JNIC2016

II Jornadas Nacionales de Investigación en Ciberseguridad

Granada 15–17 de junio

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL

ugr Universidad de Granada

Preserving the users' information privacy in location-based and context-aware solutions

Alberto Huertas Celdrán*, Manuel Gil Pérez*, Félix J. García Clemente†, and Gregorio Martínez Pérez*

* Departamento de Ingeniería de la Información y las Comunicaciones, University of Murcia, 30071 Murcia, Spain
Email: alberto.huertas@um.es, mgilperez@um.es, gregorio@um.es

† Departamento de Ingeniería y Tecnología de Computadores, University of Murcia, 30071 Murcia, Spain
Email: fgarcia@um.es

***Abstract*—Preserving the privacy of the users' information should be an essential requirement in information management systems. The mobility provided by context-aware services has increased the complexity of ensuring this challenge by allowing users to obtain, share, and provide information at anytime and anywhere. Addressing this challenge requires automatic mechanisms that allow users to control their information at real-time and on demand. In order to achieve these requirements, we proposed several context-aware solutions that allow users to manage the privacy of their information through policies. The privacy-policies managed by our solutions let users decide at real-time what, where, when, how, to whom, and at which level of precision they want to reveal their information.**

***Index Terms*—Context-awareness, location-based services, multi-context, privacy-policies**

Tipo de contribución: *Investigación publicada*

I. Introduction

Ensuring the privacy of the users' information is a challenge that sometimes is forgotten by systems that manage sensitive information. During the last decade, the complexity of protecting the users' information has been increased with the growth of mobile devices. In that sense, mobile devices have increased the number of applications offering context-aware services at anytime and anywhere. The location in a given environment about objects, devices, and people provides useful information in order to offer context-aware services.

An important number of context-aware solutions protect the users' information by using static privacy policies defined at set-up time. These solutions do not provide easy mechanisms to allow users to manage their privacy. Furthermore, static policies are not suitable for context-aware solutions, where users are constantly changing of environment. In that sense, users should be able to manage (grant or deny) the access to their information at real-time depending on their context and situation. In our opinion, context-aware solutions should allow users to control what information they want to release, who can access them, and in which contexts and situations they want to disclose such information.

In order to improve the preservation of the users' information, we have proposed several context-aware and privacy-preserving solutions that allow developing applications and services preserving the users' privacy. Specifically, users are able to manage their information through our solutions, which make use of privacy policies that consider the context or environment in which they are located. These policies allow users to share their information to the right users, at the right granularity, at the right place, and at the right time.

II. Privacy-preserving and context-aware solutions

During the last decade, several proposed works let users define privacy-preserving policies to control their personal information. The users' mobility has brought an evolution from proposals that protected the users' information in specific contexts (intra-context solutions), to systems that control the users' information considering multiple and independent context (multi-context solutions).

A. Intra-context solutions

Among the solutions that protect the information in intra-context scenarios, we proposed a framework called *SeCoMan* (Semantic web-based Context Management) [1] which provided support for developing context-aware applications preserving the users' privacy in a "Semantic oriented" Internet of Things (IoT) vision. Using SeCoMan, applications were able to collect the information generated by the IoT using a set of predefined queries. In order to cover the privacy of the users' information the queries provided by our solution considered the privacy-policies defined by the users previously. These policies allowed users to share their location to the right users, at the right granularity, at the right place, and at the right time. Specifically, using our solution users were able to hide their locations to other persons; mask their position with fictitious ones; establish the level of granularity at which they wanted to be located; and define the level of closeness accepted to be located. Fig. 1 shows the SeCoMan architecture, which is composed of three layers to allow framework actors to manage the resources and develop applications more efficiently. Note that the three layers that form the architecture are common for the proposals explained below.

B. Multi-context solutions

Multi-context solutions consider intra- and inter-context scenarios in order to protect the users' information when they move between independent contexts or environments. In that sense, CAPRIS (*Context-Aware PRIvacy-preserving system Supervised by users*) [2] was our first approximation to this kind of solutions. Specifically, CAPRIS was in charge of protecting the users' information in the context where they were. Using CAPRIS, users were able to decide at real-time what, where, when, how, to whom, and at which level of precision they want to release their information. This information can be the *space* in which they are located with different levels of granularity; the users' *personal information*

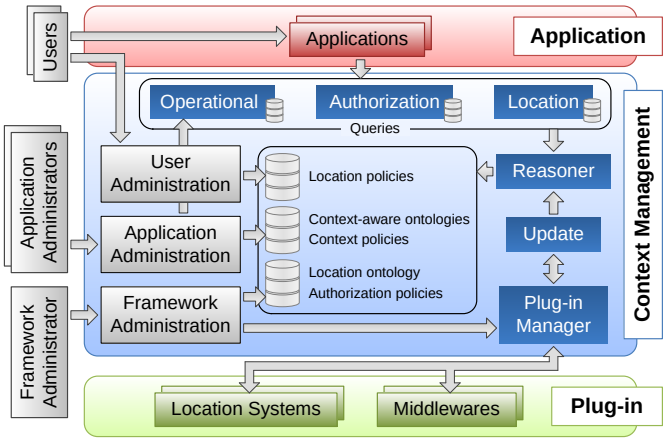

Fig. 1. Overview of the multi-layered architecture of our context-aware solution

with different levels of precision; the users' *activity*; and the information oriented to the *context* in which they are located. Using CAPRIS, users did not have to manage their privacy, but they just have to choose the most appropriate group of policies suggested by our solution considering their preferences.

Finally, MASTERY (Multicontext-Aware System That prEserves the useRs privacY) [3] is an evolution of CAPRIS that protects the privacy of the users' information in multi-context scenarios (intra- and inter-context scenarios) incorporating the user consent to reveal his/her personal information. To this end, MASTERY suggests to the users several sets of privacy-preserving and context-aware policies, called *profiles*. In order to protect their information, users just have to choose the most suitable profile according to their interests in the context where they are. Furthermore, using our solution users are able to modify the profiles adding, deleting, or modifying some of the policies that form the profiles. Finally, when the information is going to be shared the owner receives a notification at real-time and he/she decides if grant or deny the exchange of information.

Fig. 2 shows an example of privacy-preserving and context-aware profiles. The example is composed of two different contexts, *Context_A* and *Context_B*. *Context_A* has two context-aware profiles, *Profile_A* and *Profile_B*. On the other hand, *Context_B* has the *Profile_A* and *Profile_B*. Each profile is composed of several privacy policies which can be shared by the profiles existing in that context.

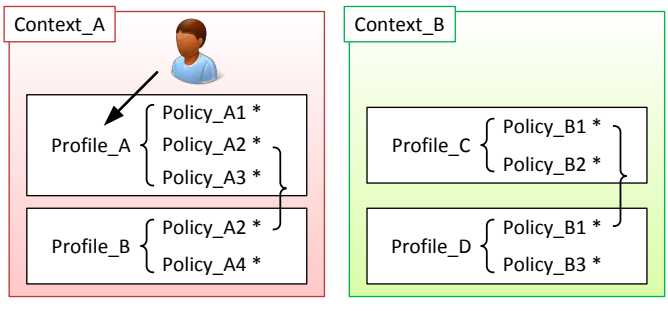

Fig. 2. Context-aware profiles with several policies for each context

The policies that compose the privacy-preserving and context-aware profiles can be categorized into two different groups, intra- and inter-policies. These two groups of policies allow users to protect their location, personal information, activities, and context-aware information. Specifically, intra-policies protect the users' information inside of specific contexts, and inter-policies preserve the users' information between different contexts. In order to protect the information, the intra- and inter-policies' groups are composed of *disclosure* and *reveal* policies. *Disclosure* policies are in charge of indicating what information of the users can be shared. On the other hand, *reveal* policies indicate where, when, and how the information can be shared.

Disclosure and reveal policies are composed of specific fields such as *Type*, the kind of policy; *Maker*, the user or service administrator who defines the policy; *Target*, the user whose information is being managed; *Requester*, the user, or group of them, who request information; *Result*, the relationship that determines the access to the information; *What*, the sensitive information revealed by the target; *Where*, the place or context in which the policy must be applied; *When*, the date when the policy must be applied; and *How*, the activity done by the target or the requester.

$$Type \wedge Maker \wedge Target \wedge Requester \wedge What \wedge Where \wedge When \wedge How \rightarrow Result$$

III. Conclusions

We have presented in this paper several solutions in charge of protecting the users' information at real-time in context-aware environments. The privacy-preserving policies provided by our system consider the context in which users are located to manage the users' information. The users of our solutions can modify the policies at will by adding, deleting, and modifying information to control what, where, when, how, and to whom the users want to reveal their information.

Acknowledgment

This work has been supported by a Séneca Foundation grant within the Human Resources Researching Training Program 2014, the European Commission Horizon 2020 Programme under grant agreement number H2020-ICT-2014-2/671672 - SELFNET (*Framework for Self-Organized Network Management in Virtualized and Software Defined Networks*), the Spanish MINECO (project DHARMA, *Dynamic Heterogeneous Threats Risk Management and Assessment*, with code TIN2014-59023-C2-1-R; and project TecMASAS, *Techniques to Improve the Architecture of Servers, Applications and Services*, with code TIN2015-66972-C5-3-R), and the European Commission (FEDER/ERDF).

References

[1] A. Huertas Celdrán, F. J. García Clemente, M. Gil Pérez, G. Martínez Pérez: "SeCoMan: A semantic-aware policy framework for developing privacy-preserving and context-aware smart applications", in *IEEE Systems Journal*, To appear.

[2] A. Huertas Celdrán, M. Gil Pérez, F. J. García Clemente, G. Martínez Pérez: "What private information are you disclosing? A privacy-preserving system supervised by yourself", in *6th International Symposium on Cyberspace Safety and Security*, pp. 1221-1228, 2014.

[3] A. Huertas Celdrán, M. Gil Pérez, F. J. García Clemente, G. Martínez Pérez: "MASTERY: A multicontext-aware system that preserves the users' privacy", in *2016 IEEE/IFIP Network Operations and Management Symposium*, To appear, 2016.