PROTOCOL FOR OWNERSHIP OF PHYSICAL OBJECTS IN UBIQUITOUS COMPUTING ENVIRONMENTS

Paulo Tam
School of Network Computing, Monash University
McMahons Road, Frankston VIC 3199
paulo.tam@infotech.monash.edu

Jan Newmarch
School of Network Computing, Monash University
McMahons Road, Frankston VIC 3199
jan.newmarch@infotech.monash.edu

ABSTRACT

With business losing large amounts of money due to increased violations of the rights of owners of electronic content by millions of people on the internet, the need has arisen for Digital Rights Management (DRM) and ownership technologies. This need however, was only recognized as something required after the rights had been violated. Ubiquitous computing is heading towards a world where there will be a great number of computing and smart devices per person that will be available to handle applications including ownership mechanisms. In this paper, we look at the definitions of what ownership is in a physical sense in order to build mechanisms for our ownership system that are based in ubiquitous environments. As the mechanisms of ownership are of a similar nature to those of e-commerce, we examine what requirements that are needed from everyday e-commerce as well as those which would apply to ownership in a ubiquitous computing environment. We also provide an example ownership transfer protocol for smart devices.

KEYWORDS

Ownership, Rights, Protocol, Ubiquitous.

1. INTRODUCTION

The availability of the Internet to everyday home users has enabled easy access to digital content through services that are provided by peer-to-peer programs and the World Wide Web (Fox 2001). These services make digital content easier to reproduce than something that is physical. Digital Rights Management (DRM) have been created and implemented to enable owners of digital content to exert their rights and track and manage their rights of content that they have produced (Camp 2003).

While there have been advancements in that type of management of rights, we would like to look at them in the smart devices area. We believe that these problems about ownership rights in the smart devices area should be addressed now rather than fixed retrospectively such as DRM systems are to digital content.

The concept of ownership has always existed and whenever we see an object we assume that it has an owner. In addition, our legal systems support the ideas of ownership and have the power to enforce ownership rights. When we speak about things, we also use words that imply ownership is attached to those things. We indicate this by the use of words such as the personal pronouns his, hers, mine and yours (Harris 1996). However, those words can be misleading as they can involve the issue of possession which is a different concept to ownership (This is looked at in section 2).

Weiser (1993) has estimated that in the area of ubiquitous computing the number of devices that a person owns will increase. In the beginning, mainframes were in vogue with many people connecting to one machine. Then, personal computers became more affordable and the situation changed to one person to one

machine. Now, the vision is that within the field of ubiquitous computing, one person will have many devices.

This vision is already close to reality with many people having a PC or laptop along with other computing type devices such as mobile phones and PDA's. For example, Nokia is developing a system whereby 20 barcodes and a barcode scanner are attached to a mobile phone (Thomas 2004). Devices need not be small. For example, motor cars have many embedded devices and can be regarded in many ways as a computing device. Devices such as these are opening the possibility for many applications, one of which would be that the owners are able to attach identification to their objects. However, a bar coding system for ownership could be seen as an insecure means of setting ownership, in that someone could remove the tag and replace it with their barcode tag. Despite this, the beginnings of simple ubiquitous environments are emerging.

Through combining the two areas of ownership and ubiquitous computing, we hope to create a method of ownership identification and controls for ownership rights for physical objects within ubiquitous computing environments. As we have seen with file sharing, ownership rights have only been an issue when persons discover that they are not gaining recognition for their property. Ownership should be an issue that is dealt with from the beginning before it becomes a problem.

In section 2 of this paper, we will firstly look at the definitions of ownership from philosophy and from a legal stand point as well as the issues that are involved in creating a new system of ownership. In Section 3, we will briefly describe the ideal environment for our system, which in turn affects the requirements that a protocol should meet in section 4. Some of these requirements are found from the definitions presented in section 2 of this paper, others are related to e-commerce requirements. Following this, we outline a sample protocol in section 5, and discuss related works in section 6. Finally, in section 7 we present our conclusions, discuss the limitations and make suggestions for future work.

2. DEFINITIONS OF OWNERSHIP

There are many different definitions of ownership available. The ones that we are most interested in are those that can add value to a ubiquitous ownership system. A very short definition of ownership is 'possession, identity of the owner' (Moore 1991). Although in an initial instance possession of an object can mean ownership of that object, there are many scenarios when a person may posses something which is owned by someone else. For example, the fact that driving a car does not automatically give ownership of the car to its driver.

Rather than using the word 'possession' as the definition of ownership, the concept of 'identity of the owner' is a better fit for this electronic environment. In another reference to ownership, Beloff and Kolbert (1997) state that 'property and the concept of ownership walk hand in hand. Property may exist without an owner, but it is in that condition an exception' and that 'we assume that where there is property there is at least one owner'. One exception, is the land of Australia as it was originally declared as "terra nullius" as a vacant land and uninhabited despite an existing aboriginal population. This decision was later overturned by courts, giving aboriginal land rights.

These ownership definitions give us some understanding of what ownership is. However, a more elaborate definition of ownership can be found from a legal point of view. Butterworth's Concise Australian Legal dictionary (Nygh and Butt 1998) states that ownership is 'the right recognized by the law, in respect of a piece of property (real or personal), to exercise with respect to that property all such rights as by the law are capable of being exercised with respect to that type of property against all persons, including the right to possession of the property and any proceeds of its sale'. This definition now writes about ownership as a right to the possession of the property.

There are many philosophers who write about ownership as a right or a relationship (Grunebaum 1987; Macquarie 1993; Guest 1961; Ryan 1987). This right mainly refers to right of possession, to occupy, to enjoy, to destroy and to alienate. As well as defining these specific rights that are available, the limit of these rights has also been stated as open ended (Grunebaum 1987; Harris 1996). These rights cannot be fully listed as the rights for one object are usually different from those for a different type of object.

In our ubiquitous environment we would ideally be able to see all objects in the room and securely find out who owns what object (subject to privacy), but we would also like to be able to describe and enforce the

owners' rights onto each of those objects, ensuring that only the owner has the right to that object, and that all non-owners cannot interfere with it.

Although the rights that can be described are different for each object and are open ended, there are mechanisms that all ownership systems perform. These involve: assigning rights and prescribing mechanisms for the acquisition, transfer, and alienation of these rights (Grunebaum 1987). In its initial stage, an ownership system must be able to perform these two functions.

In our ubiquitous environment those mechanisms (for acquisition, transfer and alienation of these rights) can be provided as services of our ownership system, which includes:

- **Acquisition**: the first mechanism can be interpreted as being able to gain or acquire the ownership title of a ubiquitous device from the very beginning of its existence. This is an initial way of gaining ownership of an item that exists in the world and that no one else owns at that point in time.
- **Transfer**: the second mechanism would simply pass title of ownership from one person to another. When both parties can pass a physical document of title it is not a difficult task. However, when a person has to change ownership of an item where ownership exchange occurs over a medium such as the internet, an issue about security arises. The next section of this paper will deal with the properties that are required from an ownership protocol.
- **Alienation**: the third mechanism is a way that would enable owners to alienate that ownership title away to no one.

There are restrictions to this last mechanism, and there are restrictions to ownership overall. Firstly, we will discuss the restriction to alienate. Although it would seem appropriate to be able to disown an object, there can be instances where it may not be allowable to do so until other criteria are met. For example, you cannot just drop you rubbish on the street. Disposal of an object no longer needed is limited by the owner's responsibility for the object in relation to other people. These types of responsibilities are related to common sense and legal influences.

Secondly, restrictions on ownership are very dependant on the type of object that we are dealing with and are important when transferring ownership from one person to another. For instance, car transfers and house transfers require a stamp duty be paid to a third party being the government body before the transfer can occur. Restrictions like this should be included in an electronic ownership system so it can mirror restrictions that occur in the real world. However, this also depends on our ubiquitous computing environment. If we assume that all objects will be included in our ubiquitous world, then there will be some items that have restrictions.

There are also levels of ownership. Ownership can be to the fullest, or ownership can be minimal. To the fullest extent, a person could say that they fully own an object and have all the rights to that object. In a minimal state, however, ownership can include group ownership where the rights are shared amongst other people, or it can mean that ownership to the fullest extent belongs to someone else and some partial rights belong to them. However, an individual could argue that they have some rights to the object as they were given them by the owner. This level of ownership is often in practice in rental situations, where a person has rights to an object but not the fullest. However, the rights in these situations are clearly stated in contracts which both parties agree upon before any rights are handed over.

3. UBIQUITOUS ARCHITECTURE

In any ownership scenario, whether physical or electronic, there are at least two parties involved. These will include a current owner and a new owner. However, for this electronic ownership we also now need to include the object as an involved party assuming that the object itself has certain abilities. Estimated abilities that all ubiquitous computing objects would have include being able to process and retain information and to communicate with other objects in a ubiquitous environment. With these estimated abilities the object can now keep track of its owner via electronic means and not by paper based means.

As far as processing ability is concerned there have been some advances in laptop and PDA device technology with CPU's becoming smaller and the perspective of smart dust (Khan, Khats & Pister 1999) giving CPU power to small objects.

Networking is also a very much required feature for a ubiquitous computing object. Although there has been no specific standard set for the use of ubiquitous devices, the range of networking technologies is for ever expanding. This issue was covered briefly by Newmarch and Tam (2004) in that IPv6 addresses could be used to cover a number of objects that exist in the ubiquitous computing environment.

Another feature that is needed is memory, which physically gets smaller as capacity gets bigger. The inverse relationship that memory has to capacity should ensure that its availability for ubiquitous devices is not a problem. This will allow very small through to very large objects being part of the ubiquitous environment.

With this ubiquitous architecture and ownership information being stored electronically by the object rather than by paper based systems, owners' typical tasks of ownership are to change and check ownership values. This can be done by checking ownership with the object itself as there is now a level of intelligence within it.

4. REQUIREMENTS OF OWNERSHIP/RIGHTS SYSTEM

As we have seen from the definition of ownership the total numbers of rights that can be applied are limitless. There are also a set of rights that are common to any and all items and can be represented in mechanisms. Even though we are creating a new system of ownership in ubiquitous environments by the design and implementation of a protocol, protocols for current e-commerce already exist and have been further developed. Several properties that are required in their protocol systems are also required here, with the difference being that the structures are different. This section looks at those differences and how they do or do not apply to ownership rights in ubiquitous environments. The properties for ownership will also be different to e-commerce applications in general because they are different in nature especially as ownership is defined here as the identification and changing of the title of owners.

While there are many different protocols in existence that handle e-commerce transactions they all mainly perform the task of transferring details about electronic money and thus, are not suitable to transfer ownership details due to the nature of the content. Hence, there are many differences that would be needed in a protocol.

While both e-commerce transactions and ownership transactions require attributes that are similar, these are also different and should be treated in different ways because of the environment in which they exist. Attributes that have been already defined and discussed by Neuman (1995) for e-commerce requirements are listed below as well as properties derived from other sources. They are security, reliability, scalability, anonymity, acceptability, customer base, flexibility, convertibility, efficiency, ease of use, privacy, low overhead and confidentiality. In our case, some of these are just not achievable due to the nature of ownership, and others are a must.

- **Security**: all protocols in their design phase have security issues. Attackers may attack depending on the purpose of the protocol. The difference to an ownership protocol relates to ownership details about being sent.
- **Reliability**: any protocol created for the purposes of e-commerce or electronic ownership transfer must be reliable. Anything we do with a protocol must be assured and the message sender must be prevented from sending an invalid message or deny the sending of a message. The protocol should require the digital signature of the message sender not only for message authentication but also for message integrity.
- **Scalability**: e-commerce is an area that is often talked about as a growing area. It is argued that there will be a greater demand for its uses and hence any procedures that are created must be scalable to cater for demand. This issue for ownership in ubiquitous environments has already been looked at in Newmarch and Tam (2002).
- **Anonymity**: primarily in many e-commerce transactions the task is to make sure that the seller receives their payment from the consumer. This can be done anonymously through the use of some e-commerce protocols. Anonymity in ownership transfers may be a highly desired property. However, the analysis of such a desire is outside the scope of this paper.
- **Acceptability**: for this new form of electronic ownership to be accepted, all users have to agree that this form of ownership can hold true to what ownership information it holds.

Only then can one user be able to transfer ownership to another user. To be accepted at the first stage, electronic ownership systems must be able to reflect physical ownership papers that currently exist and are accepted at that time.

- **Customer Base**: this property of e-commerce is the same for electronic ownership. Only if there is enough of an acceptability of the electronic form of ownership would there then be a large enough customer base for systems to then adopt this electronic form of ownership. Furthermore, the ubiquitous half of the technology would in effect also need to be able to create a large enough customer base.
- **Flexibility**: in e-commerce payment transactions there is a need to be able to be flexible for different forms of payments. In ownership there is the need for flexibility in the different levels of ownership which are attainable. These levels include scenarios of group ownership, rentals and leasing. Any protocol that we create should be flexible in order to allow extensions to cater for these types of ownership in the future.
- **Convertibility**: we are especially creating this system for the uses of ownership titling and transferring. There is no need to be able to convert this system for other uses.
- **Efficiency**: in payment systems, efficiency is one property that is desired as mechanisms would happen over infrastructures that are not necessarily the company's so they need to be efficient and not generate too much cost. For our electronic ownership vision, the infrastructure is already created by the ubiquitous environment and we assume that there is no cost to the user to transfer any data from object to object.
- **Ease of Use**: in e-commerce there is the requirement that the tool created is easy to use, otherwise it can affect the acceptability of the mechanism. An ownership protocol must be worthwhile as is the case for any e-commerce application.
- **Privacy**: once ownership is set, there should be a way to blind the information so that no one can access it without the owner's permission. For some it maybe a status issue in that they want people to see what they own, for others they may require that ownership of an item be unknown to protect their interests.
- **Low Overhead**: in the system we are proposing, the architecture allows for the requirement that there is no other party that is required to validate people as a Certificate Authority does. Although this could be implemented to provide more security assurances, it would come at the cost of exchanging of more information.
- **Confidentiality**: in e-commerce, the bulk of transactions exist in the business to business or business to consumer realm. For our type of ownership identification and transferring we can be dealing with both realms plus the consumer to consumer relationship as well. As a result of this, there is a possibility that one consumer well rely on another to keep their information details secret.

5. AN EXAMPLE OWNERSHIP TRANSFER PROTOCOL

The previous sections define what ownership is and the mechanisms we would implement when creating an ownership system for ubiquitous computing environments. This section will now cover an example protocol to transfer ownership.

Assumptions for our system fall into two categories. These are firstly in relation to the problem of ownership in ubiquitous environments, and secondly in the actual protocol. Firstly, Assumptions in relation to ownership, we are assuming that when an object is created the ownership is already set to its maker. The idea behind this assumption is that a manufacturer would control the initial ownership of the objects they have created. Once they have a buyer and hence a new owner, they would transfer the ownership of the object to them and this process would continue down to the consumer in the end. The advantage to this is that it replaces the need to place different barcodes for the objects throughout the different stages of its life. At this stage, we are also assuming that there can only be one single owner at any time, and that identities of all parties are already known to each other, and that only the owner has the ability to transfer ownership as in section 2. We are also assuming that there is not any hiding of transfer information.

Secondly, the actual protocol is based on other computing concepts, these are as follows.

1. Reliance on public key cryptography being secure.
2. Objects in the ubiquitous world being all connected together via IP addresses in the Networking
3. Objects having the capacity to be able to process cryptography functions in order to be able to authenticate and secure messages.

Notations we have used are as follows.

- A stands for Alice
- B stands for Bob
- O stands for our object
- public key(Alice) stands for the public key of Alice
- $S_{alice}(X)$ stands for a Signature from Alice of message X
- A → O stands for communication between Alice and the object.
- A → O: X stands for the message X is communicated to object from Alice.

The main mechanism that we have outlined is that of ownership transference. To do this in our system these are the steps that are required. The example we will use is if Alice would like to give the full ownership rights of an object to the new owner Bob. Ownership is already set to Alice and she has verified it. And Bob and Alice have already discussed any money exchange or trade and are now dealing with the ownership change only. They have already exchanged public keys securely.

The following list is a protocol to transfer ownership from Alice to Bob. These steps can also be visualized from figure 1.

1. A → O: S_{alice}(Change ownership to Bob, identity of Bob)
2. O → B: S_{object}(my ownership is about to change to you, accept or reject)
3. B → O: S_{bob}(response to of accept or reject)
4. O → A: S_{object}(acknowledgement of status of transfer)

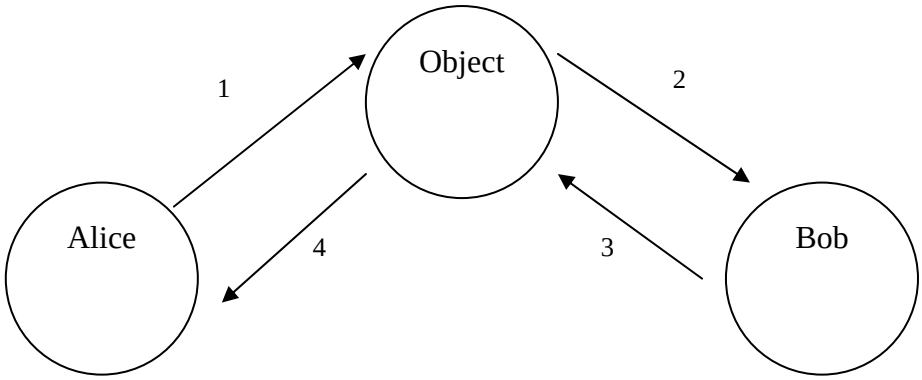

Figure 1. Model of entities in our system and the message being passed between them

1. Alice creates a message to the object. In this message it includes instructions that ownership is to change to Bob and provides identification. Message is then signed with Alice's private key. Message is then sent to the Object.
2. The object receives the message and can verify that it comes from Alice as it contains her signature. Object then prepares a message for the new proposed owner that asks if they are willing to accept ownership of it.
3. Upon receivership of that message Bob can decide whether or not to accept the ownership of it, and creates that response and signs the message and sends it back to the Object.
4. Object knows if Bob is willing to accept as the object can verify with the public key given by Alice, and then creates an acknowledgement back to Alice that the transfer was successful or not. Sets the ownership if Bob was willing to accept and then reply to Alice of the change.

The design of this protocol addresses the issues of security, reliability, flexibility and scalability. However, the designed protocol does not address issues of anonymity, efficiency, privacy and low overhead. These will require extensions to the existing base transfer protocol. And the other properties of acceptability, customer base, convertibility, ease of use, confidentiality are either not applicable to an ownership protocol or have nothing to with the protocol itself but the system it is created for.

6. RELATED WORK

This work aims to create a method of identification for the ownership of a physical object and have that information available over ubiquitous computing environments. As we have discussed in the introduction, the ownership rights issue has come about as a result of the ability of ubiquitous devices to be able to store and process information, leading to the possible removal of paper based or other ownership systems. A system that has been created to control digital rights over the Internet is DRM technology. Clearing House Electronic Sub-Register System (CHESS) is another system that identifies ownership of items electronically and is a system that is used by the stock market. Both these system control the rights of something that exists in cyberspace, however, in this paper we are attempting to control the ownership rights of something that is physical but represented in cyberspace. However, some of the issues that CHESS and DRM technology bring forward are also related to this work and we shall briefly discuss those.

CHESS (ASX 2003) is used to control the ownership of stocks listed on the Australian Stock Exchange electronically. CHESS creates statements that can be kept as proof of transactions to keep track of shares. This concept is similar to ours in that we can have the object sign a message concerning its ownership, and someone could use it as a proof of ownership at that specific point in time.

DRM which was briefly touched upon in the introduction, is a technology that exists in the current e-commerce environment and has come about due to owner rights being violated. DRM mainly exists in the music and movie industry. However, other digital content is also touted as being within the scope of DRM systems. The main digital content types are movies in MPEG-21 (Bormans 2003), music in WMA and writings in e-books (Camp 2003).

There are several similarities between both systems and ours. All systems require a way of identifying the persons to delegate rights. In CHESS, users are given a Holder Identification Number (HIN). In DRM systems, a vCard is used or a piece of information that is accessible only from the hardware is needed. In our system we rely on every person having public and private keys to use for the purpose of identification. Aside from the differences in the systems of identification, they also have different levels of authentication to them. A user in the CHESS environment is required to partake in a formal agreement before they are given a HIN, whereas in DRM systems, vCards can be created by the user on demand, in a similar way as a public key pair can be. Extensions to our system could see a Certificate Authority being added into the model and would give us more reliability in those identifications.

7. CONCLUSION

The need for a system of ownership is highly dependant on the availability of ubiquitous environments. However, when that technology does become available, ownership and ownership rights should be something that is managed and controlled from the beginning rather than being created later as a reaction to rights being broken.

In this paper, we have looked at the definitions of what ownership is. Thus, all ownership systems should provide mechanisms to perform ownership tasks. Based upon those mechanisms we can create services to enable ownership to be controlled in our ubiquitous environment. We have also outlined an example protocol that can be used to transfer ownership of an object in a ubiquitous world and do so securely, reliably, while having flexibility and scalability.

However, there are limitations to the protocol in that it is dependant on the technologies of ubiquitous computing and that it will only work when all objects in the world become ubiquitous items. Once objects become ubiquitous, then the applications that are possible are limitless. For any object in the world we

assume there is an owner attached to it and what we have presented is a way that we can define ownership and control the identification of physical objects on itself over an electronic medium.

Another limitation is the legal factors that would be involved. Just because we can define ownership in this manner does not mean that ownership will be accepted. These issues were touched upon in the ownership definition section.

As far as all systems that exist in the ubiquitous realm there is an element of breaching the privacy of users with information being readily collectable from ubiquitous objects. This work is no different and information about who owns this object could be used maliciously against the owner. This is an area of future work as well as the possibility of a group ownership protocol. Such a protocol would expand on example protocol detailed in section 5, however it would incorporate functionality such that a group of owners of one item could then create a digital contract and each provide authorization to pass ownership of that object to someone else.

ACKNOWLEDGEMENT

This paper is based upon work partly sponsored by the Cool Campus Project, an arrangement between the Faculty of Information Technology, Monash University and Hewlett Packard.

REFERENCES

ASX., 2003. *ASX Clearing House Electronic Sub-Register System*. available at http://www.asx.com.au/about/pdf/CHESSIntro.pdf, last accessed 19-05-2003

Beloff, M. B. and Kolbert. C. F., 1997. *The idea of property : in history and modern times : the Sir Ian Mactaggart memorial lectures and complementary essays*. Glasgow, I. Mactaggart Trust in association with Churchill Press.

Bormans, J., Gelisson., J., and Perkis, A., 2003, *MPEG-21: The 21st century multimedia framework.* IEEE Signal Processing Magazine 20(2): 53 - 62.

Camp, L. J., 2003. *First principles of copyright for DRM design.* IEEE Internet Computing 7(3): 59 - 65.

Fox, G., 2001. *Peer-to-peer networks.* IEEE Computational Science and Engineering 3(3): 75 - 77.

Grunebaum, J. O., 1987. *Private ownership*. London ; New York, Routledge & Kegan Paul.

Guest, A. G., 1961. *Oxford essays in jurisprudence : a collaborative work.* London ; New York, Oxford University Press.

Harris, J. W., 1996. *Property and justice*. Oxford ; New York, Clarendon Press.

Khan. J.M., Katz. R.H., and Pister K.S.J., 1999. *Next century challenges: mobile networking for "Smart Dust"*. The 5th annual IEEE International Conference of Mobile Computing and Networking, Seattle, Washington, USA.

Macquarie, 1993. *The CCH Macquarie dictionary of law.* North Ryde, N.S.W, CCH Australia by arrangement with Macquarie Library.

Moore. B. (Compiler), 1991. *Australian Oxford Pocket Dictionary: Second Edition.* Victoria, Oxford University Press.

Neuman, B. C. and Medvinsky. G., 1995. *Requirements for network payment: the NetCheque perspective.* Compcon '95.'Technologies for the Information Superhighway', Digest of Papers.

Newmarch, J. and Tam, P., 2002. *Issues in Ownership of Internet Objects.* The Fifth International Conference on Electronic Commerce Reaserch, Montral, Canada.

Nygh, P. E. and Butt, P. J., 1998. *Butterworths concise Australian legal dictionary*. Sydney, Butterworths.

Ryan, A., 1987. *Property*. Milton Keynes, Open University Press.

Thomas, D., 2004, *Nokia brings RFID to mobile phones.* Available at: http://www.vnunet.com/News/1153568, last accessed 17-03-2004

Weiser, M., 1993. *Hot topics-ubiquitous computing.* IEEE Computer 26(10): 71 - 72.