Misuse case techniques for mobile privacy

Inah Omoronyia[1], Mazeiar Salehie[1], Raian Ali[1], Haruhiko Kaiya[3] and Bashar Nuseibeh[1, 2]

[1] Lero – The Irish Software Engineering Research Centre, Uni. of Limerick, Ireland
[2] Department of Computing, The Open University, UK
[3] Shinshu University, Department of Information Engineering, Nagano, Japan

1 Introduction

Functional use cases are a popular technique that focus on the users of a system, not the system itself, thus enabling real system needs to be considered early [1]. *Misuse cases* extend use cases to describe undesirable or unacceptable use of a system. Misuse cases have also been shown to be an effective approach for eliciting security and safety requirements of software systems [2]. However, while privacy and security are related concepts, their objectives are sometimes contradictory. For instance, while surveillance might be a means to achieve security, it may also be regarded as invasive of one's privacy. In general, security analysis techniques are not sufficient to reveal privacy issues – while security can be a cross-cutting quality of a system irrespective of an individual or associated group, privacy is inherently personal to a user of a system or the group in which the user belongs.

We are motivated by the view that privacy analysis can benefit from utilising misuse case technique as a means to identify system usage that might threaten privacy. Our aim is to understand the specific implications of using misuse case techniques for eliciting privacy requirements of mobile system users. We focus on mobile applications, as mobility is an increasing common characteristic of systems and their users. We suggest that misuse cases can potentially help to better model contextual aspects of mobile privacy, such as malicious users intending to reveal privacy information of stakeholder. In this paper, we present an overview of the applicability and associated challenges of deploying misuse case techniques for the analysis of privacy sensitive problems. First, we introduce a privacy misuse case model. Using a mobile application scenario, we then illustrate and discuss possible extensions to general misuse cases that can help in the realisation of such model.

2 Misuse case model for privacy

The steps for discovering and eliciting security requirements with misuse cases were proposed by Gottorm and Opdahl [2]. To extend these steps to eliciting privacy requirements, there is a need to recognize that privacy issues are highly contextual and contingent. As suggested by Altman [6], privacy is actually a condition of relative inaccessibility involving a *dialectic and dynamic boundary regulation process.* This privacy regulation process varies depending on specific times, places, associated audience and other contextual factors. Our aim is to capture this notion of privacy in

misuse cases by highlighting the steps for eliciting security requirements and the corresponding notion of steps for eliciting privacy requirements with misuse cases.

The first step for the security misuse case process involves the identification of critical assets. Corresponding assets in privacy are typically one or more attributes related to the user of the system which if disclosed can result in privacy violation (the term attribute here is loosely used to generally refer to data, information or other references about a user that can be collected in a device and subsequently processed or disseminated). Furthermore, since the privacy of an attribute depends on a number of contextual factors, it is also important to identify the circumstance surrounding the designation of a specific attribute as being private. For instance, the location of a user in a mobile environment might be private, whereas the same user's name is not private. Additionally, the location of the user might only be private in regions where crime-level is known to be high. Ultimately, the responsibility of preserving a private asset can fall to the user of the system or a third party system (data holder), or both.

The second step for security misuse case process involves the definition of a security goal. This step is normally aided by a standard typology of security goals such as confidentiality, integrity, availability, authenticity and non-repudiation [4]. While such goal aiding standard does not yet exist for privacy, existing research such as the taxonomy of privacy proposed by Solove [3] can act as a starting point in understanding a privacy objective. Solove's taxonomy accounts for privacy problems that have achieved a significant degree of social recognition. The taxonomy also cuts across a basic group of activities such as collecting, processing and disseminating of personal attributes of a user that can be harmful. Based on this taxonomy, a privacy objective will be an endeavour to avoid activities that result in privacy problems such as unsolicited surveillance, aggregation, decisional interference, inappropriate disclosure, appropriation, to mention a few.

The identification of threats and risk analysis are the third and fourth step for security misuse case process. Threat identification for privacy is similar to that proposed by Guttorm and Opdhal for security, and involves identifying misusers that may intentionally violate the privacy of the user of the system and the sequence of actions that may result in such violation. The core challenge here is while there are standard techniques for risk analysis and costing from the view point of security [5], there are none known for privacy. The final step in the application of misuse case for privacy is also similar to security, and involves the definition of privacy requirements that mitigates the identified threats to achieving a privacy objective.

Table 1 is a summary of corresponding considerations for privacy requirements across each of the security misuse case steps. Figure 1 is also the representation of privacy misuse case interrelation with other use case concepts. The misuser is the actor that threatens privacy. A privacy misuse case identifies the private attributes of the user; defines the circumstance surrounding the privacy of user attribute; and

Table 1

Steps for eliciting security requirements with misuse cases:	***Corresponding considerations for using misuse cases for eliciting privacy requirements***
1. Identify the critical assets.	1. Identify the private attributes of the user 2. Define the circumstance surrounding the privacy of user attributes.
2. Define security goals.	3. Define privacy objectives
3. Identify threats	4. Identify threats
4. Identify and analyse risks	5. Identify and analyse risks
5. Define security requirement	6. Define privacy requirements

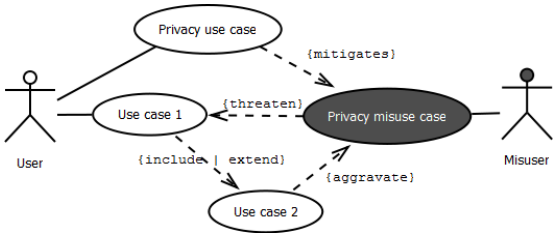

Figure 1 Privacy misuse case interrelation with stakeholders, functional and privacy use case

highlights the sequence of actions that a misuser can perform within the identified circumstance for which if allowed to complete will ultimately violate the privacy of the user. Finally, a privacy use case identifies the privacy requirement necessary to mitigate a privacy misuse case.

3 Illustration and discussion

An illustration of privacy misuse cases for a smart parking system is shown in figure 2. The system operates based on a participatory sensing technique [7] that uses the real-time location of cars in parking lots and of drivers to indicate the availability of free parking spaces. For this system, 'arrives parking lot', 'departs parking lot' and 'views empty parking space' are the functional use cases that a driver interacts with in order to achieve the goal of the system. Inappropriate disclosure is a typical privacy misuse case where a misuser (fake driver) attempts to subvert the system so that a user (driver) will disclose his/her parking location in a manner that can put the user at risk of blackmail, appropriation or even misjudgement.

The details of inappropriate disclosure privacy misuse case are further illustrated by the template shown in figure 3. The attributes in non-italics represent attributes from the original misuse case introduced by Sindre and Opdahl [2]. The steps that a fake driver will initiate in order to violate a driver's privacy are as shown in the basic path of events. The mitigation points attribute identifies those actions in a basic or alternative path where the misuse of an asset can be mitigated. For privacy, understanding the perspective for which an asset can be misused and hence mitigated requires: firstly, knowledge of the attribute of the user that is private; and secondly, the circumstances surrounding the designation of a specific attribute as being private (see section 2). For instance, there might be no need for the driver to negotiate her privacy by selectively disclosing her location if she is familiar with every driver requesting an empty parking space. We have introduced two new properties to the misuse case template as proposed in [2] (in *italics* figure 3) that highlight this contextual property of privacy. The *private node* attribute highlights the information or data of concern, which if divulged can result in a privacy violation, while the *circumstance* attribute captures the context within which an event in a basic or alternative path of a use case might impact on the identified private node. These two attributes are subsequently used to consider the necessary mitigation for a privacy threatening event. Typically, each mitigation point can give rise to a privacy use case that provides insights about the privacy requirements that mitigate a misuse case.

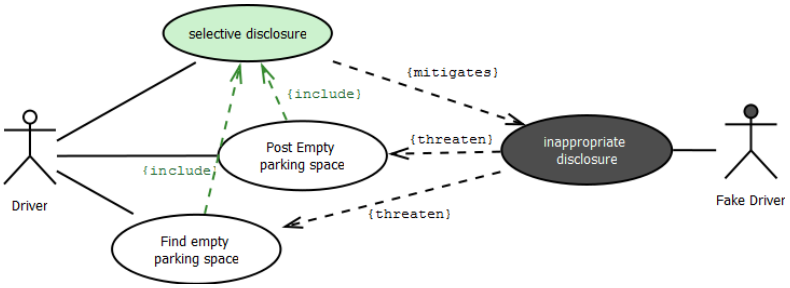

Figure 2 Smart parking space misuse case example

Attribute	Description	
Misuse Case Name:	Inappropriate disclosure	
Basic path of events:	1) Fake driver arrives city centre 2) Fake driver sends request for notification of available near-by parking spaces 3) Fake driver receives notification of available near-by parking spaces 4) Fake driver views details of available near-by parking spaces 5) Fake driver arrives at notified empty parking space	
Alternative path:	[…]	
Private node:	Location	
Circumstance:	**C1:**	At action 1, posting driver arrives at a car parking location known for high crime and parking abuse.
	C2:	At action 2, requesting driver (fake driver) is not a member of predefined group
	…	
Mitigation points:	**MP1:**	At action 2, Drivers are able to change their preference to only broadcast empty parking spaces to only members of a predefined group (in this case, drivers will be broadcasting to a cohort of drivers they are familiar with).
	MP2:	At action 4, Drivers are able to broadcast in car parks located in high crime regions using pseudonyms only understood by group members (Prevents fake unknown drivers from understanding drivers postings).
	MP3:	At action 5, Drivers are able to change their preference to broadcast details of empty parking space using dynamic encryption that expires after a specified time (prevents the fake driver from holding a drivers details for longer than necessary).
Extension Points:	[…]	
Triggers:	Driver/departs arrives parking lot	
Assumptions:	The fake driver is able to connect to the mobile network via smart parking device.	
Preconditions:	The fake driver is able to send a request for notification of available near-by parking spaces	
Mitigation guarantee:	The driver is able to selectively disclose available parking spaces through the smart parking device	

Figure 3 Smart parking space misuse case template description with privacy enabling extensions

4 Conclusion and further work

This paper presents preliminary research that exploits the functional properties of use and misuse cases to describe privacy requirements of a system user. We have described a privacy misuse case model by highlighting the contextual properties that uniquely characterize a privacy misuse case. This has been achieved by using the steps for eliciting security requirements and showing the corresponding steps for eliciting privacy requirements. Using a simple illustration in a mobile application scenario, we argued for the introduction of private node and circumstance as two new attributes that help highlight these contextual factors in misuse case templates. Future work will focus on understanding the impact of our use case extensions on the use case analysis of privacy aware mobile systems.

Acknowledgement: Supported, in part, by Science Foundation Ireland grant 03/CE2/I303_1 and the EPSRC PRiMMA project (EP/F024037/1).

References

1. A. Cockburn (2001). Writing Effective Use Cases. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc. ISBN 0-201-70225-8.
2. Guttorm Sindre and Andreas L. Opdahl. 2005. Eliciting security requirements with misuse cases. Requir. Eng. 10, 1 (January 2005), 34-44.
3. D. J. Solove, Understanding Privacy: Harvard Uni Press, 2008.
4. CCIMB (1999) Common criteria for information technology security evaluation. Technical report, CCIMB-99–031, Common Criteria Implementation Board
5. Devanbu PT, Stubblebine S (2000) Software engineering for security: a roadmap. In: Proc. of ICSE 2000, future of software engineering track, Limerick, Ireland
6. I. Altman, Privacy regulation: culturally universal or culturally specific? Journal of Social Issues, 33 (3), 66-84. 1977.
7. J. Burke , D. Estrin , M. Hansen , A. Parker , N. Ramanathan , S. Reddy , M. B. Srivastava ., Participatory sensing, in WSW'06 , ACM Sensys. 2006, Colorado, USA.