Driving Privacy Controls with Social Context

Chris Smith and Aad van Moorsel
Abstract

Mobile applications frequently gather, use and share our personal information. To protect our privacy, any use of our personal information by these applications should ideally be controlled in a manner which is consistent with our specific privacy attitudes. This article takes the premise that such attitudes are determined by the social context in which the gathering, use and sharing of personal information takes place. Based on this observation, a novel approach to privacy controls is introduced which is driven by social context.
Bibliographical details

SMITH, C., VAN MOORSEL, A.

Driving Privacy Controls with Social Context
[By] C. Smith, A. van Moorsel

(Newcastle University, Computing Science, Technical Report Series, No. CS-TR-1316)

Added entries

NEWCASTLE UNIVERSITY

Abstract

Mobile applications frequently gather, use and share our personal information. To protect our privacy, any use of our personal information by these applications should ideally be controlled in a manner which is consistent with our specific privacy attitudes. This article takes the premise that such attitudes are determined by the social context in which the gathering, use and sharing of personal information takes place. Based on this observation, a novel approach to privacy controls is introduced which is driven by social context.

About the authors

Chris Smith is a Research Associate in the School of Computing Science. His research focuses on the trust, security and privacy implications of digital technologies, taking both a technical and social perspective. He completed his PhD in Computing Science at Newcastle University in 2010.

Aad van Moorsel is a Professor in Distributed Systems at the School of Computing Science in Newcastle University. His group conducts research in security, privacy and trust. Almost all of the group's research contains elements of quantification, be it through system measurement, predictive modelling or on-line adaptation. Aad worked in industry from 1996 until 2003, first as a researcher at Bell Labs/Lucent Technologies in Murray Hill and then as a research manager at Hewlett-Packard Labs in Palo Alto, both in the United States. He got his PhD in computer science from Universiteit Twente in The Netherlands (1993) and has a Masters in mathematics from Universiteit Leiden, also in The Netherlands. After finishing his PhD he was a postdoc at the University of Illinois at Urbana-Champaign, Illinois, USA, for two years. Aad has worked in a variety of areas, from performance modelling to systems management, web services and grid computing. Most recently, he was responsible for HP's research in web and grid services, and worked on the software strategy of the company.

Suggested keywords

PRIVACY
SECURITY
SOCIAL CONTEXT
INSTITUTIONS
Driving Privacy Controls With Social Context

Chris Smith and Aad van Moorsel

Abstract—Mobile applications frequently gather, use and share our personal information. To protect our privacy, any use of our personal information by these applications should ideally be controlled in a manner which is consistent with our specific privacy attitudes. This article takes the premise that such attitudes are determined by the social context in which the gathering, use and sharing of personal information takes place. Based on this observation, a novel approach to privacy controls is introduced which is driven by social context.

Index Terms—

1 INTRODUCTION

Increasingly, mobile applications on smartphones and tablets are being used to support our everyday activities in a variety of different domains, including retail, healthcare and finance. These mobile applications frequently gather, use and share personal information, such as our current location, medical conditions or purchasing habits, for a wide range of purposes, including personalized functionality and targeted advertising. For example, healthcare applications such as NHS Direct [1] and iTriage [2] gather and use our medical symptoms to provide a medical diagnosis and recommend appropriate treatments.

As the integration of different mobile applications into our everyday activities grows, so is the scale and frequency with which our personal information is being gathered, used and shared by these applications. This leaves us vulnerable to applications which use our personal information for purposes which we do not consider acceptable, and that we would wish to prevent. For example, the sharing of our medical symptoms by a healthcare application with a retail application for the purpose of targeted advertising can have significant social, monetary and physical costs, exposing us to threats such as discrimination, identity theft and stalking [3].

In order to reduce our vulnerability to privacy violations, we need to control “whether, when, and to whom personal information is released” [4] by these applications in accordance with our specific privacy attitudes [5]. Often though, it is the attitudes of the application developer or application marketplace, rather than our own, which determine how our personal information is controlled by such applications. For example, the developer of a healthcare application may consider the sharing of medical symptoms with a retail application for the purpose of targeted advertising to be acceptable, which may contrast with our own privacy attitudes. In such cases, it should be our attitudes that prevail, and ultimately determine the manner in which our personal information is controlled.

This article takes the premise that our privacy attitudes are determined by the social context in which interactions involving our personal information take place [6]. This social context frames an interaction in terms of a flow of information between entities which assume social roles as part of particular social activity. For example, an interaction might involve the flow of Medical Symptom information between entities in the roles of Doctor and Patient as part of a Diagnosis activity. Within a particular social context, there are social “institutions” [7], [8] such as cultures, norms or laws. These institutions represent sets of rules which are defined and enforced on a societal level, and which constrain the purposes for which the
gathering, using and sharing of certain personal information is deemed acceptable by that society. For example, norms and laws exist to stipulate those purposes for which the sharing of Medical Symptoms by a Doctor with a Third Party is acceptable.

Existing mobile application platforms, such as Google Android [9], Apple iOS [10] and Windows Phone [11], provide certain mechanisms to control the use of our personal information by mobile applications. Unfortunately, our information may still be gathered, used and shared by applications with greater frequency, on a larger scale, and in more depth than is consistent with our privacy attitudes [12]. We believe that this indicates a shortcoming in the ability of such mechanisms to enable appropriate control over our personal information. Instead, these mechanisms often emphasize the attitudes of application developers or application marketplaces over our own attitudes. These attitudes are likely to favor application functionality and the economic value of personal information over the protection of our privacy, and are therefore unlikely to be consistent with our own attitudes.

To address this problem, we describe a novel approach to privacy controls for mobile applications which is driven by social context. This approach enables the interaction between mobile applications to be characterized by social context, and the flow of personal information between applications to be controlled using applicable social institutions. This leads to privacy controls which are consistent with our specific privacy attitudes, and reduces our vulnerability to privacy violations. Moreover, it leads to privacy controls which can be generalized across large numbers of mobile applications, given we may have multiple applications which interact within analogous social contexts, and therefore be subject to analogous social institutions. Finally, the commonality amongst individuals in a society can be exploited, enabling individuals with common cultures, norms or laws to have pre-configured privacy controls which are in accordance with these institutions, reducing the knowledge, time and rationality [13] required for configuration.

2 Privacy Controls

Mobile application platforms provide the execution environment for applications on a mobile device. These platforms provide mechanisms which can be used to control the use of our personal information by mobile applications on our smartphones and tablets. They provide authentication mechanisms which associate an identity with each mobile application; determining the “to whom” [4] of privacy controls. Additionally, they provide authorization mechanisms which associate with these different identities the ability to gather, use and share personal information, determining the “whether” [4] of privacy controls. These associations typically remain fixed over time, such that the “when” [4] of privacy controls is either always or never. Together, these authentication and authorization mechanisms determine the different interactions which can be performed between mobile applications, and the personal information which can be gathered, used and shared as part of these interactions.

Unfortunately, the mechanisms provided by existing mobile application platforms often lead to privacy controls which are inconsistent with our specific privacy attitudes. For example, there have been a number of recent cases in which mobile applications have utilized our personal information without consent and for undefined purposes (see [14], [15]). Such cases highlight the fact that our personal information is often gathered, used and shared by mobile applications with greater frequency, on a larger scale and in more depth than our attitudes would determine, and used for purposes which we do not consider acceptable.

We argue that a key determinant of such inconsistencies is that the authentication and authorization mechanisms used by existing platforms focus on the functionality of applications, and are driven by technical context. As such, the vocabulary used to define and enforce control over our personal information is focused upon controlling an application’s access to, and manipulation of, shared computational, storage and network resources, and use of shared hardware, such as microphones and cameras. Each mobile application is uniquely
identified with some identifier (such as a cryptographic key), and this identifier is associated with a set of permissions defining access to, and manipulation of shared resources, and use of shared hardware (see [16]). Whilst such permissions implicitly provide control over our personal information, they do not enable our specific attitudes to privacy to be appropriately expressed. Moreover, these permissions are often defined by application developers and marketplaces, and as such focus principally on functionality rather than our privacy.

For example, a retail application may be permitted to access and manipulate the storage resource of a healthcare application. Whilst there may be purposes for which such access and manipulation may be acceptable, the permission does not enable us to express these attitudes at an appropriate level of granularity. The permission does not appropriately express what personal information is released by the healthcare application to the retail application, or when this information is released. Therefore, whilst there is control over personal information, the manner in which the controls are defined and enforced are insufficient to ensure their consistency with our specific privacy attitudes.

By driving privacy controls with technical context, existing platforms provide significant barriers to realizing privacy controls which are consistent with our specific attitudes. Whilst the permissions determine “to whom” information is released, they do not enable sufficient control over the “what” and “when”. Moreover, this manner of defining privacy controls seems unnatural, and inconsistent with our “mental model” [17] of privacy. We do not think of control over our personal information in such a technical manner, where we are required to analyze the implications for the gathering, use and sharing of our personal information which emerges from the technical capabilities associated with applications. Quite simply, we usually lack the necessary knowledge, time and rationality [13] to do so, particularly given the increasing number of mobile applications for which this would be required.

3 DRIVING PRIVACY CONTROLS WITH SOCIAL CONTEXT

To address this problem with existing approaches to privacy controls, we describe a novel approach which is driven by social context. Very broadly, context can be used to refer to any information that can be used to characterize the situation of an entity [18]. Building on this definition, social context can be used to refer to any information that characterizes the social situation of an entity, such as social structure and social relations between entities. In our case, the entities are mobile applications, and we wish to describe the social situation in which these applications interact. This enables us to exert control over our personal information based upon this social context. For a given interaction, the social context can be defined using the following concepts:

- **Domain**: A domain is set of specific roles, activities, information and institutions. For example, the Healthcare domain.
- **Role**: An entity with responsibility for performing certain activities. For example, Patient and Doctor in the Healthcare domain.
- **Activity**: One or more actions of gathering, using or sharing information to achieve an outcome. For example, Diagnosis and Referral in the Healthcare domain.
- **Information**: A piece of data with associated semantics. For example, Medical Symptoms or Medications in the Healthcare domain.
- **Institutions**: A set of rules over the gathering, use and sharing of our information by a certain role for a certain activity.

Using our approach, the authentication and authorization mechanisms within the application platform, which control our personal information are driven by this social
context. The concepts above provide the vocabulary with which these controls are defined and enforced. For a given interaction between mobile applications, each application is placed into a role within a certain domain, and the interaction between these roles is placed into an activity involving certain (personal) information. The acceptability of the flow of personal information between these mobile applications, and therefore our specific privacy attitudes, are then determined based upon the social institutions which are applicable to that social context. For example, there may exist an applicable law which states that the sharing of Medical Symptoms with a Third Party by a Doctor for use in targeted advertising is not acceptable.

Fig. 1. Driving Privacy Controls With Social Context

Figure 1 provides an illustration our approach. In this case, a healthcare application, myHealth, is placed into the role of Doctor, and a retail application, myShopping, is placed into the role of Third Party. Both of these roles are defined within the Healthcare domain, as is the Marketing activity into which the interaction between these two roles is placed. This interaction involves the sharing of Weight information between the Doctor and the Third Party, and there exist applicable social institutions in the Healthcare domain, which determine the acceptability of this sharing.

We now look in more detail at how the processes of authentication and authorization are carried out in our approach.

3.1 Authentication

In order to place interactions between applications into a social context, we must map observable attributes of those applications, data and interactions to appropriate concepts in the social context. For example, myHealth may be mapped to the role of Doctor through an observable digital certificate. The mapping of these attributes to social context requires domain knowledge. Such knowledge enables us to determine which attributes are relevant in denoting certain roles, activities and information, and to attest to the veracity of these attributes can be attested.

Domain knowledge can be obtained from a variety of different sources, including our own experiences within a domain. Yet, since our experience across different domains is inherently limited, it is more likely that such knowledge would be provided by authorities in particular domains for widespread usage. This mitigates any requirement for each individual to possess such knowledge, or spend the time and effort necessary to obtain such knowledge. For example, the National Health Service [19] is an authority which could provide such knowledge for the Healthcare domain. This knowledge can also be encoded within the application platform, such that authentication can take place without our involvement. Instead of prompting us for a manual decision about the mapping in every interaction, the platform can use encoded knowledge to automatically perform the mapping. This is particularly relevant given the high number of interactions which are likely to take place between applications.

In performing this authentication process, ambiguity may be encountered. This ambiguity arises from the ability of applications to assume a number of different roles, and perform
different activities in different domains. For example, an interaction may be performed between two mobile applications which hold the roles of Doctor and Teacher, and Patient and Student respectively. It should be clear from the authentication which roles are assumed by these applications in a specific interaction. This is likely to require use of the specific activity and information involved in the interaction. For example, if the information is Medical Symptoms, then it is likely that a Diagnosis activity is taking place, and therefore that the first application assumes the role of Doctor and the second application will assume the role of Patient.

3.2 Authorization

After placing an interaction between applications into a social context through the authentication process, our attitudes towards the gathering, use and sharing within this interaction must be determined, and control exerted over our personal information appropriately. As we have previously mentioned, we take the premise that our attitudes are determined by the social institutions which apply to the specific context. There are a number of different types of social institutions which can define rules over the acceptable gathering, use and sharing of information in a particular social context [8]:

- **Cultures**: Controls which are implicitly defined and self-enforcing, e.g. public greetings such as sharing your full name and affiliation when introducing yourself to a colleague.

- **Norms**: Controls which are defined within certifications and accreditations, and enforced by morality, e.g. codes of conduct defined by the General Medical Council for the Healthcare domain.

- **Laws**: Controls which are defined within formal statutes and enforced by formal sanctions, e.g. the Data Protection Act 1998 defined by the UK Government.

Such institutions represent privacy controls defined and enforced at the societal level, and represent the convergence of individual attitudes within society on a certain collective attitude. For example, individuals within a certain geographical region or of a certain religion may have a culture which means that their attitude to the gathering, use and sharing of their personal information is more restrictive.

In order to determine whether an interaction in a particular social context is consistent with our specific privacy attitudes, we must determine the applicable social institutions, and then verify that the interaction is consistent with those institutions. In a similar manner to domain knowledge, these social institutions can be defined by authorities within a given domain, such that individuals are not required to define these rules themselves from scratch. The cultures, norms and laws which are applicable for us in various domains can be pre-encoded by these authorities and integrated into the application platforms during an initialization process. For example, the National Health Service [19] could provide encoded norms applicable to the Healthcare domain, which provide a basis for controlling the flow of personal information between applications during interactions in that domain.

This process of determining when an application can gather, use and share our personal information is a process of authorization, where the social institutions provide the authorization rules. Based upon the applicable rules, the flow of personal information which is implied by an interaction is either permitted or denied. Given the number of applicable social institutions which may exist in a certain context, there may exist conflicts between the rules defined by these institutions. For example, the cultures applicable to a certain context may conflict with the laws in that context. In these situations, there must exist methods by which these conflicts can be appropriately resolved. For example, given a conflict between culture and law, the method may always apply the rules of law to avoid sanctions.
4 Realizing Privacy Controls Driven by Social Context

Our approach to privacy controls can be integrated into mobile application platforms through some changes to the existing authentication and authorization mechanisms. In our prototype, these mechanisms form part of a conventional policy-based management architecture. This architecture mediates the interaction between applications on the platform in order to control any flow of personal information in accordance with social context, and permitted or denied in accordance with social institutions.

Figure 2 illustrates the realization of these our approach as part of the application platform, and shows how control is exerted over a given interaction between myDiet and myShopping using social context as the driver. The authentication process begins when the myShopping application makes a request to the Policy Enforcement Point (PEP) to obtain certain information, X, from myHealth. This information is referenced by some addressing scheme such as a Universal Resource Indicator (URI). The PEP then forwards this request to the context handler, which takes the request for personal information and frames the interaction in a social context.

The key challenge is to be able to derive this social context from the attributes of the application, data and interaction. In order to do so, the context handler utilizes the Policy Information Point (PIP) component to perform the mapping from attributes to social context, using domain knowledge provided by authorities. In this case, the authorities are those in the Healthcare domain, such as the National Health Service or General Medical Council. For our approach to gain widespread use and acceptance, this domain knowledge must be encoded into application platforms during the setup of a device, reducing the knowledge and time required from ourselves.

The authorization process then begins when the context handler forwards the interaction, mapped to a social context, to the Policy Decision Point (PDP). The social context obtained from the context handler is then checked by the PDP to see if the gathering, use and sharing of personal information implied by the interaction is consistent with the relevant cultures, norms and laws. The cultures, norms and laws are encoded within one or more policies at the Policy Authoring Point (PAP). Again, in a similar manner to the domain knowledge, these policies can be loaded into the platform during setup of the device to provide relevant default privacy controls.

This yields a decision to permit or deny the interaction between the two applications which is forwarded to the PEP. In this case, the social institutions determine that myShopping is permitted to access Weight from myHealth. The PEP enforces the decision and forwards Weight from myHealth to myDiet. If it was determined that such sharing were not permitted, then the PEP would send an appropriate message to myDiet denying access to the information.

5 Discussion

Whilst we have demonstrated the applicability of an approach to privacy controls which is driven by social context, there are a number of key challenges which remain to be overcome before it can be realized in mainstream mobile application platforms. Firstly, each specific domain, such as healthcare and finance, requires its roles, activities, information and social institutions to be defined and encoded within the application platform. This requires that appropriate authorities in these domains exist and can provide such definitions. Secondly, better algorithms are required to characterize the social context of an interaction. Such algorithms will need to resolve any ambiguity and conflicts in this characterization. This may be ambiguity with regard to which social context is most relevant, when there are multiple feasible contexts, and also which social institutions are most relevant, when there are multiple feasible institutions.

Our approach to privacy controls has significant potential for improving the manner in which we control the gathering, use and sharing of our personal information by mobile
applications. Through our emphasis on social context, we base control on concepts which have real-world analogies. In doing so, our approach yields privacy controls which are easier to generalize across large numbers of mobile applications, and allows us to exploit commonality in terms of social institutions to provide applicable default controls, and reduce the need for us to unilaterally define and edit our privacy controls.

ACKNOWLEDGMENTS

This work was supported by the RCUK Digital Economy Programme grant EP/G066019/1 - SIDE: Social Inclusion through the Digital Economy.

REFERENCES


