2008

Modelling social networks as authorised domains with decay

Nicholas Sheppard
University of Wollongong, nps@uow.edu.au

Reihaneh Safavi-Naini
University of Wollongong, rei@uow.edu.au

Modelling social networks as authorised domains with decay

Abstract

Sharing multimedia among friends and acquaintances is a common practice that, in appropriate settings, need not be detrimental to the interests of copyright owners. In this paper, we propose a model for sharing multimedia based on the notion of an acquaintance domain whose members will have access to the domain owner's multimedia. Membership of an acquaintance domain is determined by the closeness of a relationship – where "closeness" can be defined by factors such as the frequency of visits – and membership of the domain deteriorates as the relationship becomes more distant. We have made an implementation of the proposal based on the Open Mobile Alliance's specification for an authorised domain.

Disciplines

Physical Sciences and Mathematics

Publication Details

Sheppard, N. P. & Safavi-Naini, R. (2008). Modelling social networks as authorised domains with decay. In R. Grimm, B. Hass & J. Nutzel (Eds.), Virtual Goods: Technology, Economy and Legal Aspects (pp. 183-195). New York: Nova Science Publishers.

Modelling Social Networks as Authorised Domains with Decay

Nicholas Paul Sheppard
School of Computer Science and Software Engineering, University of Wollongong
Northfields Ave, Wollongong NSW 2522, Australia
nps@uow.edu.au

Reihaneh Safavi-Naini
Department of Computer Science, University of Calgary
2500 University Dr. NW, Calgary AB T2N 1N4, Canada
rei@cpsc.ucalgary.ca

Abstract

Sharing multimedia among friends and acquaintances is a common practice that, in appropriate settings, need not be detrimental to the interests of copyright owners. In this paper, we propose a model for sharing multimedia based on the notion of an *acquaintance domain* whose members will have access to the domain owner's multimedia. Membership of an acquaintance domain is determined by the closeness of a relationship – where "closeness" can be defined by factors such as the frequency of visits – and membership of the domain deteriorates as the relationship becomes more distant. We have made an implementation of the proposal based on the Open Mobile Alliance's specification for an authorised domain.

1 Introduction

A typical multimedia user has a social circle consisting of a group of acquaintances with which he or she interacts with varying degrees of frequency. Users often find it desirable to share commercial multimedia amongst these acquaintances [4, 24], but existing digital rights management ("DRM") systems impose strong restrictions on such behaviour in order to protect the copyright interests of multimedia creators.

A small degree of sharing, however, is not necessarily detrimental to the interests of copyright owners [3, 26, 10], and in this paper we propose a simple model for controlled social sharing in digital rights management by adopting and extending the concept of an authorised domain.

An *authorised domain* is a group of devices to which licences to use multimedia works can be issued, such that all of the members of a domain can access the content without requiring multimedia to be licensed to each device individually. Existing authorised domain systems are typically targeted at household domains, in which an authorised domain is set up to cover all of the devices owned by a single household. Rights-managed multimedia purchased by members of the household is licensed to the domain rather than individual devices. New devices enter the domain when a member of the household purchases them, and devices leave the domain when they are discarded or sold.

A simple approach to implementing sharing in social circles is to allow each multimedia user to define an authorised domain into which his or her acquaintances' devices can be enrolled. We will refer to such a domain as an *acquaintance domain*. A device's membership of an acquaintance domain is controlled by the strength of the relationship between the domain's owner and the device's owner, where "strength" can be measured by the frequency of contact between the two or other factors.

Existing schemes for authorised domains are *crisp* – that is, every device is either a member of the domain, or it is not. In Section 3 of the present paper, we introduce the notion of a *fuzzy domain* in which devices may hold an arbitrary degree of membership in the sense of membership in a fuzzy set. We use the notion of fuzziness to model relationships such as "Alice is acquainted with Bob" that do not take on binary truth values.

In Section 4, we introduce the notion of an acquaintance domain through which a purchaser of rights-managed multimedia may share his or her possessions within his or her social circle. Devices may enter an acquaintance domain if their owner is acquainted with the owner of that domain in some sense and we allow membership of an acquaintance domain to decay gracefully over time if acquaintances do not maintain contact.

We describe an implementation of our proposal in Section 5, based on the Open Mobile Alliance's digital rights management system [18]. Finally, we conclude with a discussion of our experiences and topics for future work in Section 6.

2 Previous Work

2.1 Fuzzy Access Control

Fuzzy logic describes a system of reasoning in which the truth value of a statement about an object is represented as its degree of membership of a *fuzzy set* rather than as a binary truth value. For example, Bill – who is 180cm tall – may belong to the set of tall men to a moderate degree, while Frank – who is 190cm tall – belongs to the set of tall men to a high degree. Fuzzy logic is widely used in control applications where some electromechanical controller needs to make decisions about imprecise concepts such as "hot", "fast", etc. A detailed description of the logic can be found textbooks such as Ross' [22], but we require only an understanding of the fuzzy set concept for the purposes of the present paper.

Fuzzy reasoning has been used in a number of access control models, beginning with Hosmer [11, 12] in 1992 and more recently by Casola, et al. [6, 5] in 2004. Fuzzy reasoning is also used in a number of biometric authentication systems, beginning with de Ru and Eloff's typing biometric in [7] in 1997. Al-Muhtadi, et al. [1, 21] use fuzzy reasoning and probabilistic reasoning in a similar vein to combine the "confidence" in the authentication of an entity by sensors in a ubiquitous computing network.

While the foregoing systems use fuzzy reasoning as part of evaluating an access control request, they ultimately return a binary decision to either permit or deny access. In this paper, we use fuzziness to model the degree of “truth” of a statement such as “Alice is acquainted with Bob”. We allow access control decisions to return fuzzy values that can be interpreted as a degree of permission to perform an action, and implemented by reducing the quality of an action in accordance with the degree of permission.

Katzenbeisser, et al. [14] propose a system in which each new multimedia work is shipped with a list of identifiers of unauthorised copies of older works that have been discovered by content providers. Upon receiving each new multimedia work, a multimedia player can check whether or not it has been used to create unauthorised copies in the past. As the number of unauthorised copies found increases, the performance of the player degrades gracefully by applying sanctions such as warnings, reduced playback quality and denial of premium features. Macrovision’s “Fade” technology provides sanctions for unauthorised copies of computer games [9].

The approach of Katzenbeisser, et al. and Macrovision is similar in spirit to the approach used in this paper and the sanctions proposed in those systems can be used to implement the diminished permission proposed in this paper. Our proposal, however, focuses on authorising a specific mode of sharing rather than responding to unauthorised sharing.

2.2 Acquaintance Domains

Microsoft’s Zune portable media player [17] supports a mode of sharing in which one Zune player can obtain a sample version of a piece of music from another Zune player within WiFi range. The receiving player is permitted to play the music three times over a period of three days. The owner of the receiving player can flag the track to be purchased after the sample period if he or she wishes to obtain permanent access to the music. Similar sampling concepts are used in other file-sharing systems such as Weed [23].

In the present paper, we propose a general social sharing model that supports arbitrary methods for determining “acquaintance” between two devices and arbitrary schemes for decaying membership of a domain. Zune’s sharing model can be seen as a specific instance of the model proposed in this paper. The particular implementation described in this paper supports a finer-grained model of sampling in which access to the sample does not end abruptly after a particular number of uses or a particular amount of time.

3 Fuzzy Authorised Domains

Many recent digital rights management systems support the notion of an *authorised domain* [18, 16, 20, 25, 19, 2, 15, 13], shown in Figure 1. An authorised domain is a group of devices to which a *rights issuer* may issue a licence to access a particular multimedia work. Every device in the domain may use the licence without needing to obtain an individual licence.

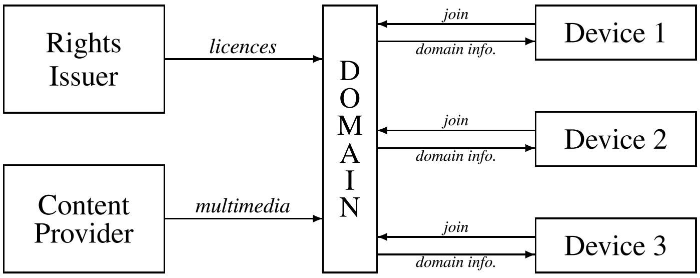


Figure 1: An authorised domain.

Devices may join and leave a domain independently of any licences issued to the domain. The conditions under which devices may join a domain, and the mechanisms for doing so, vary from system to system. In this paper, we will assume that every domain has one or more *permanent members* who are made members of the domain by some central authority. Other devices may become *temporary members* of the domain by contacting one of the permanent members and satisfying some conditions specified by the central authority.

It is easy to extend the notion of an authorised domain to the notion of a *fuzzy domain*, membership of which is modelled as membership of a fuzzy set in fuzzy logic. Every fuzzy domain is associated with an arbitrary *membership function* that, given some information about a domain member, computes a *degree of membership* in the domain ranging from zero (not a member) to one (a full member).

Every device is assumed to contain a licence interpreter that, given a licence and a multimedia work, is able to determine whether or a not that licence permits a domain member to perform some particular action on that work using two-valued logic as normal. If the device is a full member of the domain, it may proceed with the action as normal. If the device is not a member of the domain, it must refuse the action as normal.

If the device is a partial member of the domain, however, it may proceed with the action in some diminished form. Katzenbeisser, et al. suggest a variety of straightforward "sanctions" that represent diminished permission to proceed with an action [14]. These are summarised below, together with some other straightforward sanctions that might be used.

Warning. The player displays a warning before proceeding with the action as normal.

Degradation. The player deliberately reduces the quality of rendering by down-sampling or otherwise degrading the multimedia work.

Denial of premium content. The player permits access to the main body of a composite multimedia work as normal, but denies access to additional features such as extra scenes and bonus tracks.

Fade. Macrovision's "Fade" technology reduces the players' experience of a pirated shooting game over time by gradually reducing the accuracy of their shots and reducing the amount of ammunition they have [9].

Watermarking. The player reduces the quality of rendering by inserting a perceptible watermark into the display and/or audio.

Domain shrinkage. The player reduces the effective number of works available to a diminished member of a domain by making selected multimedia works in the domain inaccessible.

Randomness. The player permits the action to proceed normally with some probably related to the device's degree of membership in a domain.

It is up to the designers of a particular system to determine how a degree of membership is mapped to a degree of sanctioning. For example, the probability of permitting an action may decrease linearly with a decreasing degree of membership, or it may decrease non-linearly in order to achieve some more complex probability distribution.

Obviously not all techniques for implementing diminished actions are applicable to all kinds of media or all kinds of domains. Text, for example, might be deemed to be either readable or unreadable rather than decaying gracefully via down-sampling or watermarking. A fully-featured fuzzy domain system may support a combination of techniques in order to achieve a particular balance of incentives for users.

4 Acquaintance Domains

In this paper, we are specifically concerned with sharing amongst groups formed by social relationships such as friendship, family and common interests. We use a fuzzy authorised domain called an *acquaintance domain* to represent the (devices belonging to the) social circle of a human user.

In social network theory, every person is represented as a node in a social network. A social network is represented as a graph in which a link exists between two nodes if those two people have contact with each other. In a *valued* network, links may be associated with a weight reflecting the strength of the contact. For example, frequent contact may be represented by a high-value link while infrequent contact is represented by a low-value link.

We consider every human user to own an acquaintance domain that represents his or her local area in a social network. While it is possible to consider acquaintance domains that include "acquaintances" that are at distance greater than one from the domain's owner in a social network, we will focus on domains representing the immediate social circle of their owners, that is, that person's immediate neighbourhood in a social network.

All of the devices owned by a particular user are permanent members of that user's acquaintance domain. Assuming that devices can have only one owner, a device may be a permanent member of at most one acquaintance domain at any one time. We assume that users have some means to obtain multimedia works for their acquaintance domain, either by purchasing licences for works directly or by transferring licences from another domain.

Devices that are not owned by the owner of an acquaintance domain may become temporary members of an acquiantance domain upon meeting some criterion indicating that the owner of the incoming device is acquainted with the owner of the acquaintance domain. We will give some example policies below.

The degree of membership of a temporary member of an acquaintance domain diminishes over time according to some membership function determined by the rights issuer. Temporary membership may be renewed by re-asserting the acquaintance criteria. We will give some specific examples of membership functions below.

4.1 Examples

4.1.1 One-Hop Domains

One model of sharing allows the owner of an acquaintance domain to simply nominate a fixed number of acquainted devices. If the number of devices in an acquaintance domain has reached its limit, a device must be expelled before any new devices are admitted. Devices may be explicitly removed from the acquaintance domain by the domain's owner, or may drop out of the domain automatically if their membership is not renewed within, say, one year of joining.

4.1.2 Proximity Domains

Bob is a blues music fan and every week he shares a table with like-minded friends at a blues night at a local bar. Any device within Bluetooth range of Bob's portable music player is permitted to join Bob's acquaintance domain, so anyone at the table is able to renew his or her device's membership of the domain and share in Bob's collection of blues music. Membership of the domain expires after a week so that Bob's friends will lose access to his music collection unless they keep turning up at the blues night.

Suppose Bob meets Alice at a party and finds that Alice is also a blues fan. Bob can make Alice's mobile phone a member of his acquaintance domain so that she can sample some musicians he recommends to her. A week after the party, however, Alice's mobile phone's membership expires and she has to purchase any of the music she has taken a liking to for herself.

5 Implementing Acquaintance Domains

For the purposes of illustration, we chose to implement a fuzzy domain scheme based on Version 2 of the Open Mobile Alliance's digital rights management specification [18]. Our principal reason for choosing OMA DRM is simply that our research group has experience with the OMA DRM specification, and has access to an implementation of the specification. We expect that almost any scheme for managing an authorised domain could be adapted to support fuzzy domains by making modifications similar to those we will describe in this section.

In OMA's digital rights management scheme, every DRM-enabled device is required to contain a tamper-resistant *DRM agent* that is trusted to comply with the rules of the digital rights management scheme.

Any multimedia object can be protected by encrypting it with a unique *content encryption key* ("CEK"). A *rights issuer* who knows the content encryption key can grant permission to use the object by issuing a *rights object* written in a restricted form of the Open Digital Rights Language. The rights object sets out the rules under which the object may be used, and contains the content encryption key in an encrypted form.

OMA DRM Version 2 supports two kinds of rights objects: rights objects that are issued to individual DRM agents, and rights objects that are issued to *domains*. In this paper, we are only interested in the latter kind.

Domains are created by rights issuers. Every domain is associated with a unique *domain key* ("DK") that is used to encrypt the content encryption key in rights objects issued to that domain. A DRM agent may join a domain and obtain the domain key by executing the Join Domain Protocol with the rights issuer that created the domain. It is up to rights issuers to decide whether or not they accept any particular request to join the domain.

Once a DRM agent has joined a domain and obtained the domain key, it may access any rights objects issued to that domain by using the domain key to decrypt the content encryption key in the rights object. A DRM agent can leave a domain voluntarily by executing the Leave Domain Protocol with the rights issuer and deleting the domain key from its memory. It is not normally possible to force a DRM agent to leave a domain, though the specification provides a limited capacity to revoke devices if a domain key becomes compromised. In our implementation, the membership level of a DRM agent in a domain decays over time – potentially to zero – but the DRM agent never executes the Leave Domain Protocol other than voluntarily.

5.1 Fuzzifying OMA Domains

Our scheme does not modify any of the cryptographic aspects of the OMA digital rights management scheme, but requires

- the OMA domain protocols to be extended to associate each domain with a membership function; and
- the OMA DRM agent to be extended to reduce the quality of an action if permission to perform that action is derived from a rights object issued to a domain in which the DRM agent has a reduced degree of membership.

Figure 2 shows the architecture of a DRM agent modified to support fuzzy domains. The rights object interpreter, decryptor and renderer are the same as they would be in an ordinary OMA DRM agent, but the DRM agent's domain information database has been extended to include the information required to compute the membership function (in our case, the time at which the domain was joined, and the half-life of the domain). A mem-

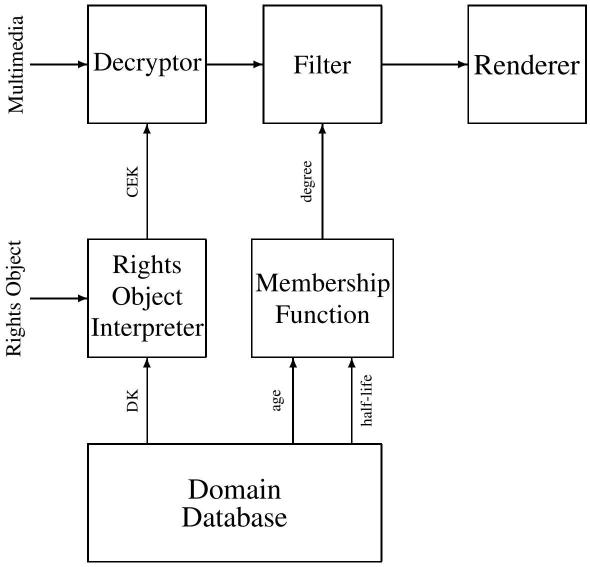


Figure 2: A DRM agent modified to support fuzzy domains.

bership function unit has been added to compute a degree of membership that controls the degree of filtering that occurs between decryption and rendering.

Membership Functions. In general, membership functions for a domain may be chosen arbitrarily by the rights issuer that created the domain. This function must be communicated to a new domain member as part of a successful executation of the Join Domain Protocol, and can be sent in the same message as the one that communicates the domain key to the new member, as shown in Figure 3. The device then stores the function and computes its value every time its user attempts to perform an action on a multimedia work through that domain.

There are a variety of methods that might be used to express membership functions, ranging from defining a fixed number of parameterised functions expressed in XML to defining arbitrary functions in mathematical programming languages such as MATLAB. Of course authors of membership functions must consider what functions can be computed by their target DRM agents: there is no point in creating a domain with a membership function containing location information, for example, for DRM agents that cannot determine their own location.

Sanctions. As for membership functions, a specific type of sanction could be chosen for each domain and communicated to new domain members as part of the Join Domain Protocol. Our existing implementation, however, supports only one sanction, and so there is no need to specify a particular form for each domain.

```
<roap:joinDomainResponse status="Success">
  <roap:deviceID>...</roap:deviceID>
  <roap:riID>...</roap:riID>
  <roap:domainInfo>
    <roap:notAfter>Infinite</roap:notAfter>
    <roap:domainKey>
      <roap:encKey>
        <xenc:KeyInfo>...</xenc:KeyInfo>
      </roap:encKey>
      <roap:riID>...</roap:riID>
      <roap:mac>...</roap:mac>
    </roap:domainKey>
    <roap:membershipFunction>
       starttime = 8 May 2007 13:41:56;
       age = currenttime() - starttime;
       return exp(-0.1 * age);
    </roap:membershipFunction>
  </roap:domainInfo>
  <roap:signature>...</roap:signature>
</roap:joinDomainResponse>
```

Figure 3: The OMA Join Domain Response message extended to contain a membership function, written in a hypothetical programming language.

5.2 Acquaintance Domains in OMA

We wanted our implementation to illustrate a scenario similar to the ones given in Section 4.1. We suppose that some rights issuer has granted an individual with an "acquaintance domain" into which they may place their friends' devices, but the membership level of these devices decays over time if it is not constantly renewed.

Membership Policy. OMA DRM does not specify the policy used by rights issuers to accept or reject requests to join a domain. A rights issuer who has established an acquaintance domain will presumably only accept requests to join the domain from devices that are somehow acquainted with the owner of the domain.

We have not implemented any particular policy in our demonstration software. One useful policy, however, might be to limit the number of devices permitted in an acquaintance domain at any one time, and/or to require that devices be in close physical proximity to the domain owner's mobile phone in order to join the domain. For mobile phones in particular, one method of measuring "proximity" might be to require an incoming phone to be located in the same mobile phone cell as the domain owner's phone. Other methods include use of the time taken for a message to make a round trip from the permanent device to the incoming device [8], and use of a communications medium with limited range, as for Zune.

Membership Renewal. Devices may renew their membership of the domain an arbitrary number of times by executing the Join Domain Protocol as usual. Renewing membership of the domain causes the membership function to be reset so that the effects of any decay are removed. Devices that do not renew their membership will gradually obtain poorer and poorer access to objects in the domain.

Membership Function. We chose a simple parameterised membership function with exponential decay in the time elapsed since the domain was last joined. Every domain is associated with a half-life. The domain membership function starts at 1 at the time of joining a domain, and halves for every half-life that elapses since joining the domain. There is no reason other than convenience for choosing this function.

Sanctions. Our filter reduces the resolution of an image[1] in proportion to the DRM agent's degree of membership in the domain through which the image was accessed. For example, a 1024×768 image will be displayed at 1024×768 until the first half-life elapses, then 512×384 until the second half-life elapses, and so on, as shown in Figure 4. Again, there is no reason other than convenience for choosing this filter.

6 Discussion

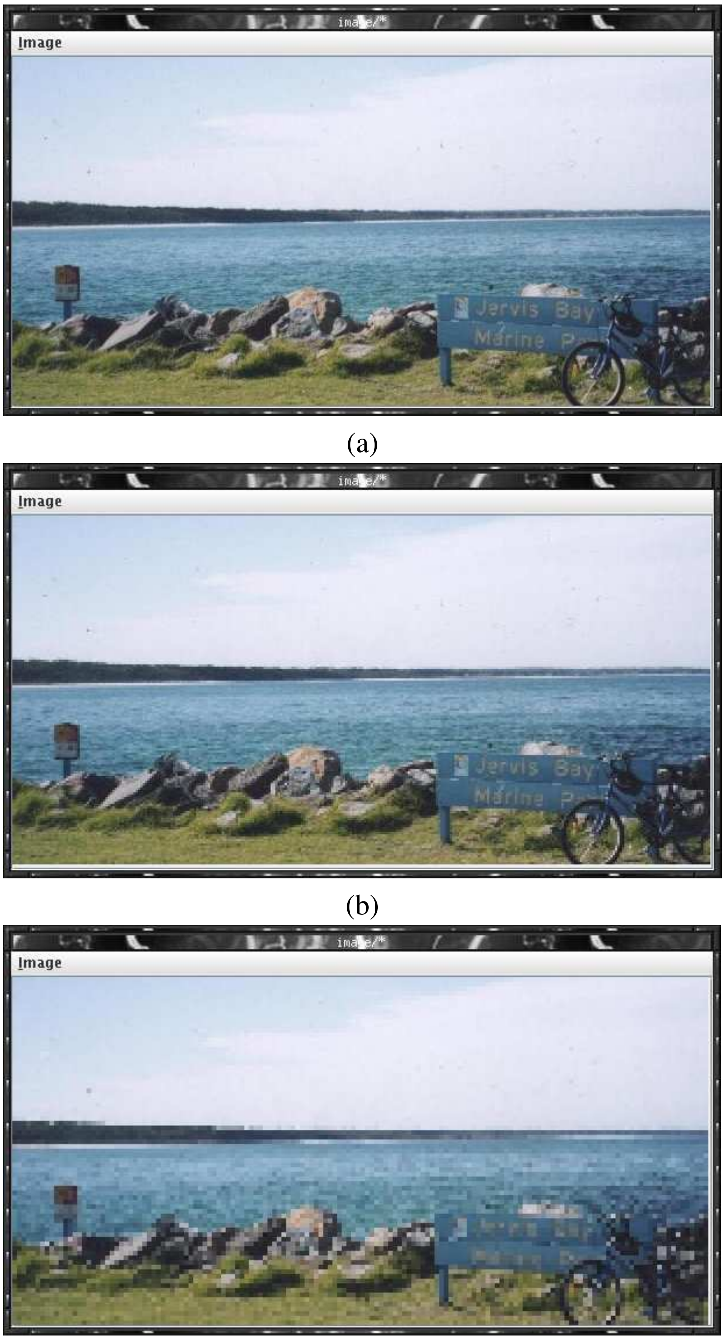
Fuzzy domains provide a general model for representing relationships between devices that do not have simple binary values. In this paper, we have chosen to focus on acquaintance relationships between device owners, but fuzzy domains may be applicable to other scenarios in which it is desirable to allow someone to sample multimedia without taking full possession of it. For example, regular visitors to a shop or other premises could be rewarded with a gradual increase in their level of membership in the premises' domain.

It is natural to ask: what kinds of membership functions and filters might be useful? We do not know the basis on which products such as Zune choose their policies for sample content, and our own membership function and filter were chosen simply for ease of implementation. Alternative membership functions that could be used include:

- piecewise functions that stay constant for a period of time before decaying sharply;
- functions that depend on the history of renewals – for example, decreasing the rate of decay if there have been frequent renewals in the past; and
- functions that depend on a device's relationship to other devices in the acquaintance domain – for example, decreasing the rate of decay for devices that form a clique by being members of each other's acquaintance domains.

While there is work supporting the economic advantages of sharing markets for content providers [3, 26, 10], and work indicating that multimedia users value the ability to share

[1] or video, but our existing renderer does not support video.



(a)

(b)

(c)

Figure 4: Decaying permission to view an image: (a) after no half-lives have elapsed; (b) after one half-life has elapsed; and (c) after two half-lives have elapsed.

[4, 24], we are not aware of any work that attempts to define a model that best leverages these economic advantages, or best meets the expectations of users. We will leave the design and testing of possible membership functions as future work.

7 Conclusion

Fuzzy authorised domains with decay can be used to model the gradual decay of an acquaintance relationship over time so that people who see each other regularly are considered strongly acquainted while others are weakly or ephemerally acquainted. Existing authorised domain schemes such as the one proposed by OMA can be modified to support fuzzy domains in a straightforward way without modifying the overall security architecture of the system.

Our model for fuzzy acquaintance domains generalises some existing content-sharing models and can be applied to a variety of scenarios given appropriate choices for a domain's membership policy and membership function. In this paper, however, we have focused on the technical aspects of describing and implementing fuzzy domains, and the design and evaluation of particular membership functions for specific applications remains an open area of research.

8 Acknowledgements

This work was supported by the Co-operative Research Centre for Smart Internet Technology, Australia. We would particularly like to thank members of the User-Centred Design Group at the Royal Melbourne Institute of Technology for stimulating discussion in this area.

References

[1] J. Al-Muhtadi, A. Ranganathan, R. Campbell, and M. D. Mickunas. Cerberus: A context-aware security scheme for smart spaces. In *International Conference on Pervasive Computing and Communications*, pages 489–496, 2003.

[2] J.-P. Andreaux, A. Durand, T. Furon, and E. Diehl. Copy protection system for digital home networks. *IEEE Signal Processing Magazine*, 21(2):100–108, 2004.

[3] Y. Bakos, E. Brynjolfsson, and D. Lichtman. Shared information goods. *The Journal of Law & Economics*, 42:117–156, 1999.

[4] B. Brown, A. J. Sellen, and E. Geelhoed. Music sharing as a computer supported collaborative application. In *European Conference on Computer-Supported Collaborative Work*, pages 179–198, 2001.

[5] V. Casola, R. Preziosi, M. Rak, and L. Troiano. A reference model for security level evaluation: Policy and fuzzy techniques. *Journal of Universal Computer Science*, 11(1):150–174, 2005.

[6] V. Casola, M. Rak, R. Preziosi, and L. Troiano. Security level evaluation: Policy and fuzzy techniques. In *International Conference on Information Technology: Coding and Computing*, pages 752–756, 2004.

[7] W. G. de Ru and J. H. P. Eloff. Enhanced password authentication through fuzzy logic. *IEEE Expert*, 12(6):38–45, 1997.

[8] A. W. Dent and A. Tomlinson. Regional blackouts: Protection of broadcast content on 3G networks. In *Fifth IEE Conference on 3G Mobile Communication Technologies*, pages 442–446, 2004.

[9] B. Fox. 'Subversive' code could kill off software piracy. *New Scientist*, page 21, 11 October 2003.

[10] R. D. Gopal, S. Bhattacharjee, and G. L. Sanders. Do artists benefit from online music sharing? *Journal of Business*, 79(3):1503–1533, 2006.

[11] H. H. Hosmer. Using fuzzy logic to represent security policies in the multipolicy paradigm. *ACM SIGSAC Review*, 10(4):12–21, 1992.

[12] H. H. Hosmer. Security is fuzzy!: Applying the fuzzy logic paradigm to the multipolicy paradigm. In *Workshop on New Security Paradigms*, pages 175–184, 1993.

[13] F. L. A. J. Kamperman, Ł. Szóstek, and W. Baks. Marlin common domain: Authorized domains in Marlin technology. In *CCNS/CES Workshop on Digital Rights Management Impact on Consumer Communications*, 2007.

[14] S. Katzenbeisser, K. Kursawe, and J. Talstra. Graceful infringement reactions in DRM systems. In *ACM Workshop on Digital Rights Management*, pages 89–95, 2006.

[15] P. Koster, F. Kamperman, P. Lenoir, and K. Vrielink. Identity based DRM: Personal entertainment domain. In *IFIP Conference on Communications and Multimedia Security*, pages 42–54, 2005.

[16] B. Marušič, P. de Cuetos, L. Piron, and Z. Lifshitz. TIRAMISU: That's unobtrusive DRM in the home domain. *Indicare Monitor*, 2(5), July 2005. `http://www.indicare.org/tiki-read_article.php?articleId=125`.

[17] Microsoft Corporation. Zune. `http://www.zune.net`, 2007.

[18] Open Mobile Alliance. OMA DRM v2.0 approved enabler, 3 March 2006.

[19] F. Pestoni, J. B. Lotspiech, and S. Nusser. xCP: Peer-to-peer content protection. *IEEE Signal Processing Magazine*, 21(2):71–81, 2004.

[20] B. C. Popescu, B. Crispo, A. S. Tanenbaum, and F. L. A. J. Kamperman. A DRM security architecture for home networks. In *ACM Workshop on Digital Rights Management*, pages 1–10, 2004.

[21] A. Ranganathan, J. Al-Muhtadi, and R. H. Campbell. Reasoning about uncertain contexts in pervasive computing environments. *IEEE Pervasive Computing Magazine*, 3(2):62–70, 2004.

[22] T. J. Ross. *Fuzzy Logic with Engineering Applications*. Wiley, Hoboken, NJ, USA, 2004.

[23] Shared Media Licensing, Inc. Weed. `http://www.weedshare.com`, 2005.

[24] S. Singh, M. Jackson, J. Waycott, and J. Beekhuyzen. Downloading vs purchase: Music industry vs consumers. In *Digital Rights Management: Technology, Issues, Challenges and Systems*, pages 52–65, 2005.

[25] S. Sovio, N. Asokan, and K. Nyberg. Defining authorization domains using virtual devices. In *Symposium on Applications and the Internet Workshops*, page 331, 2003.

[26] H. R. Varian. Buying, sharing and renting information goods. *The Journal of Industrial Economics*, 48(4):473–488, 2000.