Location Constraints in Digital Rights Management

Adam Muhlbauer [1], Reihaneh Safavi-Naini [2], Farzad Salim, Nicholas Paul Sheppard *, Martin Surminen [1]

School of Computer Science and Software Engineering, University of Wollongong, NSW, 2522, Australia

Abstract

Digital rights management allows information owners to control the use and dissemination of electronic documents via a machine-readable *licence*. This paper describes the design and implementation of a system for creating and enforcing licences containing location constraints that can be used to restrict access to sensitive documents to a defined area. Documents can be loaded onto a portable device and used in the approved areas, but cannot be used if the device moves to another area. Our contribution includes a taxonomy for access control in the presence of requests to perform non-instantaneous controlled actions.

Key words: digital rights management, access control, location, HTTP-Enabled Location Delivery

1. Introduction

Electronic devices for accessing information are becoming increasingly mobile. There are, however, a number of scenarios in which the owner of some information might want to restrict access to that information to a particular geographical area. For example, companies want to prevent sensitive trade secrets and intellectual property from leaving the boundaries of their offices, and publishing houses want to maximise the value of their publications in different geographic markets.

Over the past decade, digital rights management ("DRM") has become an important technology in the protection of copyrighted multimedia works, sensitive corporate information and private data. DRM allows information owners to control the use and dissemination of electronic files via a machine-readable *licence* that sets out the terms and conditions under which a file can be used.

A licence for a file sets outs who may access the file, what they may do with it, and under what conditions they may do it. In this paper, we are principally concerned with licences that restrict the use of files to a particular geographical area, such as the physical premises of an organisation or a particular legal jurisdiction. We will give an overview of digital rights management and location constraints in Section 3.

Enforcing location-based access control policies requires the access control enforcement point to be aware of the movement of a mobile device during the exercise of a controlled action. We introduce a taxonomy for access control systems in the presence of non-instantaneous actions in Section 4.

We then present our implementation of a location-aware digital rights management system in Section 5. Our implementation is based on the MPEG-21 Intellectual Property Management and Protection ("IPMP") Components [1] and supports non-instantaneous "play"

* Corresponding author. Tel.: +61 2 4221 3995. Fax: +61 2 4227 3277.

Email addresses: adam.muhlbauer@andrew.com (Adam Muhlbauer), rei@cpsc.ucalgary.ca (Reihaneh Safavi-Naini), fsalim@uow.edu.au (Farzad Salim), nps@uow.edu.au (Nicholas Paul Sheppard), martin.surminen@andrew.com (Martin Surminen).

[1] Present address: Andrew Corporation, PO Box U40, University of Wollongong, NSW 2500, Australia.

[2] Present address: Department of Computer Science, 2500 University Dr. NW, Calgary AB T2N 1N4, Canada.

actions by polling a trusted location information server using the HTTP-Enabled Location Delivery ("HELD") protocol [2]. The digital rights management approach allows for location constraints to be imposed on electronic files in a straightforward and transparent fashion, and use of the HELD protocol allows our system to take advantage of future developments in location determination technology without the need for end users to upgrade their devices.

Finally, Section 6 presents and evaluation of our prototype and discusses the issues facing the deployment of a security system of this kind.

2. Related Work

Numerous systems have been proposed for determining or verifying the location of a mobile device. For access control decisions, we require the location of a mobile device to be verified such that a dishonest user cannot fake his or her location. Many such systems have been proposed, based on WiFi networks [3–11], GPS [8,12–16], cellular telephone networks [13,15,17–19], RFID [20] and other sensor networks [21–23].

Each of these systems has a number of advantages and disadvantages relative to other systems. WiFi networks, for example, can provide very high accuracy in indoor environments with existing networks, while cellular telephone networks provide lower accuracy but higher existing coverage in outdoor areas. Furthermore, the location technologies available to be used may vary according the nature of the devices to be located.

In this paper, we are not concerned with the particular method by which a device is located. We assume that we have a trusted location provider able to securely locate a device. The location provider may use any method that it deems appropriate for the nature of the area and the device to be located, without affecting the DRM system discussed in this paper.

Many authors have also proposed models for access control policies that include rules about location or other context information [24–34], and both of most prominent languages used for writing digital rights management licences – the Extensible Rights Markup Language ("XrML") [35] and the Open Digital Rights Language [36] – support clauses that constrain the use of a file to a particular location.

Mundt [16] proposes a DRM system in which a device checks location constraints using an on-board GPS-like receiver. In our prototype, the location of the terminal is determined by an off-board location provider that may use any technology deemed to be appropriate.

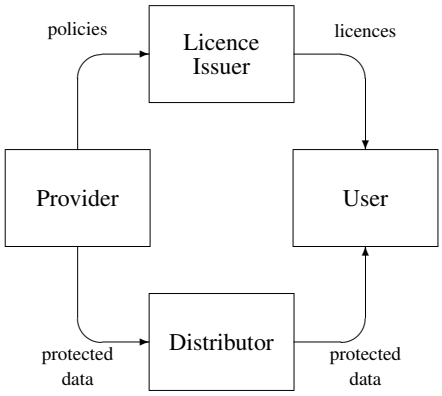


Fig. 1. The components of a digital rights management system.

Al-Muhtadi, et al. [37] propose a location-aware access control system in which sensitive computer files are encrypted with a secret key that is accessible only in the region in which the files are to be accessed. This approach has some similarities to ours, in which a secret key is only made available if the conditions of a licence are satisfied. Our prototype, however, separates the expression of an access control policy from its enforcement, which allows arbitrarily expressive policies to be supported in a straightforward and modular way.

Tolone, et al. [27] point out the need for context-based access control systems to account for actions that take a non-zero time to complete, since the context that enabled an action to begin may change prior to the action being completed. The only systems of which we are aware that implement access control of this sort are those of Lee, et al. [38] and White, et al. [39], which both implement what we will call the "event-based" model. We will consider other methods of enforcement and develop a taxonomy for them in Section 4.

3. Digital Rights Management

Figure 1 shows our reference model for a DRM system. Information is created by a *provider*, and transmitted in a protected (for example, encrypted) form to a *user* via some distribution channel. In order to access the protected data, the user must obtain a *licence* from the *licence issuer*.

Licences are written in a machine-readable *rights expression language* that sets out the terms of use of the data and the information required to access the protected content. We use the MPEG Rights Expression Language [40] in this paper.

The fundamental security requirement for a DRM system is that the hardware and/or software used to

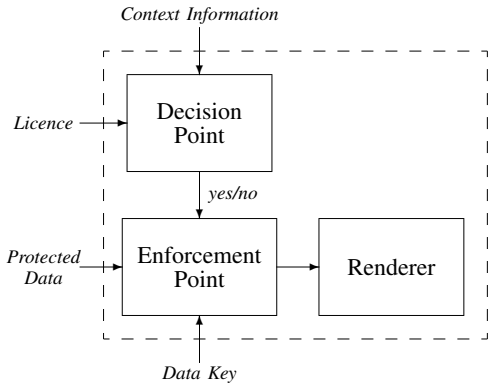


Fig. 2. The components of a terminal.

access protected data be guaranteed by its manufacturer to behave in accordance with licences. For the purposes of this paper, a *terminal* is an abstract single-user player, editor, or similar that may be implemented as a hardware device, a software application or combination of the two.

Figure 2 shows our reference model for a terminal. When a user wishes to perform some particular action on a particular item of data, the *decision point* checks that the user possesses a licence that permits that action. It further checks that the licence has been signed by a recognised licence issuer, and that any conditions associated with the permission are satisfied. If a suitable licence does not exist, or the conditions are not satisfied, the decision point will refuse to carry out the operation. Otherwise, the *enforcement point* will be permitted to retrieve the data key, and the *renderer* enabled to carry out the desired operation.

3.1. *Location Constraints*

In general, the human user of a terminal, the enforcement point, the decision point and the renderer may be separated by arbitrarily large distances – speakers may be connected to a music player via an arbitrarily long cable, for example, or someone may view a screen through a telescope. For ease of exposition of this paper, we assume that the renderer, decision point and enforcement point all are contained within a monolithic terminal whose components cannot be separated and whose location can be securely determined, such as a laptop computer or mobile telephone. It is possible, however, to apply our system to non-monolithic terminals so long as the decision point is able to determine the location of renderer as distinguished from itself, as in [41].

Technologies for locating devices have varying degrees of accuracy, with errors ranging from less than a metre for special-purpose wireless networks up to hundreds of metres or more for GSM telephone networks. Inaccuracies in location information may cause location conditions to be enforced incorrectly by the access control system: a user might be either incorrectly given permission to perform an action if his or her terminal is incorrectly located within a permitted area, or might be incorrectly refused permission if his or her terminal is incorrectly located outside the permitted area.

In the present paper, we assume that the inaccuracy in a location measurement is insignificant compared to the distance over which a device would need to travel in order to defeat the system. For example, an error of a few metres seems acceptable if leaking company information to a competitor requires travelling to an office several kilometres away. Some other suggestions for handling inaccuracy in location measurements for access control can be found in [34].

4. Access Control for Non-Instantaneous Actions

In traditional access control, we tend to think of actions as being instantaneous. For example, a process is either permitted to open a file for reading, or it is not; there is no option to control the period of time (for example) for which the file may be open. Access control systems with continuing actions appear to have inspired interest only very recently [27,38,39].

In a context-aware access control system, it may be possible to circumvent an instantaneous access control decision by initiating an action while in an approved context, then moving to an unapproved context without completing the action. For example, a dishonest employee might open a document on a laptop computer while in a company's offices, then take the computer to a competitor's office without closing the document.

We define the *precision* of a non-instantaneous access control system as the time taken for an access control decision to be updated after a context change occurs affecting that decision. In general, there is a trade-off between the precision of a system and the cost of implementing it. We will discuss the trade-offs for individual mechanisms below.

Note that the methods listed below are not mutually exclusive: it is possible to implement a system in which a device can both poll the context manager and react to events sent to it by the context manager, for example, or in which starting a new action forces an otherwise poll-based system to obtain new context information.

4.1. *Trivial Models*

The trivial option is to simply allow an action to continue indefinitely once it has been approved, regardless of any changes in context. Obviously this option is only appropriate where the value of the protected data is ephemeral.

4.2. *Event-Based Models*

The systems proposed by Lee, et al. [38] and White, et al. [39] are examples of *event-based* systems in which some context manager is able to notify the access control system when an environment condition ceases to be true. For Lee, et al. and White, et al., notification is provided by an existing ubiquitous computing network, which may be expensive to implement if it does not exist already.

Event-based systems are very precise, but are obviously susceptible to tampering with the channel that communicates events to the access control decision point. If an attacker is able to mount a denial-of-service attack on the channel, the access control decision point may not receive an event indicating that an access control decision must be reversed.

4.3. *Poll-Based Models*

The prototype described in this paper is an example of a *poll-based* system in which the access control decision point requests updated context information at regular intervals. Polling can resist denial-of-service attacks by reversing an access control decision if context information cannot be obtained.

Poll-based systems are straightforward to implement, and precision can be traded against computational cost by varying the interval at which new context information is requested. We chose polling for our system due to the ease with which an existing location service could be incorporated into our application without modifying the existing infrastructure, and because it is easy for the licence issuer to make a good estimate of the required polling frequency by considering the size of the area described by a location constraint.

4.4. *Exclusion-Based Models*

A user can be given incentive to cease performing an action by excluding him or her from performing further actions until the first action is stopped. This forces context-dependent conditions to re-checked every time the user requests to perform an action.

Exclusion-based systems obviously have low precision, and are only effective if principals have an incentive to constantly perform new actions. However, they can be implemented with very little infrastructure and eliminate the need for the access control decision point to be in constant contact with the context manager.

4.5. *Prevention-Based Models*

Rather than reverse an access control decision should some relevent context change, an access control system may be able to *prevent* context from changing by forbidding any actions that would cause an unacceptable change in context. For example, upon opening a document that may only be read in a given room, the access control system may cause the door to the room to lock until the document is closed.

In many applications, prevention-based systems may be prohibitively expensive, socially unacceptable or simply impossible. Where practical, however, such systems can provide very high precision and security, and may be useful in small-scale high-security scenarios.

5. Location-based DRM Prototype

We developed a prototype location-based DRM system called *IPLocDRM* (for "Internet Protocol Location DRM"). IPLocDRM allows information providers to cryptographically protect their files in such a way as to permit access only when the renderer is located within a particular location. The DRM system on which IPLocDRM is based supports conditions other than location, but we will only discuss the location condition in this paper.

5.1. *DRM Implementation*

The IPLocDRM prototype is based on the Smart Internet Technology Digital Rights Management system ("SITDRM") [42], a DRM framework based on the MPEG-21 Multimedia Framework [43] developed by the Co-operative Research Centre for Smart Internet Technology, Australia.

The MPEG-21 Multimedia Framework is centred on the notion of a *digital item*, which represents a hierarchical collection of multimedia objects using the Digital Item Declaration Language ("DIDL"). The IPMP Components define a mechanism by which vendor-specific

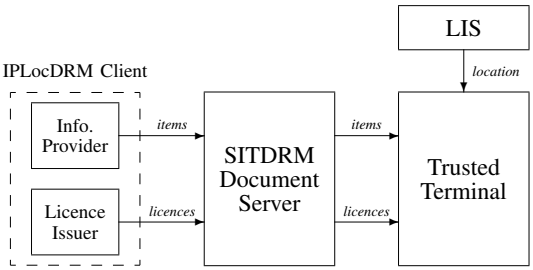


Fig. 3. The IPLocDRM system.

IPMP tools may be associated with *governed* (rights-managed) elements. IPMP tools are plug-ins that implement particular decryption, key management and other algorithms. IPLocDRM adds a location-aware IPMP tool that interprets location constraints and retrieves location information.

Licences are written using the MPEG Rights Expression Language ("MPEG REL"). Each licence contains a collection of *grants* issued by some licence issuer. Each grant awards some *right* over some specified *resource* to a specified *principal*, that is, user of a resource. Grants may be subject to *conditions*, such that the right contained in the grant cannot be exercised unless the condition is satisfied. We will describe the licences used in our prototype in Section 5.3.

IPLocDRM's cryptographic architecture is similar to that used by other DRM systems. Every trusted terminal T is assumed to possess a public key K_T whose authenticity can be verified using some public key infrastructure. The corresponding private key $\bar{K}_T$ is known only to the terminal; in particular, it is not known to the human user of the terminal.

Every governed resource x is encrypted with a unique symmetric resource key k_x. Any licence that grants permission to access a resource x on a terminal T must contain k_x encrypted by K_T, and be digitally signed by the owner of x. In this way, only T is able to extract k_x and therefore x; and T will only accept licences that were issued by the owner of x. Since T is trusted to comply with the conditions imposed by the grant, only the uses permitted by the grant are possible.

5.2. *IPLocDRM Architecture*

The IPLocDRM prototype adapts the existing SITDRM architecture, shown in Figure 3. The high-level components are separated logically and communicate via a network, using web services or (in the case of location information) using the HTTP-Enabled Locaton Delivery ("HELD") protocol [2].

Location information is provided by a Location Information Server ("LIS") - a device capable of determining the location of an IP-enabled device within its network of influence, and respond to location requests using HELD. Our prototype uses the current open source LIS under development by Andrew Corporation, which is capable of providing location within a wired IP network [44].

The IPLocDRM Client (shown in Figure 4) is a location-aware Java GUI application used by both the information provider and licence issuer to create and submit documents to the SITDRM document server The document server then serves these documents and licences in response to requests from terminals.

When the user (logged into a trusted terminal) attempts to perform an action associated with a location condition, our IPMP tool requests the terminal's current location from the LIS. If the location condition is satisfied, access is granted and a periodic location checking process is initiated to enforce this condition over an indefinite amount of time.

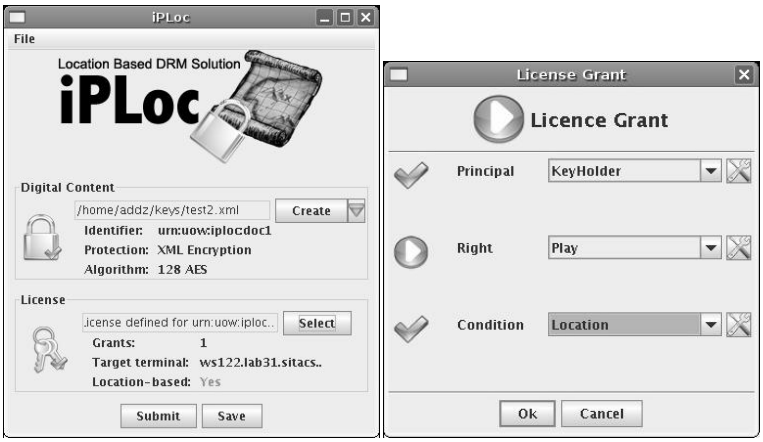
5.3. *The* `Territory` *Condition*

MPEG REL uses the `Territory` condition to bind a grant to a geographic region. An example similar to the licences used in our prototype is shown in Figure 5. This licence permits a principal that possesses a private key corresponding to a given public key (omitted for brevity) to "play" (view) the document `urn:uow:iploc:doc1` if his or her device is located at 1 Crown St in Wollongong, Australia.

The prototype uses the civic location (that is, street address) format due to the ease with which it can be defined by a licence issuer. This format, however, may lack granularity for certain applications, such as restricting use in non-urban regions such as parks and wilderness. The HELD protocol also supports a geodetic (that is, longitude and latitude) format that may be more appropriate in these scenarios.

Civic locations are compared by requiring all of the non-empty fields of the condition to match the corresponding fields returned by the location provider. This allows a match to be made if the location provider supplies information that is more specific than that in the licence. Geodetic locations can be compared using straightforward geometric methods.

A `Territory` condition is composed of a single `LocationProvider` element defining an external service from which to request location information, and one or more `LocationInfo` elements describing a



(a) (b)

(c)

Fig. 4. IPLocDRM: (a) protecting a document; (b) issuing a licence; and (c) adding a `Territory` condition.

```
<r:license>
  <r:grant>
    <r:keyHolder>
      <r:info>
        <dsig:KeyValue>
          <dsig:RSAKeyValue>
            ...
          </dsig:RSAKeyValue>
        </dsig:KeyValue>
      </r:info>
    </r:keyHolder>
    <mx:play/>
    <mx:diReference>
      <mx:identifier>
        urn:uow:iploc:doc1
      </mx:identifier>
    </mx:diReference>
    <sx:territory>
      <sx:LocationProvider>
        <sx:Handler>
          au.edu.uow.iploc.held.HeldClient
        </sx:Handler>
        <sx:Url>
          https://lis.informatics.uow.edu.au
        </sx:Url>
      </sx:LocationProvider>
      <sx:LocationInfo>
        <sx:PollFrequency>
          20000
        </sx:PollFrequency>
        <sx:CivicLocation>
          <cl:country>AU</cl:country>
          <cl:A1>NSW</cl:A1>
          <cl:A3>Wollongong</cl:A3>
          <cl:A6>Crown</cl:A6>
          <cl:HNO>1</cl:HNO>
          <cl:PC>2500</cl:PC>
        </sx:CivicLocation>
      </sx:LocationInfo>
    </sx:territory>
  <r:grant>
</r:license>
```

Fig. 5. An MPEG REL licence binding playback to a particular location.

location and the frequency with which the condition should be checked. This allows the licence issuer to specify a location provider that he or she trusts.

For convenience, locations are described using the *Presence Information Data Format Location Object* ("PIDF-LO") format used by HELD rather than the similar format used in the MPEG REL specification. Both formats only allow locations to be specified in a positive fashion in that they specify where a device must be rather than where it must not be. Negative conditions such as "playing is permitted if the principal is not located in a moving vehicle" could be implemented using a "not" operator, but our prototype does not yet support this.

Binding the poll frequency to the defined location has two main advantages. Firstly, our solution does not have to explicitly acknowledge any difference in scale between locations. Furthermore, by specifying the poll frequency at the time of licence creation, the licence issuer has control over the specific value. When the licence is created, a decision can be made on an appropriate timing interval based on a number of factors including the total area of the restricted region, the sensitivity of the information being accessed, and any specific organisational information or security polices.

6. IPLocDRM Evaluation

6.1. *Channel Security and Trust*

Since the accuracy of location information is critical to enforcing a grant, it is necessary to authenticate the identity of the LIS and ensure the integrity of the location information received. The HELD protocol provides integrity and authentication of location information using the Transport Layer Security ("TLS") protocol [45], and this method is employed by IPLocDRM.

The integrity of the distribution channels used to transmit a governed resource and its corresponding licence is less critical to the security of the system. As described in Section 5.1, a governed resource is protected by a unique symmetric key which is in turn protected by the terminal's public key and stored in the licence. Assuming that the terminal is trusted, we do not require trusted distribution channels.

IPLocDRM allows the licence issuer to verify the trustworthiness of the LIS, while the terminal must verify its identity at run-time. As mentioned in Section 5.3, the licence issuer supplies the URL of a LIS deemed to provided accurate location information by organisational process or policy outside the scope of IPLocDRM. When the terminal uses TLS to contact the LIS, a decision must still be made whether to accept the presented certificate (and hence the LIS's identity) or not.

It should be noted that the HELD protocol can determine the location of a trusted terminal, but not that of its user. Terminals can, however, provide some assurance of the location of their users by rejecting access to location sensitive information if a user is logged in via some remote log-in service.

6.2. *Location Mechanism*

Using an off-board location provider for IPLocDRM allows the system to scale across multiple networks, potentially using different access technologies. So long

as the terminal is in a network covered by the LIS that is able to provide location with an accuracy acceptable to the licence issuer, the system will work, and IPLocDRM can operate independently of the network that the terminal is in without modification.

IPLocDRM uses polling to ensure that an action is halted should a `Territory` condition cease to be satisfied. It is up to the creator of a licence to determine the frequency with which polls will be conducted, such that a user cannot make sensitive changes to his or her location between poll events. Intuitively, we expect licence creators to choose lower frequencies for larger areas, and higher frequencies for smaller areas, since it would take a user a longer time to move from one large area to another (e.g. from city to city) as compared to small areas (such as buildings).

By this fact, we note that a poll-based model for access control decisions is more appropriate when used with medium to large restricted regions – such as an entire office building. Restricting access to a smaller scale region (for example, individual rooms within an office) might require a very high poll rate and still lead to imprecise access control decisions.

An event-based model, as described in Section 4.2, provides more precise access control for smaller regions by detecting when the user moves and notifying the access control system. Unfortunately, implementing an event-based model using the HELD protocol is difficult, as all forms of HELD requests provide location only when executed. Implementing an event-based (or prevention-based) model requires an additional context-aware network to be developed and deployed, possibly at very high expense.

7. Summary

IPLocDRM shows how digital rights management can be used to restrict access to electronic files to a particular location. IPLocDRM's licence interpreter is independent of the form of location determination in use, and allows licence issuers to specify which location providers they trust to deliver accurate and reliable location information using the HTTP-Enabled Location Delivery protocol.

IPLocDRM uses a simple polling mechanism to prevent users from defeating the system by opening documents in a permitted location, then moving their viewing device to an unpermitted location without closing the device. Other mechanisms are possible, however, and we have proposed a taxonomy for access control in the presence of non-instantaneous actions.

The digital rights management approach allows new conditions to be added to an access control policy in a straightforward way, and allows all policy information to be gathered and processed by a single component. This allows the data protection system to be designed in a modular and consistent fashion.

8. Acknowledgements

We would like to thank members of the Andrew Corporation in Wollongong for stimulating discussion on this project. We would also like to thank the Co-operative Research Centre for Smart Internet Technology for allowing us to use the SITDRM software as the basis of our prototype.

References

[1] International Standards Organisation, Information technology – multimedia framework (MPEG-21) – part 4: Intellectual property management and protection components, ISO/IEC 21000-4:2006.

[2] J. Winterbottom, M. Thompson, B. Stark, HTTP enabled location delivery (HELD), Internet Draft, `http://www.ietf.org/internet-drafts/draft-winterbottom-http-location-delivery-05.txt` (2 March 2007).

[3] P. Bahl, V. N. Padmanabhan, RADAR: An in-building RF-based user location and tracking system, in: Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies, 26-30 March 2000, pp. 775–784.

[4] P. Castro, P. Chiu, T. Kremenek, R. Muntz, A probabilistic room location service for wireless networked environments, in: Ubicomp, 2001, pp. 18–34.

[5] T. Roos, P. Myllymäki, H. Tirri, P. Misikangas, Sievänen, A probabilistic approach to WLAN user location estimation, International Journal of Wireless Information Networks 9 (3) (2003) 155–164.

[6] P. Tao, A. Rudys, A. M. Ladd, D. S. Wallach, Wireless LAN location-sensing for security applications, in: ACM Workshop on Wireless Security, 2003, pp. 11–20.

[7] M. A. Youssef, A. Agrawala, A. Udaya Shankar, WLAN location determination via clustering and probability distributions, in: Pervasive Computing and Communications, 2003, pp. 143–150.

[8] T. Mundt, Two methods of authenticated positioning, in: Second ACM Workshop on QoS and Security for Wireless and Mobile Networks, 2 October 2006, pp. 25–32.

[9] M. J. Surminen, N. P. Sheppard, R. Safavi-Naini, Location-based DRM using WiFi access points, in: International Symposium on Communications and Information Technology, Sydney, Australia, 2007, pp. 882–886.

[10] Newbury Networks, WiFi Watchdog, `http://www.newburynetworks.com/products-watchdog.htm` (2006).

[11] Ekahau, Ekahau, `http://www.ekahau.com` (2007).

[12] D. E. Denning, P. F. MacDoran, Location-based authentication: Grounding cyberspace for better security, Computer Fraud and Security (February 1996) 12–16.

[13] E. Gabber, A. Wool, How to prove where you are: Tracking the location of customer equipment, in: Fifth Conference on Computer and Communications Security, 1998, pp. 142–149.

[14] B. Hulsebosch, A. Salden, M. Bargh, Context-based service access for train travelers, in: European Symposium on Ambient Intelligence, 2004, pp. 84–87.

[15] U. Greveler, Enforcing regional DRM for multimedia broadcasts without trusted computing, in: Digital Rights Management: Technologies, Issues, Challenges and Systems, 2005, pp. 345–353.

[16] T. Mundt, Location dependent digital rights management, in: Tenth IEEE Symposium on Computers and Communications, 2005, pp. 617–622.

[17] M. Looi, Enhanced authentication services for Internet systems using mobile networks, in: IEEE Global Telcommunications Conference, 2001, pp. 3468–3472.

[18] C. Wullems, M. Looi, A. Clark, Enhancing the security of Internet applications using location: A new model for tamper-resistant GSM location, in: Eighth IEEE International Symposium on Computers and Communication, 30 June - 3 July 2003, pp. 1251–1258.

[19] Ericsson, Mobile positioning system, `http://www.ericsson.com/mobilityworld/sub/open/technologies/mobile_positioning/index.html` (17 February 2007).

[20] K. Nakanishi, J. Nakazawa, H. Tokuda, LEXP: Preserving user privacy and certifying location information, in: Second Workshop on Security at the Ubicomp Conference, 2003.

[21] N. Sastry, U. Shankar, D. Wagner, Secure verification of location claims, in: ACM Workshop on Wireless Security, 2003, pp. 1–10.

[22] T. Kindberg, K. Zhang, N. Shankar, Context authentication using constrainted channels, in: Fourth IEEE Workshop on Mobile Computing Systems and Applications, 2002, pp. 14–21.

[23] A. Vora, M. Nesterenko, Secure location verification using radio broadcast, in: Eighth International Conference on Principles of Distributed Systems, 15-17 December 2004, pp. 369–383.

[24] M. J. Covington, W. Long, S. Srinivasan, A. K. Dey, M. Ahamad, G. D. Abowd, Securing context-aware applications using environment roles, in: ACM Symposium on Access Control Models and Technologies, 2001, pp. 10–20.

[25] G. Sampemane, P. Naldurg, R. H. Campbell, Access control for active spaces, in: Annual Computer Security Applications Conference, 2002, pp. 343–352.

[26] F. Hansen, V. Oleshchuk, Spatial role-based access control model for wireless networks, in: IEEE Vehicular Technology Conference, 2003, pp. 2093–2097.

[27] W. J. Tolone, R. A. Gandhi, G.-J. Ahn, Locale-based access control: Placing collaborative decisions in context, in: IEEE International Conference on Man, Systems and Cybernetics, 5-8 October 2003, pp. 4120–4127.

[28] A. Corradi, R. Montanari, D. Tibaldi, Context-based access control for ubiquitous service provisioning, in: International Computer Software and Applications Conference, 2004, pp. 444–451.

[29] E. Bertino, B. Catania, M. L. Damiani, P. Perlasca, GEO-RBAC: A spatially aware RBAC, in: ACM Symposium on Access Control Models and Technologies, 2005, pp. 29–37.

[30] W. Han, J. Zhang, X. Yao, Context-sensitive access control model and implementation, in: International Conference on Computer and Information Technology, 2005, pp. 757–763.

[31] R. J. Hulsebosch, A. H. Salden, M. S. Bargh, P. W. G. Ebben, J. Reitsma, Context sensitive access control, in: ACM Symposium on Access Control Models and Technologies, 2005, pp. 111–119.

[32] I. Ray, L. Yu, Short paper: Towards a location-aware role-based access control model, in: First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 5-9 September 2005, pp. 234–236.

[33] M. L. Damiani, E. Bertino, Architectural issues for a location-aware role-based access control system, in: ACM Symposium on Applied Computing, 23-27 April 2006, pp. 1184–1185.

[34] S. K. S. Gupta, T. Mukherjee, Venkatasubramanian, T. B. Taylor, Proximity based access control in smart-emergency departments, in: Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, 12-17 March 2006.

[35] ContentGuard, Extensible Rights Markup Language, `http://www.xrml.org` (2004).

[36] Open Digital Rights Language Initiative, The Open Digital Rights Language Initiative, `http://odrl.net` (2004).

[37] J. Al-Muhtadi, R. Hill, R. Campbell, M. D. Mickunas, Context and location-aware encryption for pervasive computing environments, in: Fourth Annual IEEE Conference on Pervasive Computing and Communications Workshops, 13-17 March 2006.

[38] A. J. Lee, J. P. Boyer, C. Drexelius, P. Naldurg, R. L. Hill, R. H. Campbell, Supporting dynamically changing authorizations in pervasive communications systems, in: Second International Conference on Security in Pervasive Computing, 2005, pp. 134–150.

[39] M. White, B. Jennings, V. Osmani, S. van der Meer, Context driven, user-centric access control for smart spaces, in: IEE International Workshop on Intelligent Environments, 2005, pp. 13–19.

[40] International Standards Organisation, Information technology – multimedia framework (MPEG-21) – part 5: Rights expression language, ISO/IEC 21000-5:2004.

[41] A. W. Dent, A. Tomlinson, Regional blackouts: Protection of broadcast content on 3G networks, in: Fifth IEE Conference on 3G Mobile Communication Technologies, 2004, pp. 442–446.

[42] N. P. Sheppard, R. Safavi-Naini, Protecting privacy with the MPEG-21 IPMP framework, in: International Workshop on Privacy Enhancing Technologies, Cambridge, UK, 2006, pp. 152–171.

[43] International Standards Organisation, Information technology – multimedia framework (MPEG-21) – part 1: Vision, technologies and strategy, ISO/IEC 21000-1:2001.

[44] Andrew Corporation, Open source HELD: LIS and client, `http://held-location.sourceforge.net` (2007).

[45] T. Dierks, C. Allen, The TLS protocol: Version 1.0, RFC 2246 (1999).

Adam Muhlbauer received BMath and BCompSc degrees from the University of Wollongong in 2007. His research interests focus on Location Based Applications, Cryptography and Network Security. He is currently employed by Andrew Corporation as a software engineer, developing next generation IP Location solutions.

Reihaneh Safavi-Naini is iCORE Chair in Information Security at the University of Calgary. She holds a Ph.D. in electrical and computer engineering from University of Waterloo. Her research interests include cryptography, computer and communication security, multimedia security, and digital rights management.

Farzad Salim is a Research Fellow in the School of Computer Science and Software Engineering at the University of Wollongong, Australia. His fields of interest include privacy, policy consistency checking, access control and digital rights management. Farzad completed a M.Sc in Computer Science at the University of Wollongong in 2006 focusing on redundancy detection and resolution within a formal privacy policy language.

Nicholas Sheppard received BSc and BE degrees from the University of Queensland in 1996, and a PhD from the University of Sydney in 2001. He has since worked as a Research Fellow at the University of Wollongong and Co-operative Research Centre for Smart Internet Technology. His research interests include digital rights management, privacy, and mobile computing.

Martin Surminen received a BCompSc degree from the University of Wollongong in 2004. He is currently employed by Andrew Corporation as a software engineer, developing next generation IP Location solutions.