Issues in Ownership of Internet Objects

Jan Newmarch and Paulo Tam

Monash University
School of Network Computing
Frankston, Melbourne, Australia
{jan.newmarch, paulo.tam}@infotech.monash.edu.au

Abstract

This paper presents an idea that extends the world of ubiquitous computing combined with the financial aspects of ownership issues. When objects can be connected in a ubiquitous world, objects themselves will have the power to compute their own processes and communicate to other devices. Physical properties will be mirrored by software properties. This paper looks at issues that would arise if ownership were regarded as a software property.

Keywords Internet Object, Ubiquitous Computing, Ownership, bill of title.

1. INTRODUCTION

There is a growing convergence between software and "things" in the real world. Analysis, design and programming methodologies are increasingly adopting an object-oriented approach. At the same time, the cost of computing devices continues to fall, and their size to decrease, so that it is becoming easier to embed processors and computers into everyday devices. To make life easier, some computers have been made to be wearable. This has enabled the users hands to be free to move about as normal while using a computer[10], Some experimental systems have even been sewn into clothing, and it is possible to get HTTP servers that fit in a matchbox.

When a large variety of things can contain computers, these objects will contain software objects that represent the physical objects themselves. Properties of objects in the physical world will be mirrored by properties of the software objects.

This paper investigates issues of ownership of objects and transfer of objects, fundamental to any commercial transactions. It considers the problems that may arise and that may need solutions if "smart objects" are to become possible. The following topics are discusses:

- Costs and possibilities for embedding network aware computers in physical objects
- Centralized versus distributed holders of electronic bills of title
- Identity of owners and objects
- Transactions: changing ownership of objects
- Leasing and renting objects
- Group ownership and other cases
- Privacy

- Infrastructure
- Legal requirements.

2. COSTS

Nowadays a PC costs a few hundred dollars and depending on the amount of processing power and hardware required the cost of embedded systems can be much cheaper. With costs going down it is more feasible to place computers in high cost consumer goods such as cars and in less expensive items such as white goods. Indeed, many of these items already have embedded computer systems; a typical new car has approximately a hundred processors. While cars do not have an Internet connection as yet, navigation systems in cars use GPS technology for location.

In addition, as hardware costs are decreasing the cost of the Internet is also decreasing and it would be feasible now to give an Internet connection to many objects. Then as costs fall further this will become possible for even cheaper objects. However, while it may be possible to add an internet connection to objects, it may take some time for smart processors combined with connection costs to become cheap enough to be attached to low very low cost items, such as cans of beans.

Whether or not it would be feasible to add an Internet connection to low cost objects would depend on the additional cost involved. RFID (radio frequency id) tags which now cost upwards of fifty cents per tag would need to be reduced to five cents per tag as discussed by the Auto-ID Center[9]. If we were to say that percentage was one percent of the item itself then, it would be feasible to add a 200 dollar component to enable connectivity to a car costing $20,000. However, a can of beans costing $2 would have to wait for the cost of the technology to drop to 2 cents before it would be feasible to add it to the cost of a $2 can of beans.

Aside from the physical costs of implementation there are the infrastructure costs that may need to be included in the overall costs. However, depending on the infrastructure implemented then additional costs could be avoided. There are three levels of costs which physical implementation of devices could be implemented: cheap, reasonable and expensive. The costs also would determine the level of security of the objects.

The cheapest option that would work, would be one where people would have the responsibility of creating and managing their own private and public key sets needed for security, and letting the objects identify themselves through those keys and an identifier. This is the cheapest option as there is no need for a certificate authority.

At the next level, a reasonable cost would be incurred. Every person with smart devices would then become a part of a community of people in a certificate authority. This would then allow a third party to verify ownership changes as an authority.

The expensive level schemes now include a X.509 PKI. Certificate Authorities (CA) now issues certificates for private and public keys for all objects and owners in the world. Systems where objects have private/public keys and can sign messages to prove ownership. PKI Certificates certified by a CA currently vary in cost and the cost decreases the more you purchase. Costs for public key certificates are around $30[7].

Depending on the identifying structure IP addresses may also need to be bought for each device.

3. ONWERSHIP OF PHYSICAL OBJECTS

There are a variety of ways of demonstrating ownership, from physical possession, and receipts to bills of title. Registration mechanisms may also be used but they are not reliable.

Ownership grants the owner certain rights over the object. In some cases these rights may be formalised by a contract (such as in buying a house), but in others (such as in buying a can of beans) no explicit contract is signed.

Leasing or renting an object may grant a different set of rights. Work by Zoran on digital contracts will prove useful in formalising rights between software objects representing the physical objects[8].

4. CENTERALIZED VERSUS DISTRUBUTED

The idea of objects having an Internet presence and having ownership control on them is not a new one. Bolero[1] is now online and has a number of companies using their system.

Bolero is a centralized scheme for bills of lading. The Bolero scheme uses digital signatures to verify messages to clients via the Core Messaging Platform. Messages are then checked for authenticity and integrity. Once the Core Messaging Platform receives messages they are then forwarded to the target client and a notification is sent back to the sender that they have sent this message forward. While world-wide in scope, this is a single system and thus has particular problems of

- single point of failure
- single point of attack
- scalability potential
- lack of privacy.

As the Bolero scheme is centralized, a bottleneck situation can occur. This would happen if all of the users decided to access the system at once. What would result would be delays in the service and possibly even denial of access to the system as too many users were using it at same time. Related to this issue of being centralized is that there is a single point of attack. If attackers found a way to bring down the Core Messaging Platform in the Bolero, the scheme consequently could be useless.

The Bolero market is growing with more and more companies using their scheme and so Bolero will grow in size. One problem that arises from the increased popularity of Bolero is that of scalability. With more and more users, will Bolero be able to scale up to the demands of all the users?

With Bolero there is also a potential lack of privacy. From a successful attack on the Bolero scheme an attacker could obtain details of all the clients of the Bolero System and the worth of products. Privacy also comes down to the workers at Bolero, where workers can access account information and that could be potentially dangerous. Issues such as this can often be read in the media. A staff member for example, has passed on or used private information such as credit card numbers to their own advantage. We are not suggesting in any way that Bolero is especially subject to such risks, only that centralized systems are.

We propose instead a totally distributed system where each "smart" object keeps the identity of its owner. Each object would then have enough processing power and network capability to maintain knowledge of its owner and to partake in network transactions. The remainder of this paper discusses issues that would need to be resolved for this to be feasible. These issue arise from a distributed choice and are identity, transactions, leasing, group ownership and other ownership issues, privacy and infrastructure.

5. IDENTITY

In the real world we have names to distinguish people. Even if we have the same first name and surname, other defining variables can often be used to tell a person’s identity. Using names as an identifier is satisfactory in a small group and confusion can be avoided when trying to single out one person. However when a large community of people are involved names alone cannot be used to identify another person and only that person. When obtaining a drivers licence several forms of proofs of identity are needed. Two instances where similar identifying documentation are required are that of Vic Roads, Australia[12] and Virginia Department of Motor Vehicles, USA[13]. In both cases they require primary and

secondary proof of identity and also a proof of residence. This means that a social security number alone will not be enough to obtain the licence and that two other forms of identity are required, such as an unexpired passport or Medicare card. This identifying process would also be required for online objects, as there may be two cars that look the same but the registration number tells them apart. Electronic objects will also need a way to be identified one from the other by their owners. And a person's online presence will need to be identifiable from that of another person.

To identify objects from each other some globally unique identification scheme must be in place. There are already a number of such schemes, such as the Ethernet MAC 48 bit addresses. A similar mechanism to these may be required, or a more sophisticated mechanism such as IP addresses could be used. This would allow objects to be directly accessed and then to be able to send and receive messages from them.

If all physical objects were given an electronic presence there must be a mechanism to uniquely identify them. In number terms there are not enough IPV4 addresses for even a small percentage of objects to be addressed (see Figure 1).

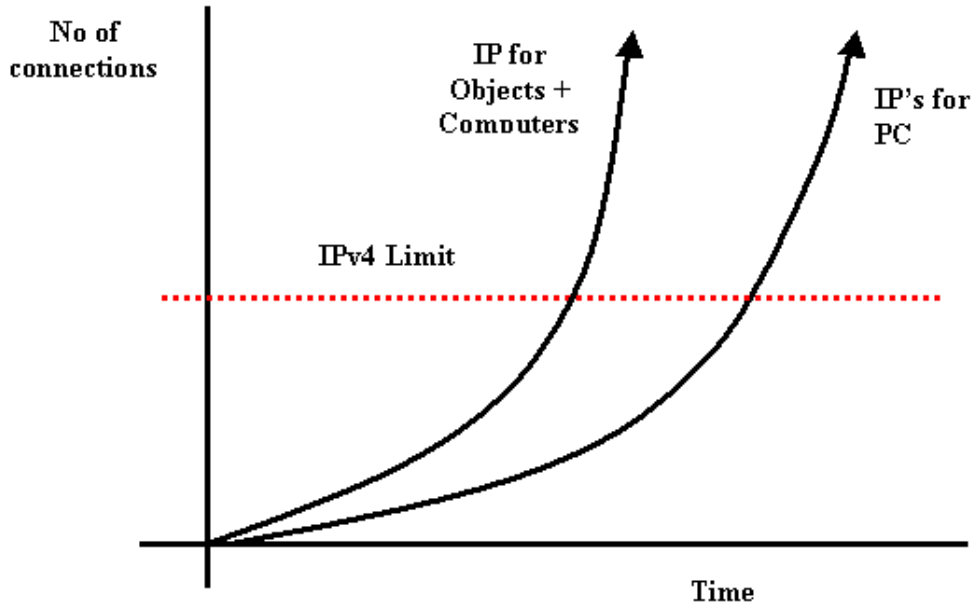

Figure 1: The number of connections required

This would require adoption of IPV6, with a corresponding infrastructure to cope with billions of addresses.

For example, consider the amount of canned goods that are produced and sold each day in the world. Heinz have estimated that they will sell 650 million bottles of ketchup per annum[5]. For each of these bottles an unique identifier would be required. Some physical items already have unique numbers added to them. A serial number is printed on canned goods and cars are plated with a chassis number and engine number. As well as a totally unique identifier on these products, a group identifier can also be found. A batch of canned products will have the same batch number and cars are grouped under the date of manufacture. These identifiers are useful in cases of recall, where news about a batch of cans should be returned for a full refund or a batch of cars need to be returned for repairs on a design flaw.

These identifiers can be a concern or not a concern at all depending on the owner. When someone buys a can of beans they do not look at the bottom of the can to see the identifier. However, when a person buys a car they check previous ownership on the car before making the decision to buy. Once someone has bought the item then ownership of that particular item becomes important to him or her. For this reason Internet Objects would also need to be able to have an identifier on a unit level to prove ownership, but usage at that level may not occur that often.

Once identities have been worked out, connectivity to those objects is an issue. By using IPv6, connectivity is already resolved as IPV6 already has the means to cope with mobility. However, the lifetime of addresses of certain items may be short, particularly for consumable objects. Depending on who created and owned the object, the lifetime of the address may be an issue but will not affect the total amount of addresses available to use in the long term. IPv6 addresses being used in an organization would typically be given a 48 bit network prefix. Depending on administrators in the company they could decide to have 16 bits for the subnets and 64 for the hosts [6]. The number of subnets may translate to the different lines of products, leaving the number of hosts to the number items. Revisiting the number of bottles of ketchup sold, assuming they constantly sold 650 million bottles per year, it would take approximately 28 379 606 267 years to exhaust the number of IPv6 addresses in the subnet used for ketchup and then worry about reusing the available ones.

Because of the identity issue involved here, people's privacy is also an area that needs to be considered (see section 9). Given there is a way to uniquely identify people and things, the owners may not want those objects to tell the world that they own them. Consumer researchers could have the opportunity to find a person's objects and then direct special advertising to that person knowing they are interested in those types of things.

6. TRANSACTIONS

Once objects have the power to process commands and have a connection to the Internet, messages can be passed to and from the object. These groups of messages would then become transactions that happen when ownership is checked upon or transfer of ownership is conducted.

Consider the scenario where an owner has decided to sell an object to a buyer. Once both parties agree on the price, physical ownership is released from one party and given to another. Consequently, not only will ownership change in this physical sense, but also in the electronic world. Electronically, ownership changes are registered by the buyer and seller through receipts, which can later be used as identifiers to the objects ownership. These receipts are messages that would be communicated between objects and people during the transfer.

Further common examples are found at the supermarket and in the process of changing car ownership. At the supermarket, once you have paid and the item is taken out of the store that item is yours. Electronically the supermarket has scanned the item and recognized that the tender for the item has been paid and no longer recognizes that the item is available stock. When changing ownership of a car, once money has been finalized then physically the keys to the car are handed over and the change in cars ownership is notified to the authorities. Physically the change has occurred but until the authorities authorize the change and record the event electronically in their database, ownership still belongs to the previous owner.

This process generally involves an exchange of messages between original owner, and new owner and maybe a third party registration authority. There are a number of aspects to this

- Security: only the owner should be able to give an object away
- Agreement: the new owner has to agree to accept ownership
- Transfer: the object must become aware of the identity of the new owner
- Registration Authority has to agree to transfer.

From a security sense some messages can be left as normal message and not signed. An example of this is when someone asks an object "who is your owner?" In this case security is low, as a message of "who is your owner" is not a command that may harm the ownership of the object.

Other messages must be signed for security. One example of this is when an owner asks the object to change its ownership to someone else. Messages must be signed to validate that they are coming from the owner and not someone trying to steal the object. In this case the object would already have the ownership public key to send a message to owner.

To go further and have the object obtain authorization of the change in ownership to him or her, the object now needs to have the recipients' public key. This now requires a public/private key infrastructure combined with a transaction protocol. The resulting PKI will need to scale up to billions of keys, far beyond the scope of existing PKI.

The current costs of PKI systems result in a current per license cost of about $30[7]. The $30 spent on the certificate goes into the creation of the certificate. This process involves background checks on the person applying for the certificate and the other policies that the certificate authority has. Because of such a screening process any people that do have these certificates are deemed to be authentic..

Other companies also offer certificates at different prices. GlobalSign certificates are around $15. These certificates are valid for one year and need to be renewed after that[4]. For PKI for billions of objects, costs will need to be reduced to a few cents. The cost of certificates could be reduced by reducing the level of trust. If there are fewer mechanisms to check the validity of a user in creating the certificate then the cost to produce the certificate is cheaper. VeriSign[11] offers three levels of certificates with three levels of trust. The class 1 level, assures that the communications originates from the original source. At the class 2 level, the identity is checked amongst other third parties. At this level VeriSign states it is a reasonable level of trust. And at the class 3 level, identities are checked in person or by other enhanced procedures.

Some transactions will result in contracts being created. There will also need to be an infrastructure for this (See Figure 2). This structure utilises IPV6 technology as the unique identifier for the objects, and indicates whether an object has a digital certificate from the Certificate Authority.

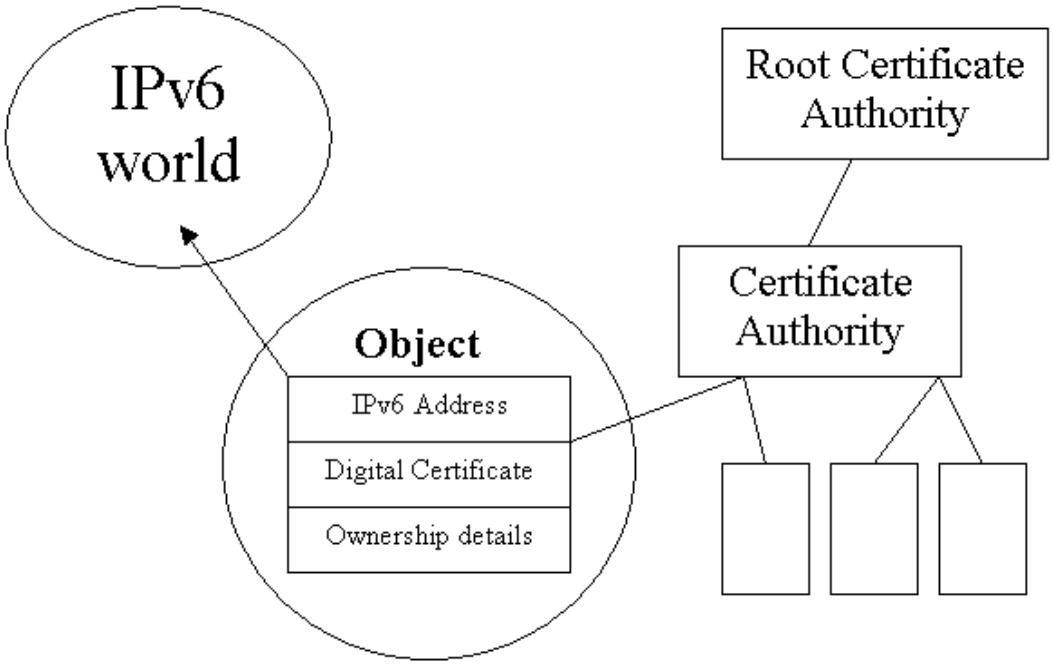

Figure 2: Internet Object Structure

7. LEASING

In the event that a physical object is leased to another person, temporary ownership is transferred to the recipient of the object. With temporary ownership a leaseholder has certain rights and responsibilities. The leaseholder should have these rights and responsibilities until the moment the time comes when the lease has expired and the object is returned to the rightful owner.

A similar feature will need to exist for objects that exist electronically. These objects will have to retain details that verifies that their ownership has not changed permanently but only for a rental period. Leasing will be similar to ownership, but with different contracts and concept of leaseholder. Leases will expire after a certain stated period.

8. GROUP OWNERSHIP & OTHER OWNERSHIP ISSUES

On certain occasions, more than one person may own an object. Such is the case of a family pet. The family pet is owned by the family and no one individual in the family should be allowed to give the animal away except with the consent of the other family members.

Other situations where ownership becomes more complex is in situations such as bankruptcy or death, in which some legal organization is able to dispose of property without the consent of the owner. If private and public keys protect ownership, there may be a need for some sort of escrow system to allow legal authorities to change ownership.

Once legal requirements have been set to legally bind objects to digital signatures other requirements may have to be created. This includes a Law enforcement agency. This issue has been raised in the UK communications Act of 2002. Public consultation in the drafting process of this document had raised issues, one of which was an issue of empowerment of an authority to demand that the secret keys be handed over for legal purposes.

9. PRIVACY

If ownership can be changed by electronic messages, then there are two particular privacy concerns including:

- Third parties may be able to eavesdrop on messages and build up information on transactions
- A purchaser may wish to keep their identity secret from the seller.

As communications will happen over open channels other parties may listen in on the communication messages that will occur when ownership of a device changes. Although the messages themselves cannot be changed without the associated private and public keys, there is a risk that others can build information about what other people are purchasing. Markets could then use this information to send ads to consumers according to the information collected from the possible eaves dropping that could occur.

Another issue is that of identity. Some purchases do not require the need to know the identity of the purchaser. An example of this is at the supermarket, for cash in hand transaction identity is not needed, and the receipt is not made out to a name.

Privacy concerns that can deal with issues of eavesdropping and purchaser identity will need to be addressed in the transaction protocol. This may or may not be resolved by anonymous crypto techniques.

10. INFRASTRUCTURE

There are billions of objects that change hands each day. In order for a large scale distributed owner system to function, there is the need for the following infrastructure:

- PKI
- IPV6
- Contracts

A Public Key Infrastructure would supply all people with the smart devices a public key and private key. On a very large scale this structure would be needed for each object that exists as a device connected to the world. This would then ensure that there is authentication by digitally signed electronic data. Within a PKI there are Certificate Authorities that handle the objects that are in its community.

There would also be many CA's otherwise we would be falling into the same trap as a centralized system. However, with many CA's there would have to be cross certification and this creates a growing problem as there are more CA's they would then require what is known as a single bridge CA, which exchanges cross certificates with other CA's. It is possible to scale. For example, DNS, but a similar engineering task would be required for PKI.

The next infrastructure needed would be one which could cope with a unique identity for a large amount of objects. This could be done using the IPv6 infrastructure where each of the objects has an IPv6 address. As objects can be mobile the mobility of IPv6 would also be utilized.

11. LEGACY OBJECTS

It will never be possible to bring all objects into such a scheme where all objects are smart devices that know ownership. For example, there is the current existing set of objects. It would be too costly to remake all existing objects into smart objects. And there are some objects which cannot have computers added, such as a glass of beer. There are other items that are just too inexpensive to make into smart objects. Either it is to physically impractical or too costly.

Objects that are more likely to become "smart" objects are ones that would have a permanent enough existence and could absorb the cost. Any system will need to cater for both smart and non-smart objects.

12. LEGAL REQUIREMENTS

In order that smart devices retain ownership properties, legal requirements would need to be changed. Digital signatures need to be allowed as a legal bind to the objects ownership claims. As a receipt of a purchase can prove ownership claims to an object, an electronic version of the receipt would need to be legally acceptable by authorities as ownership. The digital signatures that are produced in communication messages should be sufficient for this task.

Currently only a few countries will accept digital signatures as legally binding. However, most countries have acknowledged or are discussing the need for a legal framework and the usage of digital signatures in their countries.

In Australia, the Australian Commonwealth has allowed speech, text, data, and images to be digitally signed and legally bound together. This legislation was documented in 1999 in the "Electronic Transactions Bill"[3].

The UK also has enacted legislation in the "Electronic Communications Act 2000" that allows electronic signatures and related certificates to be accepted in legal proceedings as evidence in the case of data or communications[2].

A distributed ownership scheme will require additional changes in legal systems. These changes would involve having digital signatures of certificates to be recognized legally. A digital certificate would then be recognized as a valid receipt.

13. CONCLUSION AND FUTURE WORK

This paper has touched on the issues involved in a distributed ownership scheme. An idea which seems initially simple, however, has a large number of ramifications. Costs at present are high and possibly too high to start creating smart objects unless they are in high cost devices. Even with the cost being affordable there are questions still in the engineering of the objects. Once objects have a unique identity and have connectivity to owners a secure method of communication will need to be used. And on the legal issues PKI may be a solution however will need to scale up to the billions of objects that would exist. Smart and secure devices that know about their ownership still may not be recognized as legal proof of ownership and the legal questions will need to be clarified for people to then be able claim ownership of objects in this way. Privacy concerns will also require further work.

We are now looking further into several different areas: wireless access, privacy, security and legal systems. As most smart devices will me mobile different types of wireless communications and their ability to cope with Internet Ownership will need to be looked at. Privacy will continue to be an area that needs work as privacy concerns will need to be handled before smart devices with ownership can be implemented. As always security should be an ongoing study. Legal systems that people can use to prove ownership of smart devices will need to be created otherwise smart devices may not be used to tell ownership by people.

References

[1] Bolero. Available at http://www.bolero.net.

[2] Electronic act 2000. Available at http://www.legislation.hmso.gov.uk/acts/acts2000,20000007.htm.

[3] Electronic transaction bill 1999. Available at http://www.aph.gv.au/parlinfo/billnet/99131b01.doc.

[4] Global sign. Available at http://www.globalsign.net.

[5] Heinz: A clear strategy from stronger growth. Available at http://www.heinz.com/jsp/di/corp_pro2002/corpProfile2.jsp.

[6] R. Hinden and S. Deering, IP Version 6 Addressing Architecture, IETF, RFC2373, July 1998

[7] D. Messmer. Companies warming up to PKI. Network World, 18(16):1-2,2001.

[8] Z. Milsevic and R.G. Dromey. On expressing and monitoring behaviour in contracts. In IEEE International Enterprise Distributing Object Computing Conference EDOC2002, sep 2002.

[9] S Sarma. Towards the 5c tag. Auto-ID Center. Nov 2001. Available at http://www.autiid.center.com.

[10] T.E Starner. Wearable computers: No longer science fiction. IEEE Pervasive Computing, 1(1): 86-88, jan-mar 2002.

[11] VeriSign - PKI Disclosure Statement, Available at http://www.verisign.com/repository/disclosure.html.

[12] VicRoads, Available at http://www.vicroads.vic.gov.au/.

[13] Virginia Department of Motor Vehicles, Available at http://www.dmv.state.va.us/.