimes EE_2) \cup (EE_3 \otimes EE_3) \cup (EE_4 \otimes EE_4) \\ &\cup (EE_1 \otimes EE_2) \cup (EE_2 \otimes EE_1) \cup (EE_1 \otimes EE_3) \cup (EE_3 \otimes EE_1) \cup (EE_1 \otimes EE_4) \cup (EE_4 \otimes EE_1) \\ &\cup (EE_2 \otimes EE_3) \cup (EE_3 \otimes EE_2) \cup (EE_2 \otimes EE_4) \cup (EE_4 \otimes EE_2) \\ &\cup (EE_3 \otimes EE_4) \cup (EE_4 \otimes EE_3) \end{aligned}$$

where $\oplus(\text{structure}), \otimes(\text{interaction}), \cup(\text{union})$.

In our context, we particularly focus on the leakage of $EE_2 = (for \otimes E_{42}) * E_5$, which means the frauds for the leakage of personal information in phase “profile edition”. Therefore, we update the relevant objects and interactions in Eq. (6) as below.

$$\begin{aligned} &EE_2 \cup (EE_2 \otimes EE_2) \cup (EE_1 \otimes EE_2) \cup (EE_2 \otimes EE_1) \\ &\cup (EE_2 \otimes EE_3) \cup (EE_3 \otimes EE_2) \cup (EE_2 \otimes EE_4) \cup (EE_4 \otimes EE_2) \end{aligned} \quad (7)$$

where $\oplus(\text{structure}), \otimes(\text{interaction}), \cup(\text{union})$.

The interpretation of decomposed elements in Eq. (7) is shown in Table 8.

Table 8. Interpretation of decomposed elements

#	Elements	Interpretation
1	EE_2	the frauds cause the leakage of users' personal information
2	$(EE_2 \otimes EE_2)$	the frauds cause the leakage of users' personal information due to its updates
3	$(EE_1 \otimes EE_2)$	the frauds cause the leakage of users' personal information due to the interactions of login information
4	$(EE_3 \otimes EE_2)$	the frauds cause the leakage of users' personal information due to the sharing of recent updates
5	$(EE_4 \otimes EE_2)$	the frauds cause the leakage of personal information due to the interactions of contacts' information

The updated performance network is shown in Fig. 8. As we mentioned above, design is a recursive procedure. Therefore, we launch 2nd round iteration of EBD procedure for further analysis in order to find out the knowledge and the corresponding solutions.

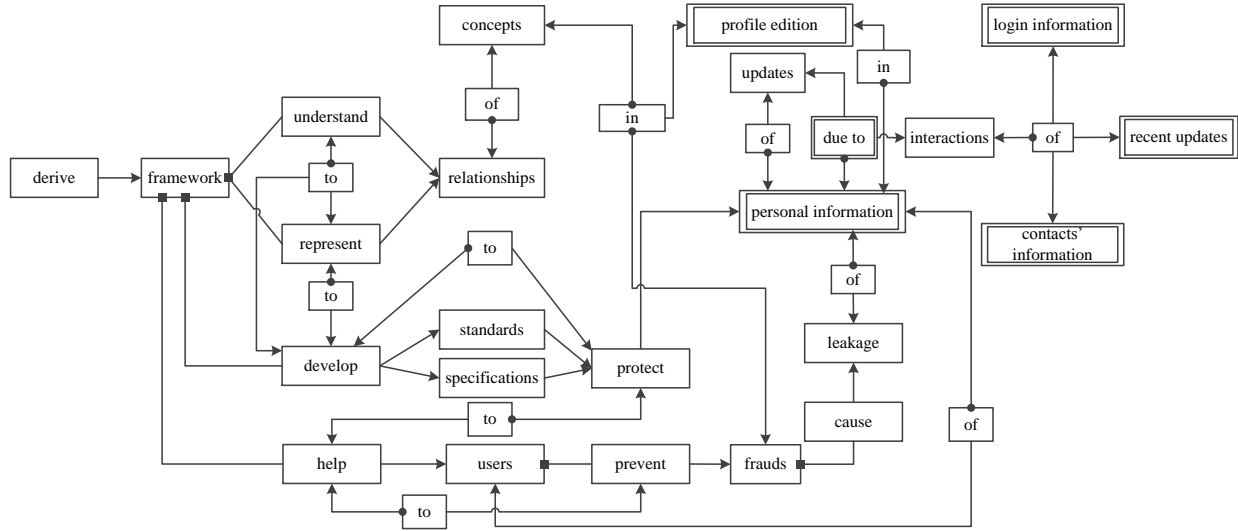


Fig. 8. Performance network after decomposition.

According to the principle of change management, in the second iteration, only the changed part will be focused in question-asking. Two generic questions are asked in Table 9.

Table 9. Question-asking (2nd iteration)

Question	Description
What do you mean the leakage of personal information?	it refers to disclosure some information to unauthorized parties (Ware, 1967).
How do frauds cause the leakage of personal information?	by attacks or inferences (Zhang et al., 2011).

According to the question 2 in Table 9, solution generation can be divided into two categories: explicit or implicit prevention. Explicit prevention means to prevent the personal information leakage from the vulnerabilities in social networking channels. Thus, the attacker uses available information collected from social media to attack the user by sending spear (Arachchilage et al., 2012) or trying to hijack the user's social media account (Cashion & Bassiouni, 2011; Xie et al., 2013). Implicit prevention refers to information leakage by inferences.

Thus, the first category aims to prevent the frauds by attacks, whereas the second category attempts to prevent the frauds caused by inferences. The second category of personal information leakage through inferences will be developed in Section 5.3.

5.2. Explicit prevention from attacks

The knowledge of explicit prevention, which refers to personal information leakage by attacks, is shown in Table 10. Corresponding to the decomposed interaction in Table 8, Table 10 shows the needed actions, and the guidance for users (solutions) in order to achieve such actions.

Table 10. Guidance of explicit prevention (personal information leakage by inferences)

Descriptions	Action needed	Guidance
prevent explicitly the frauds that cause the leakage of user personal information <i>explicitly * prevent</i> $\otimes EE_2$	avoid attacker to get login information through user incorrect behaviour, illegitimate third-party applications, false connection request, and malware etc.	<ol style="list-style-type: none"> 1. be cautious when clicking on abbreviated links 2. be careful with pop-up windows 3. log off your login immediately after each use 4. be careful with unknown third-party applications 5. reduce the quantity of tracking of web surfing 6. always erase cookies 7. use antivirus and spyware protection
prevent explicitly the frauds that cause the leakage of user's personal information due to its updates <i>explicitly * prevent</i> $\otimes (EE_2 \otimes EE_2)$	avoid attacker to access sharing updates legally	<ol style="list-style-type: none"> 8. learn and be familiar with privacy setting
prevent explicitly the frauds that cause the leakage of users' personal information due to the interactions of login information <i>explicitly * prevent</i> $\otimes (EE_1 \otimes EE_2)$	avoid attacker to access personal information by entry stolen login information	<ol style="list-style-type: none"> 9. create a unique and robust password 10. use information that nobody else would know about you when asked to create security questions 11. consider creating a unique email address for using only in your social media account 12. carefully read the privacy policy and terms of service before creating an account 13. always erase cookies 14. try to log off once finish using it
prevent explicitly the frauds that cause the leakage of user's personal information due to the interactions of recent updates <i>explicitly * prevent</i> $\otimes (EE_3 \otimes EE_2)$	avoid attacker to access personal information through the sharing of recent updates	<ol style="list-style-type: none"> 15. learn and be familiar privacy setting 16. always erase cookies
prevent explicitly the frauds that cause the leakage of personal information due to the interactions of friend's information <i>explicitly * prevent</i> $\otimes (EE_4 \otimes EE_2)$	avoid attacker to access personal information through contact's requests, called social engineering, such as phishing attacks, spear phishing, misleading solicitation, hijacked accounts etc.	<ol style="list-style-type: none"> 17. always erase cookies 18. verify the contact's holder identity before accepting the request 19. reject a request from a stranger 20. hire an identity theft protection service

The proposed guidance of explicit prevention above can be categorized into four classes: user's behaviour (guidance 1, 2, 3, 4, 5, 6, 16, 17, 18, 19), policy reviewing (guidance 8, 12), information control (guidance 9, 10, 11), and employment of security software (guidance 7, 20). Accordingly, a multi-level reference model of explicit prevention is proposed in Fig. 9.

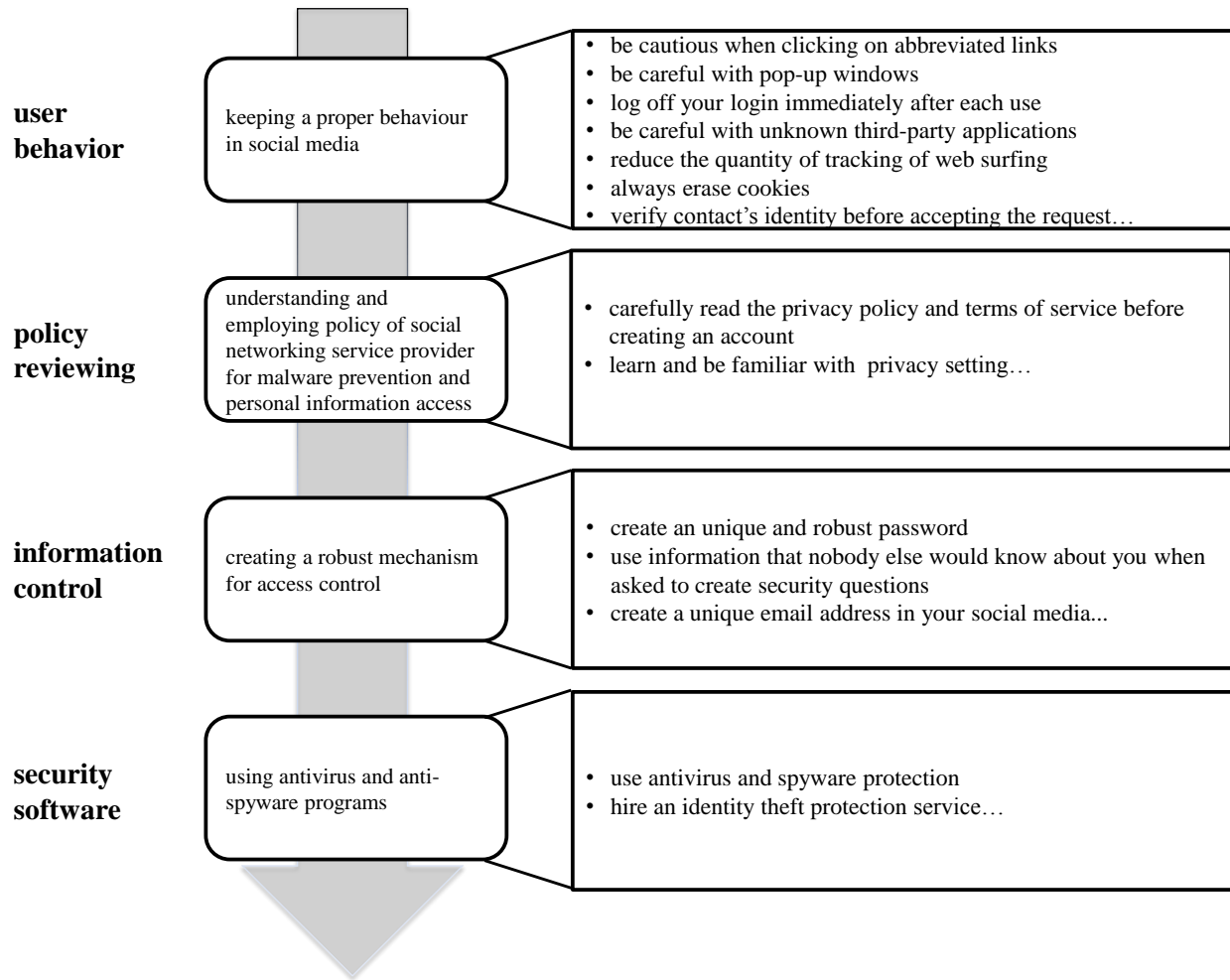


Fig. 9. Reference model for explicit inference.

5.3. Implicit prevention from inferences

Several research findings have been done to study how confidential information leakage caused by inferences in social media. Acquisti and Gross (Acquisti & Gross, 2009) provided a concrete case to show how to inference Social Security Number (SSN) from sharing information in social networking. *He et al.* (He et al., 2006) and *Xu et al.* (Xu et al., 2008) presented how to infer private information through groups of friends with same characteristics using Bayesian network approach. However, to our best knowledge, most researchers pay attention to the techniques of fraud prevention, and few of them focus on the nature of leakage by conceptual modelling. In this section, we aim to model the channel of information leakage caused by inferences in order to better understand its scenario of leakage, and then to find out a coherent solution.

5.3.1. Notation

Information leakage caused by inferences means attacker can infer personal information from user based on available information found in social media. For instance, the inference of Social Security Number (SSN) of someone based on public information found in his profile. The reasons that cause potential information leakage through inferences are listed as below:

- 1) Social media is a complex network, which has a huge amount of users connected between each other, and large sharing information. Although most of the users have the same interest and use social networking service for positive purposes, some others might have negative intentions.
- 2) Every user has its own personal information and usually tries to prevent his/her personal information from leaking to (potential) attackers. For instance, a user has his own Social Security Number (SSN), the inferrer (might be either user) may try to either infer the SSN based on information collected in social media, or directly attack it through spear phishing email or malwares.
- 3) The users' connections within social media may be set different privacy settings from the user. Therefore, when a user shares information with another user, the shared information may be leaked to third parties by the second user either deliberately or unintentionally.
- 4) There are many sorts of information sharing between users in social media. For example, a user may share his full name, date of birth, place of birth, real-time location, etc.
- 5) The relation between shared information and personal information sometimes is complicated and difficult to delimitate. It may be described with formal methods such as fuzzy set theory (Shyng et al., 2010), or with informal methods such as tables and natural language.

In order to clarify the degree of privacy within personal information, we are going to divide information into two major classes:

- 1) Personal information I_p : the information to protect by the user in social media.
- 2) Shared information I_s : all information that is shared by the user in social media either through himself or through his contacts.

Our previous studies related to information leakage in supply chains through inferences developed by (Zhang, et al., 2011), allowed us to make an analogy with our scenario and to propose the abstract conceptual model for inferences in social media. The details will be given as below.

5.3.2. Reference model of implicit prevention of information leakage caused by inferences

Fig. 10 shows the abstract conceptual model of information leakage caused by inferences in social media, which consists of the five key abstract concepts.

- 1) Personal information: personal information I_p is an abstract information object that the inferrer wants to collect in order to make the frauds against user.
- 2) User: a user is a participant who holds the personal information I_p and tries to prevent it from revealing to the inferrer.
- 3) Inferrer: an inferrer is a participant who has initial knowledge K_o , collects the user's shared information I_s and try to acquire user's I_p .
- 4) Knowledge: knowledge K_o is the initial knowledge that the inferrer has about the user. S/He will use it combined with I_s in order to try to infer I_p .
- 5) Channel: Channel is the social media through which shared information I_s is transferred from the user to the inferrer.

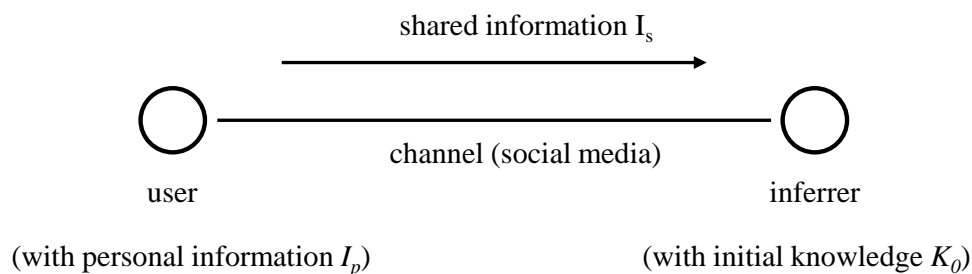


Fig. 10. Conceptual model for implicit inference.

Assuming that an attacker can obtain three sorts of knowledge: “initial knowledge”, “knowledge obtained through information shared” and “knowledge obtained through inferences”, we denote the attacker’s initial knowledge as K_o , knowledge obtained through shared information I_s as K_s , a comprehension of K_o and K_s as K_o+K_s , a knowledge inferred from K as K^* , and knowledge of information I_p from knowledge K_o as $(K_o+K_s)^*$. Based on the notations above, we can describe the relations among K_o , K_s , K^* and $(K_o+K_s)^*$ in Fig. 11.

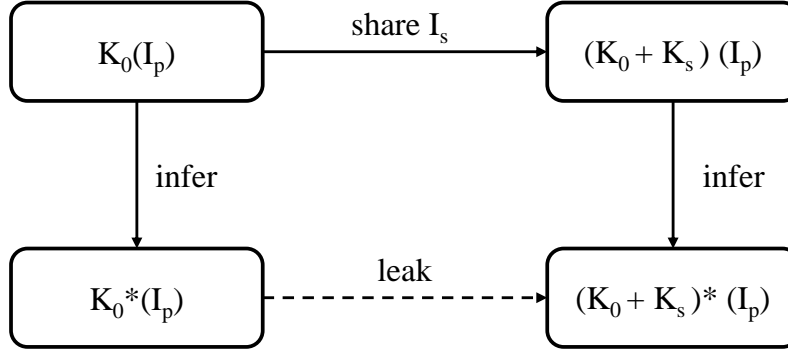


Fig. 11. Conceptual model of implicit information leakage caused by inferences.

With the above abstract model, the scenario can be derived as follows:

- 1) Initially, an inferrer has knowledge K_o ;
- 2) The inferrer’s knowledge K_o becomes K_o^* after inferring on K_o ;
- 3) When the inferrer shares I_s , due to the inferences, the inferrer’s knowledge increased to be $K_o + K_s$;
- 4) The infereer’s knowledge becomes $(K_o + K_s)^*$ after inferring on $K_o + K_s$.

If the inferrer can obtain more knowledge of the personal information I_p from $(K_o + K_s)^*$ than from K_o^* , in other words, if $(K_o+K_s)^*(I_p) > K_o^*(I_p)$, it means that there is some I_p leaked from the user to the attacker through sharing information I_s in social media. Therefore, the risk of implicit information leakage through inferences can be conceptually measured by following equation.

$$r_{s,j} = (K_o + K_s)^*(I_p) - K_o^*(I_p) = \sum_{i=1} P(I_s | \{(I_s, U_j)\}) \times C(I_s) \quad (8)$$

$$\text{where } C(I_s) = \begin{cases} 1 & \text{if } I_s \text{ is personal} \\ 0 & \text{if } I_s \text{ is not personal} \end{cases}$$

In Eq. (8), $\sum_{i=1} P(I_i | \{(I_i, U_j)\})$ is the overall probability of leakage when user U_j share information I_s is social media. According to the analysis above, we can notice that the solution is directed to minimize the risk, namely the increasing knowledge K_s , due to the sharing of personal information I_s . Therefore, user is suggested to only share the personal information with less risk of inferences. In our previous research, a set of methods has been proposed to address this issue. For more details of the methods, please refer to (Deng et al., 2012; Zeng, et al., 2012; Zhang et al., 2012; Zhang, et al., 2011), which will not be detailed in this paper, for the sake of simplicity.

6. Case Study

In this section, we illustrate the proposed reference models through a case study of identity theft prevention, namely the protection of Resident Identification Card Number of People's Republic of China. The format of Chinese ID card number has 18 digits and its format is $RRRRRRYYYYMMDDSSSC$ (CHN103755.E, 2011). $RRRRRR$ is a standard code of administrative division in which the cardholder is registered, for example, 110108 represent Haidian District of Beijing Municipality. $YYYYMMDD$ standards for the date of birth (year/month/day) of cardholder. SSS is a sequential code, which is odd for males and even for females. The final digit C is a check sum value over the first 17 digits.

As mentioned above, *Acquisti and Gross* did the similar research for US SSN (Social Security Number) prediction from public data (Acquisti & Gross, 2009). As they stated, the identity number can be attacked mainly by two ways: infection by botnet for identity theft, and inferences from sharing data.

A bot is a computer that is infected with malware and specialized with malicious tools to attack other computers. A botnet is a group of compromised computers (bots) under the remote command and control of a malicious originator (botmaster) (Zeidanloo & Manaf, 2009). Recently, some researchers have started to pay their interests on botnet command and control in social networking, called SocialNetworkingBot (Kartalpe et al., 2010; Singh et al., 2013).

The workflow of SocialNetworkingBot is depicted in Fig. 12. A botnet will firstly send a request and access token to a user via social media. The user authenticates unintentionally the token keyword and secret string to join the Botnet. Botmaster can thus send commands (tweets) by specified keywords via a Command & Control (C&C) Server, and the C&C server launches various attacks to user, including identity theft, the user's personal information can therefore be leaked.

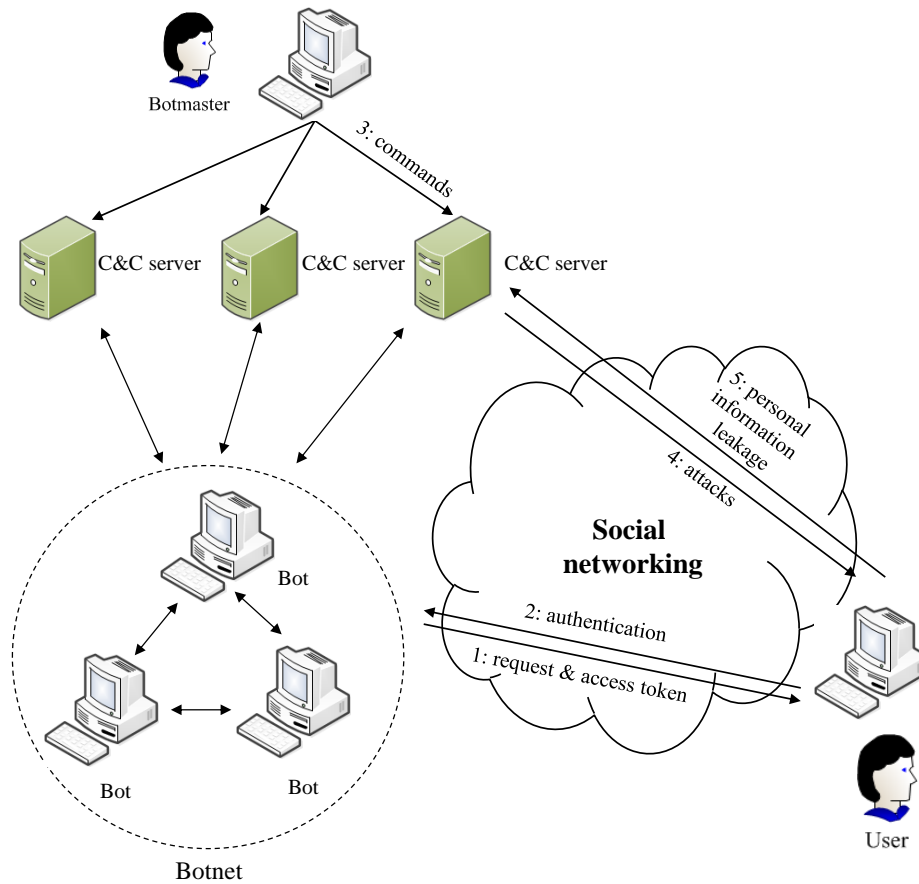


Fig. 12. Workflow of SocialNetworkingBot.

According to our analysis using EBD methodology presented above, “step2: authentication” is primary action to trigger the frauds (step 3-5). Therefore, the active conflict of “authentication” is the major challenge (conflict) of SocialNetworkingBot fraud prevention, which means how to prevent user to authenticate request and access token by downloading and installing malware. The knowledge of such prevention is shown in Table 11.

According to the generic reference model in Fig. 9, the proposed guidance can be categorized into four levels (shown in Fig. 13). The proposed guidance is generally in accordance with the proposed solutions from (Dhande, 2012), which are generated based on the observations of six case studies.

Table 11. Knowledge of prevention of user's authentication for request and access token (case study)

Descriptions	Action needed	Guidance
prevent user's authentication for request and access token	avoid malware installation by taking advantage of unintended vulnerabilities	<ul style="list-style-type: none"> ✓ establish policy to mitigate vulnerabilities ✓ keep all software up to date ✓ install antivirus software and firewall from a trusted source
	avoid tricks of malware installation	<ul style="list-style-type: none"> ✓ do not click on any unknown link ✓ do not use any third-party applications from untrusted sources ✓ do not download any files, movies, pictures from untrusted sources ✓ establish anti-malware policy
	avoid account breaking	<ul style="list-style-type: none"> ✓ use a strong and robust password ✓ provide a strict API for the access of system ✓ install antispyware software from a trusted source ✓ user external flash driver cautiously

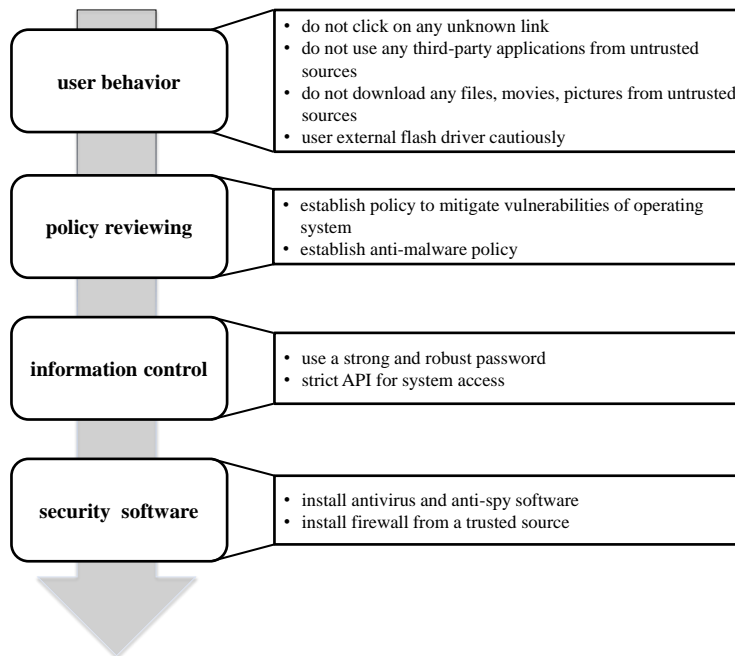


Fig. 13. Reference model for SocialNetworkingBot prevention (case study).

Next, we shift our focus on the illustration of the proposed conceptual model in Fig. 11 to prevent information leakage by inferences. In this case, the targeted personal information to infer I_p is Resident Identification Card Number. As mentioned in Eq. (8), the main idea is to detect and then reduce the risk of implicit information leakage measured by personal information sharing, and thus select the less risky one to share. In this case, we assume that the initial knowledge of inferrer is the gender of the cardholder, which can only infer 1 digit over 18 (risk=1/18) caused by inferences. Table 12 shows the scenario of risk analysis of sharing information in social media.

Table 12. Risk analysis of information sharing (case study)

Profile available information $K_0(I_p)$	Knowledge by inferences before information sharing $(K_0+K_s)(I_p)$	Sharing information (I_s)	Added knowledge by inferences after information sharing $(K_0+K_s)^*(I_p)$	Risk $(r_{s,j})$
gender	the last digit of sequential code	city of birth	first four digits of registered administrative division code	5/18
gender, city of birth	the last digit of sequential code, first four digits of administrative division code	location of primary school	last two digits of registered administrative division code, since the entrance of primary school is based on civil registry in accordance with administrative division	7/18
gender, city of birth, location of primary school	administrative division code, last digit of sequential code	birthday	digits (MMDD) of date of birth code	11/18
gender, city of birth, location of primary school, birthday	administrative division code, birthday digits, last digit of sequential code	age	digits (YYYY) of date of birth code	15/18

In Next, we shift our focus on the illustration of the proposed conceptual model in Fig. 11 to prevent information leakage by inferences. In this case, the targeted personal information to infer I_p is Resident Identification Card Number. As mentioned in Eq. (8), the main idea is to detect and then reduce the risk of implicit information leakage measured by personal information sharing, and thus select the less risky one to share. In this case, we assume that the initial knowledge of inferrer is the gender of the cardholder, which can only infer 1 digit over 18 (risk=1/18) caused by inferences. Table 12 shows the scenario of risk analysis of sharing information in social media.

Table 12, we can notice that, along with the sharing information city of birth, location of primary school, birthday as well as age, the risk of ID card number prediction increases significantly. Moreover, by utilization of big data analytics techniques, it has higher possibilities to predict more digits of Resident ID card number (Acquisti & Gross, 2009).

Being aware of the great risks of ID card stealing and abuse by above ways, the government of PRC has issued the second generation of Residence Identity Card since 2004 (CHN103755.E, 2011), which embedded a digital microchip containing cardholder information, such as name, sex, date of birth. The embedded microchip can provide only partial information to a specific card reader (Tiejun et al., 2010) according to the level of privacy. In 2011, government decided to include fingerprint data in the second generation of ID card. The law of Resident identity cards has been reviewed in a bid to combat counterfeiting (XinhuaNet, 2011).

7. Conclusion

Social networking service becomes a fashion means of communication in our life, therefore many implications caused by them have been discovered, analysed and studied currently. One of the major

topics concerning social networking service is the privacy leakage that they usually imply. Existing literatures attempt to deal with such issue using computer security technology. However, few researchers have proposed a holistic framework for privacy protection from user perspective. In this background, this paper not only focused on many different sorts of frauds that can occur through direct attacks or indirect inferences, but also suggested coherent guidelines for the users facing on identified challenges. A reference model of privacy leakage prevention was proposed using environment-based design (EBD) methodology. This reference model includes two sub-models, one is used for explicit privacy protection from direct attacks, and another is used for implicit privacy protection from inferences. For future developments, we will validate and enhance our proposed models through various case studies, and develop detailed algorithms to deal with the large-scaled privacy information leakage implied in social media.

Acknowledgments

Caue Bernardi Bispo's research work is supported by international exchange program Science without Borders (SwB), National Counsel of Technological and Scientific Development (CNPq) in partnership with the Canadian Bureau for International Education (CBIE). We also express our thanks to Mr. Ronaldo Gutierrez for his valuable comments to improve the quality of this paper.

References

- Acquisti, A. & Gross, R. (2009). Predicting Social Security numbers from public data. *Proceedings of the National academy of sciences*, 106(27), 10975-10980.
- Arachchilage, N., Love, S., & Scott, M. (2012). Designing a Mobile Game to Teach Conceptual Knowledge of Avoiding "Phishing Attacks". *International Journal for e-Learning Security*, 2(2), 127-132.
- Boyd, D. (2006). Friendster lost steam. Is MySpace just a fad. *Apophenia Blog*, 21.
- Boyd, D. M. & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210-230.
- Cashion, J. & Bassiouni, M. (2011). Protocol for mitigating the risk of hijacking social networking sites. *7th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2011)*, 324-331.
- Chen, Z. Y. & Zeng, Y. (2006). Classification of product requirements based on product environment. *Concurrent Engineering*, 14(3), 219-230.
- CHN103755.E. (2011) China: Appearance of the second-generation Resident Identity Card Research Directorate, Immigration and Refugee Board of Canada, Ottawa.
- Deng, X., Huet, G., Tan, S., & Fortin, C. (2012). Product decomposition using design structure matrix for intellectual property protection in supply chain outsourcing. *Computers in Industry*, 63(6), 632-641.
- Dhande, N. C. (2012). Botnet Prevention Strategies for Social Network users: Cases and Remedies. *International Journal of Informatics and Communication Technology*, 2(1), 46-50.
- Falahi, K. A., Atif, Y., & Elnaffar, S. (2010). Social networks: Challenges and new opportunities. *Proceedings of the 2010 IEEE/ACM International Conference on Green Computing and Communications & Cyber, Physical and Social Computing*, 804-808.
- FCAC. (2013). Online fraud: Social networking *Financial Consumer Agency of Canada*. Retrieved from <http://www.fcac-acfc.gc.ca/eng/forConsumers/topics/fraud/Pages/OnlineFr-Fraudeen-0.aspx>
- Goldberg, S. (2007). Analysis: Friendster is doing just fine. *Digital Media Wire*. Retrieved July, 30, 2007.
- Gross, R. & Acquisti, A. (2005). Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, 71-80.
- He, J., Chu, W., & Liu, Z. (2006). Inferring privacy information from social networks *Intelligence and Security Informatics* (pp. 154-165): Springer.

- Kartalpepe, E., Morales, J. A., Xu, S., & Sandhu, R. (2010). Social network-based botnet command-and-control: emerging threats and countermeasures. *Applied Cryptography and Network Security*, 511-528.
- Li, M., Cao, N., Yu, S., & Lou, W. (2011). Findu: Privacy-preserving personal profile matching in mobile social networks. *The 30th IEEE International Conference on Computer Communications*, 2435-2443.
- nextMEDIA. (2010). Social networks overview: Current trends and research challenges. *EU Commission Information Society and Media*. Retrieved from <http://cordis.europa.eu/fp7/ict/netmedia/docs/publications/social-networks.pdf>
- OASIS. (2006). Reference model for service oriented architecture 1.0. *OASIS SOA Technical Committee*.
- Puttaswamy, K. P. N. & Zhao, B. Y. (2010). Preserving privacy in location-based mobile social applications. *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*, 1-6.
- Shehab, M., Squicciarini, A., Ahn, G., & Kokkinou, I. (2012). Access control for online social networks third party applications. *Computers & Security* 31, 897-911.
- Shyng, J. Y., Shieh, H. M., & Tzeng, G. H. (2010). An integration method combining Rough Set Theory with formal concept analysis for personal investment portfolios. *Knowledge-Based Systems*, 23(6), 586-597.
- Singh, A., A.H., T., Ross, K., & Stamp, M. (2013). Social Networking for Botnet Command and Control. *International Journal of Computer Network and Information Security*, 6, 11-17.
- Tang, X. & Yang, C. C. (2012). Social network integration and analysis using a generalization and probabilistic approach for privacy preservation. *Security Informatics*, 1(1), 1-14.
- Tiejun, P., Chunlei, X., Leina, Z., Yufeng, H., & Lingbin, B. (2010). ONE-CARD system based on the second generation ID card in China. *2010 International Conference on E-Business and E-Government (ICEE)* 108-111.
- Wang, M. & Zeng, Y. (2009). Asking the right questions to elicit product requirements. *International Journal of Computer Integrated Manufacturing*, 22(4), 283-298.
- Wang, M., Zeng, Y., Chen, L., & Eberlein, A. (2013). An algorithm for transforming design text ROM diagram into FBS model. *Computers in Industry (in press)*.
- Ware, W. H. (1967). Security and privacy in computer systems. *Proceedings of the April 18-20, 1967, spring joint computer conference*, 279-282.
- Wartofsky, M. W. (1979). *Models: Representation and the scientific understanding* (Vol. 129): Springer.
- Xie, Y., Yu, F., Abadi, M., Gillum, E. C., Huang, J., Mao, Z. M., Walter, J. D., & Vitaldevara, K. (2013). Using social graphs to combat malicious attacks: US Patent 8,434,150.
- XinhuaNet. (2011). Chinese lawmakers consider adding fingerprint in resident ID cards.
- Xu, W., Zhou, X., & Li, L. (2008). Inferring privacy information via social relations. *Data Engineering Workshop, 2008. ICDEW 2008. IEEE 24th International Conference on*, 525-530.
- Zeidanloo, H. R. & Manaf, A. A. (2009). Botnet command and control mechanisms. *Second International Conference on Computer and Electrical Engineering, 2009 (ICCEE'09)* 564-568.
- Zeng, Y. (2004). Environment-based formulation of design problem. *Transactions of the SDPS: Journal of Integrated Design and Process Science*, 8(4), 45-63.
- Zeng, Y. (2008). Recursive Object Model (ROM): modeling of linguistic information in engineering design. *Computers in Industry*, 59(6), 612-625.
- Zeng, Y. (2011). Environment-based design. *Proceedings of the ASME 2011 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference (IDETC/CIE 2011)*, DETC2011-48263.
- Zeng, Y. (2014). *Environment-based design*. Berlin: Springer (to appear).
- Zeng, Y. & Cheng, G. D. (1991). On the logic of design. *Design Studies*, 12(3), 137-141.
- Zeng, Y., Wang, L., Deng, X., Cao, X., & Khundker, N. (2012). Secure collaboration in global design and supply chain environment: problem analysis and literature review. *Computers in Industry*, 63(6), 545-556.

- Zhang, D. Y., Cao, X., Wang, L., & Zeng, Y. (2012). Mitigating the risk of information leakage in a two-level supply chain through optimal supplier selection. *Journal of Intelligent Manufacturing*, 23(4), 1351-1364.
- Zhang, D. Y., Zeng, Y., Wang, L., Li, H., & Geng, Y. (2011). Modeling and evaluating information leakage caused by inferences in supply chains. *Computers in Industry*, 62(3), 351-363.
- Zheleva, E., Terzi, E., & Getoor, L. (2012). Privacy in social networks. *Synthesis Lectures on Data Mining and Knowledge Discovery*, 3(1), 1-85.

Author Biographies

Xiaoguang Deng is a Research Associate from Concordia Institute for Information Systems Engineering at Concordia University, Canada. He received his Ph.D. degree in Industrial Information Systems from University Science and Technology of Lille 1, France. His research interests address visual analytics, product and service design, and supply chain management.

Caue Bernardi Bispo is an undergraduate student in Electrical Engineering from University of São Paulo, Brazil. He was exchanged student and research trainee at Concordia Institute at Concordia University, Canada. His research interests include risk management, social networking, supply chain management.

Yong Zeng is Canada Research Chair in Design Science (Tire II) and professor from Concordia Institute for Information Systems Engineering at Concordia University, Canada. His research is focused on the modelling and computer support of creative design activities. He and his research group have been approaching the research from philosophical, mathematical, linguistic, neurocognitive, and computational perspectives. His research results, which range from the science of design, requirements engineering, human factors engineering, computer-aided product development, product lifecycle management, finite element modelling, to design and supply chain management, have been applied to manufacturing, pharmaceutical, entertainment, construction industries, and municipality.

Copyright of Journal of Integrated Design & Process Science is the property of IOS Press and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.