A. Munoz, J. A. Onieva, and J. Lopez, "On Secure Profiling", *1st International Workshop on Secure Ubiquitous Networks (SUN05)*, pp. 214-218, 2005.
NICS Lab. Publications: https://www.nics.uma.es/publications

On Secure Profiling

Antonio Muñoz, Jose A. Onieva and Javier Lopez
Computer Science Department, E.T.S.I. Informatica
University of Malaga, Spain
{amunoz, onieva, jlm}@lcc.uma.es

Abstract

Ubiquitous environments have several drawbacks to be solved. Most of them are focused on security, and relevant ones are authorization and authentication. Amongst the essential elements to adequately provide solutions, we can find profiles. A profile can be defined as a repository to store structured data from users, networks, devices, applications, etc. As profiles are needed in ubiquitous environments, and these need of secure management as well, in this paper, we provide some initial guidance on the security storage of profiles and on security levels needed for each type of profile. Additionally, we review different alternatives to bear profiles, concluding that smartcards are the most suitable devices.

1. Introduction

This paper is focused on justifying why secure mobile device is needed in order to store profiles in an ubiquitous environment. This procedure is performed analyzing every kind of profiles and their associated fields from a security engineer point of view. Following the mobility nature of profiles the main idea of this paper is the usage of smartcards to store profiles. Amongst ubiquitous researchers, this idea is very common; however we do formalize it in this study.

1.1. Related Works

The term Ambient Intelligence is defined by the Advisory Group of the European Commission's Information Society Technology Program (ISTAG) as *"the convergence of ubiquitous computing, ubiquitous communication, and interfaces adapting to the user"* [1]. Far for being introduced by ISTAG, the term ubiquitous computing was coined by Weiser in 1991, referring to computers which are omnipresent and serve lot of people in their daily lives, which work in an invisible and unobtrusively way easing connection and configuration tasks to users. More precisely, in that seminal work, he stated: "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it [2].

A more concrete definition of ubiquitous computing technology is that of any computing technology that enable human interaction away from a single workstation, which includes pen-based technology, hand-held or portable devices, large-scale interactive screens, wireless networking infrastructure, and voice or vision technology [3].

Ubiquitous computing infrastructure includes processors, sensors, networks, mechanisms, protocols, services and their surrounding physical spaces. These heterogeneous components are often incompatible and incapable of inter-operating, which makes operations and trust difficult, configuration, management and monitoring of these devices harder, and the application of uniform security policies virtually impossible. While some components of the infrastructure may contain sophisticated security mechanisms, others may be resource-limited and unable to handle complex security requirements. Additionally, it is important to consider the effects of privacy of the individual, finding a trade-off with the needs of the (often more powerful) actor who wants information. It is important to control ***how*** information is used, not just who has access to or control it. Very often, a powerful actor has a need for information that in itself poses no risk to individuals (e.g. average salary, popular products or relevant documents for a workgroup). But in order to derive the information required, more invasive raw data (how much each person makes, what products one person bought, what papers a person is reading or what they wrote in an email) are needed.

Therefore, private computation becomes the mean for two (or more) parties to agree to specific uses of

sensitive information, and prevent unauthorized uses. It is a ***computational pact*** that binds them to this agreement, and prevents others, even in the future, from using it with other purposes.

In order to get a both private and authenticated system, we need a new element which must be stored both in a secure way and in a portable device. This element must be a repository of information related to user, network, device, etc. Information stored in these elements is used to authenticate, authorize and even to perform tasks such as caching of user preferences. In this way, the concept of *profile* is developed in ubiquitous computing.

As previously stated, one of the most critical issues in pervasive environments is security. In this sense, Urien and Pujolle proposed to adapt the security architecture (IEEE 802.1x) that is going to be deployed in emerging wireless networks [4]. That is the reason why we suggest working with dedicated smartcards, as in an Internet Draft [5] for processing the Extensible Authentication Protocol [6].

Smartcards are mostly used to authenticate users; however, they can now perform more functions than that traditional one. Though limited in speed and space, chips contain microprocessors, ROM and memory, and run their own COS (Chip Operating System), on which various applications may execute. Hence, with this computing power, it may be possible to use Smartcards as mobile access points to services. Moreover, smartcards can store user information, invoke services and process temporary service results. For these reasons, we look at using smartcards as a vehicle for providing ubiquitous computing. Users of the ubiquitous scenarios that we envision should be able to access services from any place with their smartcards, not requiring necessarily a higher performance computing mobile devices, such as PDAs.

Prior to performing a discussion about securely storage of profiles, we are going to establish a profile classification, scrutinizing the security level of each of them, identifying all the fields that could be present in each profile as well as its potential associated risks. Additionally, convenience of a portable device to store profiles will be discussed so that user keeps their profiles bearer with them. Finally, we will discuss all the possibilities of profile bearers and argue that a smartcard is an ideal device for storing profiles.

With these ideas in mind, we have structured the paper as follows. In Section 2 we establish a classification of different types of profiles which arise in our work, defining them and listing their fields. In Section 3, we perform a classification of different security levels, inserting more suitable fields that compos each kind of profile, and concluding that some of these fields must be stored in a secure way. In Section 4, we review all alternatives to bear profiles, inferring that smartcards are the most suitable devices for this task. Finally, section 5 presents conclusions and propose some future work issues.

2. A classification of different types of profiles

We have previously introduced the concept of profile. Nowadays, profiles are part of the state-of-art, especially because of the impact caused by ubiquitous networks in current research trends. Next, we provide a complementary definition: A profile consists of a repository of structured data which affects other entities, and at the same time is the location where properties, features and profile characteristics are stored both in a past and in a current status. With this definition adapted to our target, we will use profiles to characterize different type of entities in an unique way. A classification on the different types of profiles that we will use follows now, as well as a description of the more important fields included in profiles.

Our definition of profile is user-centric, that is, we consider a user profile as a composition of network profile, device profile, application profile, service profile, context profile and several fields of the user. This is supported by the idea that we believe it has no sense to talk about network, device, application, service and/or context in an execution instant with no user associated.

Amongst the many profiles that could be studied, we underline the following ones: user profiles, device profiles, network profiles, application profiles, service profiles and context profiles. From a general point of view these types of profiles will be used. If more detailed profiles or different subsets in a common profile are needed, these will be *subprofiles*.

Subprofiles are like profiles, with all their features, though with one restriction: their fields are a subset of a profile, and the union of all subprofiles associated to one unique profile is exactly that profile. Using the subprofile concept we can distinguish between static user subprofiles and dynamic user subprofiles, attending to when the profile is generated. Also, we can differentiate among identity user subprofile, relationship user subprofile, capability user subprofile and preferences user subprofile, attending to data semantic features.

In other type of profiles, the same classification appears. For instance, device profiles are composed of description device, hardware-description device, network-id information device, network security device, IP network information device subprofile, etc.

We consider a Network profile as a composition of two subsets, generic information network subprofile and specific information network subprofile afterwards described. Similarly, general information service subprofile and functional information service subprofiles form Service profiles. Concerning Context profiles, we consider them as a composition of location information context subprofile and environment information context subprofile.

Going further for each of those profiles, we find several fields integrating each of them. User identity subprofiles are formed by name, surname, nickname, gender, date of birth, occupation, address, language(s), email, phone(s), fax, etc. Most of data included in these subprofiles are very sensible because such personal information might be used to replace user with a malicious purpose. However, looking at another subprofiles such as preferences user subprofile with fields as favourite applications, less favourite applications, favourite services and their configuration parameters, less favourite services, favourite interaction models and less favourite interaction models, we can appreciate that this information is not that problematic regarding security.

At this point, there is not a clear difference about which fields must be stored in a secure storage. Let us provide the following scenario. Katto (the user) keeps an USB device with both personal information and preferences information stored as a profile. Katto is in a trip out of home and he decides to go to a cybercafe located very close to the hotel where he is staying, and he wants to connect to the Internet with his usual configuration. He is in a hurry, so he tries to load his profile from his own device inserting his USB-device in the terminal of the cybercafe, but all his information is cached somehow in his terminal assigned. When he finishes his session, he pulls out his USB device and leaves to meet a friend as he is already late.

Concerning preferences information, probably there is no problem if this information is cached in the terminal PC, but some part of information stored in a profile is potentially dangerous in malicious hands, such as our real name, identification number or even our bank account number.

Therefore, in order to reach a good privacy level, we must ensure that part of this information is stored in a secure way. A first approach will consist of storing the full profile in a secure way and later relax secure constraints. This mode of operation is better in a practical way, since it is easier to relax constraints than restricting them.

3. Classification of different security levels

Concerning security, several different categories must be established amongst profiles or even sub-profiles according to what kind of data are stored inside. In this way, there are fields that if lost, potential risks could arise, such as compromising personal information from the user (name, address, private numbers etc). In order to protect this information, strict security measures have to be taken.

Oppositely, there are other fields which keep non-critical information and which storage does not need any security measures. As it is expected, most of fields are between those two sets. A lot of different security levels might be taken in this range, but we consider for the sake of clarity just one level set in this first approach. Summarizing, we perform a classification attending to three security levels: *high*, *medium* and *low*.

Ambient Intelligence surrounds user-centric systems, so our main concern in our work is user profile which, as already explained, is the composition of other profiles and its own fields added. Concerning user identity, certain fields must be included in higher security level, medium security level or lower security level.

- High security level: Name, surname, gender, birth date, occupation, address, email, telephone numbers and even account bank number. Some relationship information such as contacts data.
- Medium security level: User identification, nickname and languages. Probably some relationship information.
- Low security level: Capabilities data and preferences data. Also, some devices relation data.

Relationship information is split amongst different categories, so information related with contacts must be included in high security level, although for other fields it is sufficient to include them in the medium level established. At last, information related with relationship with different devices might be included in lower level.

Device profiles are composed of hardware features device subprofile, software features device subprofile, hardware limitations device subprofile and software limitations device subprofile. Two main set of fields can be distinguished, hardware and software features, but also their limitations need to be considered. Their associated security levels are:

- Low security level: Both hardware characteristics subprofiles and hardware limitations subprofiles. Hardware characteristics and limitations are composed of: fields as the interface types, interfaces versions, screen resolution, screen size, audio hardware, system supported, keyboard supported, mouse, memory features, etc. From our point of view, the storage of this information is not very critical. All these can be included in lower level of security.
- Medium security level: Regarding software features, even though it could be irrelevant to take any security measure on fields such as operating system (OS) name, OS vendor, OS version, OS copy serial number installed, etc., some of this information can become sensible, such as OS copy serial number installed, which could be useful for a malicious agent. Therefore, we have decided to include them in a medium level.

Network profile, which contains information related to the physical features of the network technology used, is compound of generic network sub-profile and concrete network sub-profiles. All information stored can be split in two main sub-profiles: *generic* and *concrete* information. Concrete information sub-profile contains data such as technical and performance information, which is not very sensible, although some technical information might be useful for a malicious agent.

Similarly, for the generic subprofile, fields as identification, security, IP, charging and semantic information might be included in a new higher level of security, but this is not the case. Therefore, in this first approach, we have decided to include network profile data in the higher level of security.

As for Service Profile, we identify two main subsets: *general* and *functional* information. In other words, it is a composition of general service information subprofile and functional service information subprofile. All this information (as the one in application profiles) is not sensitive and can be saved under any security measures. This is the reason why this type of profile can be classified as low security level.

We divide Context profile in two subsets: location context subprofile and environment context subprofile, and is also classified in the low security level.

4. Smartcards for a secure storage of profiles in ubiquitous environments

The main idea behind using profiles in ubiquitous environments is the close relationship with mobility and portability by the user; that is, information stored in profiles must be under the control of the user, what points out that the first requirement for a profile bearer device is portability. On the other hand, and as it has been previously discussed, there is some information in profiles that is potentially dangerous, strong reason to claim that a secure device is necessary to store this information. In the rest of this section, we briefly sketch different existing alternatives to store profiles while we analyze which of them fulfil main requirements. Then we explain why we have decided to use smartcards as profile bearers.

Among the different possible devices to bear profiles, we consider USB pen-drives, which integrate the same features as any other storage device which uses an USB interface such as MMC, SD, External HD USB, etc. These devices provide portability to the user, in such a way that the user has his device available most of the time. However, they are non-secure devices, which might be a danger if this device is stolen, lost, etc., because data might be used without any authorization. Another group of bearers is formed by local massive storage devices, which are neither secure nor portable.

Remote database is another option which could be portable and secure although these solutions present their own disadvantages. With respect to security there are several alternatives to access to a remote database in a secure way, but all of them are costly in resources because different technologies are needed, such as establishment of a secure channel, key sharing, etc. Another issue is that user will not have available his profile in an off-line environment. This issue limits somehow profile portability. In the same way, all these problems repetitively appear in other alternatives such as a remote shared folder in the network or any virtual storage device.

Finally, there is no discussion about smartcard portability. An example of this is the amount of smartcards used daily by a lot of people in organizations around the world. The second important characteristic of these limited devices are the security features they implement: such as secure storage of private key and implementation of the RSA algorithm. CPU performances are currently around 100 MIPS, and memory sizes around one megabyte for components supporting the FLASH memory technology [4].

Although available memory in smartcards is very reduced at this moment, so full profiles can not be inserted, ubiquitous computing enhances computer use by making many computers available throughout the physical environment, while making then invisible to the user [7]. According to the Moore's law, computers performance doubles each 18 months, microelectronics continuous progresses in terms of memory sizes, computing capacities, and power consumption, leads to the availability of cheap and highly integrated components, including communication resources. We should underline that memory sizes are potentially unlimited. All these features put smartcards on top of alternatives as secure profile bearer devices.

5. Conclusions and ongoing work

Nowadays more people is using smartcards, as the massive use of cellular phones shows. At the same time, it seems very clear that profiles will be used by future applications and services. With the sum-up of these facts we can conclude that, at this moment, smartcards are the best most suitable devices to store profiles for users. Although smartcards have several limitations such as memory restrictions, these restrictions are being tackled by technological progress according to the Moore's law.

As open issues in this field, a more detailed classification of different security levels is needed, being this an on-going work under development now where we are identifying more levels than the three proposed in this paper. Also, we are currently working in the description of a protocol for secure retrieval of profiles stored in smartcards using a secure way and the cryptographic capabilities provided by smartcards crypto processors. A comparative analysis of different type of smartcards in the market should be performed to evaluate several metrics of time, available memory, price, etc.

6. Acknowledgements

The study described here is partially funded by the FP6-2002-IST-1 project UBISEC, contract number 506926 and the second author has been funded by the Consejeria de Innovacion, Ciencia y Empresa (Junta de Andalucia) under the III Andalusian Research Plan.

7. References

[1] Gupta, M., "Ambient Intelligence - unobtrusive technology for the information society", *Pressbox.co.uk*, June 17, 2003, *http://www.pressbox.co.uk/Detailed/7625.html.*

[2] Weiser, M., "The Computer for the 21st Century", *Scientific American*, Vol. 265, No. 3, September 1991, pp. 94-104.

[3] Abowd, G.D., Atkeson, C., Brotherton, J., Enqvist, T., Gulley, P. and Lemon, J., "Investigating Research Issues in Ubiquitous Computing: The Capture, Integration, and Access Problem", *Proceedings of CIH'98*, April 1998, pp. 440-447.

[4] Pascal Urien1, Guy Pujolle, "A simple security model for emerging 802.11 pervasive Environments", *Proceedings of the SOC'2003 Conference,* Grenoble, May, 2003.

[5] Urien, P., Farrugia, A.J.,, Pujolle, H., Groot, M., "EAP. Support in smartcards", draft-urien-EAP-smartcard- 01.txt, internet draft, March 2002.

[6] Blunk L., Vollbrech J., "PPP Extensible Authentication Protocol (EAP)" , *RFC 228,* 1998.

[7] Weiser, M.(1993) "Some Computer Sciences issues in Ubiquitous Computing*", Communications of the ACM,* July 1993, Vol 36, n°7, pp 75-84