Finally, in order to implement the transversal concept of trust to the SIAC model, we propose to combine PKI technologies and the WOT ontology, defining a new ontology called XWOT. Using this ontology, information's origin and integrity could be asserted and verified, and trusted third parties could issue pieces of reliable identity information that a user might include in her personal profile.

Thanks to the SIAC model, social applications could share, trust and reuse identity information, and it would be easier for users to control it.

Acknowledgments. This research has been supported by Safelayer Secure Communications and the Centre for the Development of Industrial Technology (CDTI) of Spain, within the framework of the Segur@ project, reference CENIT-2007 2004 of the CENIT Programme (part of the INGENIO 2010 initiative) [15].

References

1. "Social Networks: Facebook Takes Over Top Spot, Twitter Climbs", http://blog.compete.com/2009/02/09/facebook-myspace-twitter-social-network/
2. "The Friend of a Friend (FOAF) project", http://www.foaf-project.org/
3. "Semantically-Interlinked Online Communities Project", http://sioc-project.org/
4. "WOT (Web of Trust) Schema", http://xmlns.com/wot/0.1/
5. "W3C Semantic Web Activity", World Wide Web Consortium, http://www.w3.org/2001/sw/
6. "DOAC: Description of a Career", http://ramonantonio.net/doac/0.1/
7. "Dublin Core Metadata Initiative", http://dublincore.org/
8. "An ontology for vCards", http://www.w3.org/2006/vcard/ns
9. A. Tootoonchian, K.K. Gollu, S. Saroiu, Y. Ganjali, and A. Wolman, "Lockr: social access control for web 2.0," Proceedings of the first workshop on Online social networks, ACM New York, NY, USA, 2008, pp. 43-48.
10. M. Hart, R. Johnson, and A. Stent, "More content-less control: Access control in the Web 2.0," Proceedings of the IEEE Web 2.0 Privacy and Security Workshop.
11. B. Carminati, E. Ferrari, and A. Perego, "Rule-based access control for social networks," Lecture Notes in Computer Science, vol. 4278, 2006, p. 1734.
12. J. J. Carroll, "Signing RDF graphs", Digital Media Systems Laboratory, July 2003.
13. J. J. Carroll, C. Bizer, P. Hayes, P. Stickler, "Named Graphs, Provenance and Trust", HP technical report, 2004.
14. "XML Advanced Electronic Signatures (XAdES)," ETSI TS 101 903 V1.3.2, Technical Specification, vol. 3, 2006.
15. "Proyecto CENIT SEGUR@ Seguridad y Confianza en la Sociedad de la Información", http://www.cenitsegura.com

The Impact of Contextual Information on User Privacy in Social Networks

Anna Carreras, Jaime Delgado, Eva Rodríguez and Ruben Tous

Distributed Multimedia Applications Group, Departament d'Arquitectura de Computadors
Universitat Politècnica de Catalunya, Barcelona, Spain
{annac, jaime.delgado, evar}@ac.upc.edu

Abstract. Context-aware applications are becoming very popular as they are a mean of enriching users' experiences in multimedia scenarios. Nevertheless, the acquisition, representation, and protection of contextual information are still open issues that need to be addressed. These are significant topics of interest mainly due to today's growing concern on user privacy, and are particularly relevant in the context of Social Networks. In this paper we briefly present our work developed within the Visnet-II Network of Excellence (NoE) on context acquisition and protection for context-based content adaptation. We identify the sensitive contextual information used within Social Network application scenario, and then specify a suitable privacy model. Finally, we describe how this model could be implemented through the use of the MPEG-21 Rights Expression Language (REL) standard.

Keywords: Privacy, Social Networks, Digital Rights Management, MPEG-21 DIA, MPEG-21 REL, context-aware content adaptation

1 Introduction

In the context of Universal Multimedia Access (UMA) [1], context-aware content adaptation is essential in order to allow users to access any type of content, anywhere, and anytime [2]. In particular, the use of contextual information is essential to achieve efficient and useful adaptations that enrich the user experience. Nevertheless, there is a growing concern on the illegitimate use of contextual information.

This concern is particularly significant within collaborative environments such as Social Networks, where users are willing to share a variety of information, such as personal attributes and environmental conditions, with their "friends". In reality many other entities, such as data aggregators and third-party advertisers, can also have access to this information. Many voices claim [3], [4] that current platforms (i.e. Facebook) tend to violate their Terms of Service.

The paper is structured as follows: first, it briefly describes the Digital Rights Management (DRM)-enabled and context-aware content adaptation platform developed within the Visnet-II NoE project [5], focusing on the acquisition of the different types of contextual information and their representation based on MPEG-21 Digital Item Adaptation (DIA) standard [6]. Afterwards, it identifies the sensitive

information that should be protected, while also analyzing a possible privacy model for Social Networks application scenario. And finally, it specifies suitable MPEG-21 REL [7] compliance protection techniques that could be applied in order to implement this model.

2 State of the Art

Although the concept of social networking appeared forty years ago, it is only recently that Social Networks have become massively popular. Due to this new multimedia phenomenon, big amount of (personal) data is being shared through the internet, and subsequently users' concern about privacy has risen. Even if privacy protection measures exist for the most popular internet applications (such as web browsing), Social Networks present new requirements mainly due to the fact that in this application scenario most of the information is voluntarily provided by the users. New protection techniques, including a more fined-grained control over the access to contextual information, are required. The duality between privacy protection and DRM (already outlined in the literature [8], [9] are even more evident in this application scenario, as DRM provides a mean to govern the usage of digital contents.

Even if the information provided by the users is especially sensitive, many other types of contextual information exist. Information about the network, the terminal, or the usage environment may be also gathered (and illegitimately used) without the consent of the users. This is particularly relevant in context-aware applications, and more precisely in context-aware content adaptation, where various types of contextual information are used in order to enrich the user's experience. While most the work done so far in privacy protection for Social Networks only focuses on the information provided by users, there is a clear need to integrate these two lines of research.

3 Visnet-II NoE Context-Aware Content Adaptation Platform

3.1 Architecture

The Visnet-II NoE context-aware and DRM-enabled architecture is shown in Fig.1 and detailed in [10]. The most notable advantage of this distributed and modular architecture is that it ensures scalability.

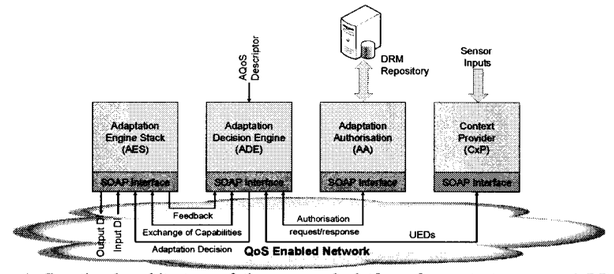


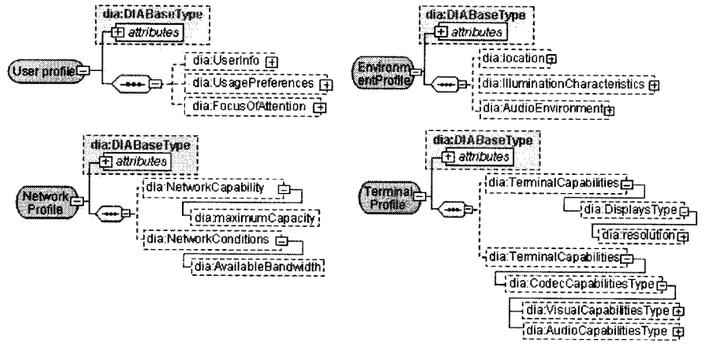
Figure 1. Functional architecture of the proposed platform for context-aware and DRM-enabled multimedia content adaptation.

Based on contextual information received from various Context Providers (CxPs), the Adaptation Decision Engine (ADE) determines the optimum adaptation options that can maximize the user satisfaction across the network. The Adaptation Authorizer (AA) [11] ensures the governed use of protected content through DRM and is based on MPEG-21 DIA and MPEG-21 REL standards. Finally, the Adaptation Engine Stack (AES) enables the execution of a variety of adaptations that can be dynamically configured and requested on the fly.

The next subsection elaborates the types of context profiles made available to the ADE.

3.2 MPEG-21 DIA Based Context Profiles

The use of standards is instrumental to enable interoperability among systems and applications, and across services. In our previous work [10], we had already analyzed the existing initiatives offering standardized representations of context. We concluded that MPEG-21 DIA specification presents the most complete set of contextual information, and subsequently, it is the standardized format used in this work. It specifies appropriate XML schemas to represent the low-level contextual information. In particular, the MPEG-21 DIA Usage Environment Description (UED) tool provides four main types of descriptors: User, Terminal, Network, and Natural Environment. Based on this division, four context profiles have been created, as illustrated in Fig. 2. With these profiles, each CxP needs only to know and implement its own sphere of action resulting in a level of interoperability enhancement.



3.3 Context Acquisition

We believe "acquisition" is a more generic term that includes not only the extraction, but also the gathering, representation and storage of contextual data, and the provision of access mechanisms to retrieve it. In our approach, CxPs act mainly as the context sources that take the initiative of generating new contextual information. From this perspective, it is not the recipient of the context (i.e., the ADE) that asks for or extracts new context on demand. Thus, we consider a "push model" rather than a "pull model" for acquiring the available context during operation. Subsequently, the acquisition of this information is presented as a flexible process that mainly depends on the capabilities of the infrastructure supplied by network providers, terminal providers and so on and so forth.

Thus, the main methodology that needs to be addressed in our platform is the gathering of stored context. Our preferred approach relies on the usage of XML [12] for context data serialization and interchange. We believe that it is the most convenient way, as it facilitates the integration with different types of applications, and supports the extensibility and generalization of the middleware for handling different types of context information. In our scenario, indeed, not only does user context need to be stored (e.g., personal data, preferences, etc), but information about the capabilities of the terminal and the network (e.g., terminal display size, network maximum bandwidth, etc) is also gathered, and thus stored. The usage of XML as an interchange format is independent from the storage mechanism. Context data in XML format can be distilled through different layers (Web Services, APIs, etc.) on top of the storage mechanism. Effective storage can be achieved through the usage of native XML databases such as eXist [13] and accessed through XML Query Language (XQuery)/XML Path Language (XPath) [14]. However, in practice, relational or object-relational databases [15] are widely used to store, search and retrieve contextual information: for example, in [16] context information about geography, people, and equipment is stored in a relational database. Moreover, in [17], historical

information about location is stored in a database that can be accessed using Structured Query Language (SQL). The most part of current commercial databases offers also XML support and XQuery-like interfaces in addition to SQL, so the decision about the underlying technology keeps transparent and depends only in performance/cost aspects.

4 Context Protection and Privacy Issues in Social Networks

This line of research is considered to be very important when developing context-aware systems, which may need to exchange sensitive personal information among different subsystems. Furthermore, in social networks, where people share all types of data, access to information resources should be allowed according to the defined policies and rules. Contextual information requires similar treatment in terms of protection and privacy issues, just like any type of information.

In our application scenario, the user is expected to be responsible for defining his/her own privacy preferences, and thus, our main objective in this section is to identify, first, the context descriptors that may need to be protected, and second, the parameters that may be required for defining the privacy model.

4.1 Identification of Sensitive Contextual Information

The first step to be taken when defining a privacy model is the identification of the information that needs to be protected. Of course, the protection of certain context will also depend on who the recipient is or its intended usage, but this will be analyzed in the next subsection. Here, we will only identify a subset of sensitive contextual information among the full set of contextual descriptors involved in our context-aware and DRM-enabled content adaptation platform.

Moreover, the sensitivity of any type of information is a very subjective qualifier. Indeed, a person may think that data about the network conditions is very sensitive information because network providers may exploit it to bother him/her regularly with new offers while other users do not mind to be localized by anyone, as they may think it is the best way to get advantage of today's context-aware applications. Thus, there is not a single classification, which is right. In Table 1, we distinguish between non-sensitive, low-sensitive, and high-sensitive contextual information.

Table 1. Classification of context descriptors based on their sensitivities

Context descriptor	Context profile	Non-sensitive	Low sensitivity	High sensitivity
User info	User			X
Impairments	User			X
Preferences	User			X
Terminal capabilities	Terminal		X	
Terminal characteristics	Terminal		X	
Network capabilities	Network		X	
Network conditions	Network		X	
Location	Natural environment			X
Time	Natural environment			X
Environment conditions	Natural environment		X	

4.2 First Approach to a Privacy Model

Once the identification of the sensitive information has been done, we need to identify the different roles of the users involved in our application scenario in order to specify the rules that will model the privacy protection system.

We focus particularly on the application of Social Networks in a business/office context, in which a number of office workers and/or clients of an organization act as the different agents involved in a collaborative network. As an example, we may identify the following user roles:

- Team manager
- Team leader
- Deputy team leader
- Team member
- Customer
- Interviewer
- Interviewee

For each of these roles, a different privacy rule should be defined. Furthermore, in a more generic identification of roles in a Social Network, we should also include the Adaptation Authorizer (AA) and the Adaptation Decision Engine (ADE) as the main agents that require access to the contextual information from the users. For example, the Location of an Interviewee may be required by the AA when accessing some content, but this information should be public neither to the rest of participants of the Network nor to the ADE.

Indeed, when protecting any type of information, the main issue that needs to be addressed is "who can obtain what and when". We already identified the sensitive information ("what"), and the different agents involved in the scenario ("who"). The

"when" is a more abstract concept that usually needs some previous parameterization. Apart from the time, it may include for example, the location, the activity, and the nearby people of the recipients. We will refer to it as a "situation". A more generic, yet still popular parameterization, is to distinguish between the purpose, the conditions and the obligations of the recipients.

Another important issue to be considered is the granularity of the parameters used to express the privacy rules. Following with the Interviewee example, he/she may be happy to reveal that he/she is in Barcelona, but not on which street; or he/she may be happy to disclose the street to the Team leader, but not to the rest of the Team members.

Table 2 summarizes the initial parameterization of our proposed privacy system, suitable for specifying the privacy rules later. Based on these parameters, many different protection rules could be defined, depending on the ethics or the relevance of the company/institution using the Social Network and the individual concern of each of the members.

Table 2. Parameterization of our Privacy Model

User role	Context descriptor	Recipients	Situation	Precision
Team manager Team leader Deputy team leader Team member Customer Interviewer Interviewee	User info Impairments Preferences Terminal capabilities Terminal characteristics Environment conditions	Team manager Team leader Deputy team leader Team member Customer Interviewer Interviewee ADE Governance Server (AA)	Location Usage Time Nearby people	Undisclosed Vague Approximate Precise

5 Specifications for Implementing a Privacy Model based on MPEG-21 REL

A number of researchers have observed a duality between privacy protection and copyright protection [18], and in particular, observed how DRM technology may be used as the basis of a privacy protection system [8], [9]. Considering that our DRM system is based on MPEG-21 Rights Expression Language (REL), we are particularly interested in the possibility of using the same standard for implementing the privacy model.

MPEG-21 REL is defined as a collection of three XML schemata, called the core schema (denoted by the XML namespace prefix "r"), the standard extension schema (prefix "sx"), and the multimedia extension schema (prefix "mx"). These schemata define the fundamental elements of the language, some widely-useful conditions, and elements useful in copyright protection applications, respectively. We present here a

suitable privacy extension schema that could be used for implementing our privacy model. The elements of the privacy extension will be denoted by the namespace prefix "px".

First of all, we need to identify the elements already contained in the MPEG-21 REL license that could be easily mapped to the parameters defined in our privacy model. For example, the user who wishes to protect his/her contextual information can be easily identified as the MPEG-21 REL *Issuer* (responsible for specifying the privacy policies) while the recipient of the contextual information corresponds to the MPEG-21 REL *Principal* (responsible for exercising the right over some content). Finally, the MPEG-21 REL *Resource* could be used to express a single or even a set of sensitive contextual descriptors that need to be protected.

The most difficult part is to identify how to express the "Situation" and the "Precision" parameters. As can be seen in Table 2, "Situation" combines contextual descriptors already contained in MPEG-21 DIA UED, such as Location or Time, along with other elements, such as "Usage" or "Nearby people". We already know, from our previous work in the adaptation authorization [11], that we can include MPEG-21 DIA descriptors inside the MPEG-21 REL *condition* field, and thus it would have sense to include "Location" and "Time" as MPEG-21 DIA constraints in the *Allconditions* field of MPEG-21 licenses. Something similar could be applied to the "Nearby people" descriptor, as we have already proposed in [19] to extend the MPEG-21 DIA UEDs with this type of contextual information, owing to its relevance to Virtual Collaboration applications (and by extension to Social Networks). Nevertheless, to the best of our knowledge, a suitable descriptor does not exist in MPEG-21 to map "Usage". Our proposal is to include a "px:usage" element in the conditions field. Finally, the "Precision" is expressed implicitly, and hence does not need a special element in MPEG-21 licenses. The issuer of the license is responsible for introducing a more or less detailed description of the context (in the resource field) associated to every principal.

It is also relevant to note that MPEG-21 REL defines an element named "r:propertyProcessor" that allows to express groups of principals (users) through roles.

An example of our proposed license based on MPEG-21 REL to govern the use of contextual information is shown in Table 3. It allows the "Team Manager" to know the "location" of the "Team members" in order to fix a meeting in the following days.

Table 3. Example of a license based on MPEG-21 REL to govern the use of context

```
<r:license xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
    xsi:schemaLocation="urn:mpeg:mpeg21:2003:01-DIA-NS DIA-2nd.xsd
    urn:mpeg:mpeg21:2003:01-REL-R-NS rel-r.xsd
    urn:mpeg:mpeg21:2003:01-REL-SX-NS rel-sx.xsd
    urn:mpeg:mpeg21:2003:01-REL-MX-NS rel-mx.xsd
    urn:visnet:privacy drm-privacy-px.xsd"
    xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
    xmlns:dia="urn:mpeg:mpeg21:2003:01-DIA-NS"
    xmlns:mx="urn:mpeg:mpeg21:2003:01-REL-MX-NS"
    xmlns:r="urn:mpeg:mpeg21:2003:01-REL-R-NS"
    xmlns:sx="urn:mpeg:mpeg21:2003:01-REL-SX-NS"
    xmlns:mpeg7="urn:mpeg:mpeg7:schema:2001"
    xmlns:px="urn:visnet:privacy"
    xsi:noNamespaceSchemaLocation="licenses.xsd">
  <r:grantGroup>
    <r:grant>
      <r:propertyPossessor>Team Manager</r:propertyPossessor>
      <!-- Principal-->
      <mx:view/>   <!-- Right -->
      <mx:diReference>
        <mx:identifier>context-location</mx:identifier>
        <!--Resource-->
      </mx:diReference>
      <r:allConditions>
        <px:Usage>meeting</px:Usage>
      </r:allConditions>
    </r:grant>
  </r:grantGroup>
  <r:issuer>
    <r:propertyPossessor>Team members</r:propertyPossessor>
  </r:issuer>
</r:license>
```


Furthermore, also to the best of our knowledge, there is no real implementation of a privacy protection system based on MPEG-21 REL. We have specified the necessary guidelines for a possible implementation of our privacy model aligned with the rest of our work during the integration of DRM and adaptation.

6 Conclusions

This paper presents the work done on privacy protection within the Visnet-II NoE project. The use of standards, such as MPEG-21 DIA for representing the contextual information and MPEG-21 REL for governing it usage, guarantees the interoperability and extensibility of our proposal. Furthermore, the parameterisation of a privacy model for Social Networks is presented, and detailed for a Virtual Office application scenario. Finally, DRM-based protection techniques that could be applied in order to implement this model are specified.

As far as we know, this is the first work trying to jointly address privacy protection for both, context-aware content adaptation and Social Networks.

7 Acknowledgements

This work has been partially supported by the European Commission IST FP6 program (VISNET II Network of Excellence, IST-2005.2.41.5) and partially by the Spanish government through the projects MCM-LC (TEC 2008-06692-C02-01) and Segur@ (Centre for the Development of Industrial Technology (CDTI), CENIT-2007 2004, under a subcontract with Safelayer Secure Communications).

References

1. Vetro, A.: MPEG-21 digital item adaptation: Enabling universal multimedia access. IEEE Multimedia J., vol. 11, no. 1, pp. 84--87. (2004)
2. Wang, Y., Kim, J.-G., Chang, S.-F., Kim, H.-M.: Utility-based video adaptation for Universal Multimedia Access (UMA) and content-based utility function prediction for real-time video transcoding. IEEE Trans. Multimedia, vol. 9, no. 2, pp. 213--220. (2007)
3. Gross, R., Acquisti, A.: Information Revelation and Privacy in Online Social Networks. In Proc. 2005 ACM Workshop on Privacy in the Electronic Society, pp. 71--80. (2005)
4. Strater, K., Lipford, H. R.: Strategies and Struggles with Privacy in an Online Social Networking Community. In Proc. 22nd British HCI Group Annual Conference on HCI 2008: People and Computers XXII: Culture, Creativity, Interaction, vol. 1, pp. 111--119. (2008)
5. Visnet II Network of Excellence (NoE) project, http://www.visnet-noe.org/
6. Information Technology – Multimedia Framework (MPEG-21) – Part 7: Digital Item Adaptation, ISO/IEC Standard ISO/IEC 21000-7:2007. (2007)
7. Information Technology – Multimedia Framework (MPEG-21) – Part 5: Rights Expression Language, ISO/IEC Standard ISO/IEC 21000-5:2004. (2004)
8. Kenny, S., Korba, L.: Applying Digital Rights Management Systems to Privacy Rights. Computers & Security, vol. 21, no. 7, pp. 648-664. (2002)
9. Sheppard, N. P., Safavi-Naini, R.: Protecting Privacy with the MPEG-21 IPMP Framework. In Proc. 6th Workshop on Privacy Enhancing Technologies, vol. 4258, pp. 152--171, December 2006.
10. Carreras, A., Barbosa, V., Kodikara Arachchi, Dogan, S., Andrade, M. T., Delgado, J., Rodríguez, E., Kondoz, A. M.: Context-aware and DRM-enabled content adaptation platform for collaboration applications. IEEE Multimedia J. (2009)
11. Carreras, A., Delgado, J.: A new type of contextual information based on the adaptation authorisation. In Proc. 9th Int. Workshop on Image Analysis for Multimedia Interactive Services (WIAMIS). (2008)
12. Extensible Markup Language (XML) 1.0 (Fifth Edition) W3C Recommendation 26 November 2008. http://www.w3.org/TR/xml/.
13. Wolfgang Meier. eXist: An Open Source Native XML Database. Web-Services, and Database Systems, NODe 2002 Web and Database-Related Workshops
14. W3C. XQuery 1.0 and XPath 2.0 Data Model (XDM). W3C Recommendation 23 January 2007. W3C, http://www.w3.org/TR/xpath-datamodel/, 2007.
15. Edgar F. Codd, A Relational Model of Data for Large Shared Data Banks, Communications of the ACM, 13(6):377-387, June 1970.
16. Naguib, H., Coulouris, G., Mitchell, S.: Middleware support for context-aware multimedia applications. In Proc. DAIS. IFIP Conference Proceedings, vol. 198, pp. 9--22. (2001)
17. Mantoro, T., Johnson, C.: Location history in a low-cost context awareness environment. In Proc. Australasian information security workshop conference on ACSW frontiers, pp. 153—158. (2003)
18. Zittrain, J.: What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication. Stanford Law Review, vol. 52. (2000)
19. Carreras, A., Andrade, M. T., Masterton, T., Kodikara Arachchi, H., Barbosa, V., Dogan, S., Delgado, J., Kondoz, A. M.: Conetxtual information in virtual collaboration systems beyond current standards. In Proc. 10th Workshop on Image Analysis for Multimedia Interactive Services (WIAMIS'09), pp.209-213, ISBN: 978-1-4244-3609-5. (2009)