33

AN INSIGHT INTO USER PRIVACY AND ACCOUNTABLE ANONYMITY FOR MOBILE E-COMMERCE TRANSACTIONS

Delia Critchlow, Dr Ning Zhang
University Of Manchester, UK
{critchld,nzhang}@cs.man.ac.uk

Abstract: In this paper the need to develop an accountable anonymity scheme specifically for mobile e-commerce is established. The requirements of such a scheme are identified and shortfalls in existing anonymity services are identified. A novel approach based on the concept of unlinking processes to prevent any meaningful collation of information on a particular on-line identity being performed is discussed. We then propose (in outline) an anonymity scheme based on this concept that will then be extended to provide accountability through on-line revocation.

Key words: security, anonymity, mobile e-commerce

1. USER PRIVACY IS AN OPEN ISSUE

In a research report [Waidner (1998)] "insecurity of financial transactions" and "loss of privacy" are stated as the most frequently cited impediments to electronic commerce. Revenue from Internet business is predicted to exceed £300 billion pounds sterling[1] by 2002 [Waidner (1998)] and with mobile e-commerce (m-commerce) -- seen as the next major development in Internet business -- having a predicted revenue in the order of £14.5 billion pounds sterling[2] by 2004, end-to-end security is seen as a must for building customer confidence [Nicolle (2000)].

The issues relating directly to securing payment transactions are currently being addressed with on-going research. Much work has been done to improve user privacy with the use of pseudonyms and anonymous payment

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35586-3_46

M. A. Ghonaimy et al. (eds.), *Security in the Information Society*

schemes such as e-cash. Techniques to provide Anonymity Services[3] are under investigation [Oppliger (1999)]. However, *pervasive anonymity* and its two main primitives, *anonymous communication* and *unlinkable credentials*, remain as open issues [Waidner (1998)] within computer science research.

Ensuring users' privacy in e-commerce is important because people carry their expectations of real-world market places to the electronic market place. For example, an individual visits a shop on the high street. They may wander around the shop and view the merchandise for sale. They may select what they want to purchase, take the goods to the checkout, pay by cash and leave with their purchase and do so with total anonymity. At no time during this process are they required to divulge any personal information. They are not required to identify themselves or where they live. They are not required to state which shops they have previously visited or where they intent to go next. What is more, such information is not obtained in a surreptitious manner. The shopper expects to go about their lawful business and not be followed through the town having their actions observed and noted. Indeed, society protects us from such intrusions of privacy through the enactment of law. There are, indeed, variations to this high street shopping scenario that mean the shopper is no longer anonymous. One instance is payment by debit/credit card instead of cash. In this case, both the shop and the card company has a record of the card details (card holder name, card number, expirary date) plus the transaction details (debit amount, time, date, location) - the shop know the shopper's identity and the card company know how the shopper has spent their money. However, the information obtained is only that which is required to complete the payment process accurately. The shopper does not expect the card to volunteer details of previous transactions or the billing address, or for the shop till to obtain such information by interrogating the card. The shopper expects their privacy to be protected.

It is these reasonable expectations - of being able to shop anonymously or at least with a high degree of privacy - that are being taken to the electronic market place but not being fully met.

2. BACKGROUND AND MOTIVATION

This paper presents the background work to an ongoing project to provide a pervasive accountable anonymity scheme suitable for m-commerce users who work for an SME. This type of user has been chosen for these reasons:

- SMEs (like individual users) are unable to benefit from the economies of scale that are available to larger organisations. SMEs (and individual users) are most likely to 'shop around' for

the best deal and as a consequence, they develop "ad-hoc" trading relationships as and when necessary rather than forming formal trading agreements with specific partners.

- and because of their frequent and continuous use of the Internet, SME employees represent users, which are relatively easy to profile (although it is the employer's activities that are at risk, not the individuals).

As the following brief review will illustrate, current business-to-business (b2b) e-commerce solutions do not address the needs of such users. E-mail is the most basic form of b2b e-commerce. It is well established and already replaces communications such as informal business letters, phones calls, faxes, printed product specification. Payments are typically made 'out--of--band' (for example via cheques or funds transfers). Timing of these payments is usually independent of the delivery date (e.g. a customer account is maintained and settled monthly) [Lacoste et al (1998)]. This is possible because *trust has already been established* -- partners in b2b e-commerce often have formal trading agreements where specific liabilities are agreed in advanced and a secure communication channel is created solely for the use of the partner(s). As more organisations become e-business enabled, the emphasis will shift toward more flexible and spontaneous relationships, similar to the potentially one off relationships that exist between general users and on-line shopping merchants. Solutions that provide dynamic, flexible trading networks that support operational efficiency and new business opportunities are being advocated by 'not-for-profit' organisations such as Rosetta Net [RosettaNet]. At present, the more sophisticated forms of b2b e-commerce comprise bespoke solutions designed to provide seamless business processes and accurate (and/or) real-time information exchanges between suppliers, manufactures, banks, trading partners, employees and customers. They typically implement EDI (Electronic Data Interchange) via open standards such as OBI (The Open Buying on the Internet) and XML/EDI. The OBI standard is "an open, flexible framework for business-to-business Internet commerce solutions" but is currently focused only on automating high-volume low-value transactions [OBI Consortium (1999)]. The XML/EDI framework is more general and provides a "dynamic process that can be infinitely extended" which supports an "ad-hoc" model (intended for use by smaller trading partners) [Peat et al (1997)]. However, XML/EDI does not specifically address security problems. Rather, messages are exchanged using Secure HTTP or Secure multipart Internet e-mail message (MIME) [Marchal et al(1998)], which provide message confidentiality, but not anonymity.

In addition to b2b e-commerce over the Internet, the advent of WAP on GSM and the prospect of UMTS on 3G mobile phones has lead to the

emergence of the *wireless*-Internet and the phenomenon of m-commerce. Organisations and individuals now have the opportunity to conduct business over the Internet using mobile phones and portable computing devices. Such technology enables business to be conducted any time, any place. Despite the opportunities for growth, development of e-commerce, and in particular, m-commerce, has not progressed as fast as recently predicted. Security concerns, privacy issues in particular, are often cited as being the single most important barrier to e-commerce [Oppliger (1999), Lacoste et al (1998)].

A scheme that ensures the anonymity while maintaining the accountability of individuals who use mobile computing devices to perform numerous, ad-hoc, b2b transactions with parties over the Internet has not yet been devised. The development of such a scheme is a novel contribution to the research area within computer science known as pervasive anonymity.

3. THE IMPORTANCE OF PROCESSES

Electronic commerce is about business processes. Much of the work done to-date on securing e-commerce has focused on single 'steps' of the business process e.g. payments [Waidner (1998)]. Security tends to be a weak link problem, where the total security is no better than the weakest part [Pipkin (1998)]. Therefore, securing a particular transaction type is a good start, but this approach does not provide 'comprehensive' security. At present, there is not much technology to protect users' privacy and anonymity. Where a particular step (e.g. payments) can be anonymized with the application of data encryption, it is unclear how to ensure 'pervasive anonymity' across the entire business process.

4. PROPERTIES OF AN IDEAL PERVASIVE ANONYMITY SERVICE

An ideal pervasive anonymity service will posses the following properties:

- By definition, a pervasive anonymity service shall ensure the anonymity of the user across the entire e-commerce (business) process. That is, the anonymity of the user is ensured end-to-end, both in terms of physical connectivity (i.e. communications infrastructure) and e-commerce transactions.
- The pervasive anonymity service shall ensure sender anonymity by preventing the non-essential disclosure of who, what and where, in respect to the user, to any other party. (Receiver

anonymity may be unnecessary since the receiver is the merchant and most merchants need to be known (e.g. they advertise) in order to attract customers. Sender-receiver unlinkability may be considered not necessary if the user has data confidentiality plus identity and location anonymity.)

- The pervasive anonymity service shall provide levels of anonymity ranging from absolute privacy, as the maximum, to possible innocence, as the minimum. Ideally, the degree of anonymity shall be user selectable.
- The pervasive anonymity service shall maintain Confidentiality Level 1 where such confidentiality already exist i.e. mobile phone air interface. That is, any failure of the anonymity service shall not reduce the users privacy below the level that already exists.
- The pervasive anonymity service shall include an on-line revocation service as a means of providing accountability for any abuses occurring whilst the anonymity service is in use. This is of particular important during payments (to prevent cheating). The idea of 'getting away with it', because the user has total anonymity, may prove too much temptation for some. A revocation facility may be used as an incentive for good behaviour. By being on-line, the revocation process may be performed much sooner and faster than the traditional approach of involving a legal authority. The most flexible approach and one which may be considered user friendly is to have levels of revocation that the user agrees to in advance. E.g. If a minor abuse of anonymity occurs then the user's on-line identity is revealed and may result in that user being barred from specific facilities. If the user performs an illegal act then their real world identity is revealed and legal authorities are notified.
- In order to support on-line revocation and to facilitate dispute resolution, the pervasive anonymity service shall also include a non-repudiation service.
- Furthermore, the pervasive anonymity service shall ensure all of the above-mentioned properties across each individual transaction phase and across multiple transactions whether they are completed successfully, aborted intentionally or otherwise by any party, or involve a dispute.

5. WHY DATA ENCRYPTION IS NOT THE ANSWER

Waidner (1998) state "Electronic commerce demands strong confidentiality, which can be implemented only by strong encryption schemes." However, encrypting everything is not practical or cost effective. In some countries, including the UK, the widespread use of strong encryption is being restricted on the grounds of national security. In other countries the use of encryption is illegal. In the UK payments on-line are encrypted by trusted third parties licensed to do so and they charge the merchants for their services. Whilst it may seem tempting to say 'hang the cost - encrypt all transmissions just to be sure', blind faith in such a policy is misplaced. The existence of such secure channels has come about due to public opinion that credit card details sent over the Internet in clear text were liable to be stolen on--the--fly by hackers. This is technically possible, although the usual route to stealing such information is to break in to the merchant's customer database where personal details are stored un-encrypted. One counter-argument is to suggest that absolutely everything is encrypted. It would appear a neat solution with just two drawbacks: i) for the information to be of any use, it will need to be deciphered every time it is required, which will increase processing costs. What is more, how do you ensure the security of the temporarily un-encrypted data? How temporary is temporary? ii) the encryption of everything would include the encryption of routine traffic. Part of that encrypted traffic would be predictable information providing an observer with enough 'clues' to reverse the algorithm. The advantage of encryption is lost. It is simply a matter of time and computational power before the encrypted messages are deciphered.

Further more, encryption alone does not ensure anonymity. Consider the following situation where two companies are preparing for a merger. Their negotiations require full and complete confidentiality. The use of encryption may safeguard the contents of the communications but does not reduce the visibility of such communications. An observer may be able to draw inference from the traffic patterns.

6. OPEN ISSUES

The state of the art anonymity services surveyed include a number of schemes: electronic- and anonymous-payment [Cybercash, Digicash, E-gold, IBM, Mondex, CMU], unlinkable credentials [Chaum (1985), Shi et al (2000), Camenisch et al (2000)] and anonymous communications [Preneel (1999), Chaum (1981)] including anonymous connections[Syverson (1998)],

anonymous e-mail [Preneel (1999)] and anonymous web browsing [Preneel (1999), Reiter et al (1998), Shields (2000], plus anonymity services specifically for wireless networks [Jokela (1999),

Buttyan et al (1999), Shi et al (1997)]. The following open issues apply to the surveyed anonymity services in general:

- Current state--of--the--art anonymity services, the majority of which have been developed for implementation on the wired-networks, do not *ensure* user privacy - individual schemes can be defeated by specific attacks. The more robust schemes suffer portability problems such as performance and scalability.
- Encryption Overhead - many of the schemes discussed use encryption to provide anonymity and these have one disadvantage in common. The data has to be cryptographically processed resulting in an overhead. In addition to this, where connection anonymity is provided by mixes the network traffic is increased (by the average number of hops). Therefore, for any given application, anonymity through encryption results in a performance decrease.
- Many of the schemes require intervention from a real world Legal Authority to invoke any revocation scheme that may exist. This is slow and costly, and for these reasons more likely to be initiated by organisations and not individual users.
- There is no overall scheme to provide *pervasive* anonymity.

The application specific services i.e. anonymous payments, anonymous e-mail and anonymous web browsing, by design apply only to specific transaction types. In order that a pervasive anonymity scheme be developed, only the more general services will be considered further.

A comparison, between the ideal pervasive anonymity scheme described earlier and the surveyed anonymity services, has been conducted.It is noted that no one scheme completely satisfies all the requirements of the ideal pervasive anonymity service. In particular, none of the anonymous communications schemes support anonymous payments or have any form of revocation. Only a few have non-repudiation as an extension. Unlinkable credentials compare more favourable: this is a more recent area of research and so the value of incorporating payments schemes (a research area with much commercial interest) and non-repudiation and revocation (to counter economic fraud) has been recognised by researchers. The portability of such schemes to mobile networks is unknown or at the least, questionable. Anonymity schemes specifically for the UMTS wireless networks are more complete. They are, by design, (more) suitable for implementation on UMTS mobile devices and networks. Solutions to the issues of non-repudiation, on-line revocation and incorporation of anonymous payments either exist as

proposals or have been listed as extensions to the work. The two most complete schemes [

Buttyan et al (1999), Shi et al (1997)] involve a major change to the mobile phone infrastructure and business processes through the addition of third parties.

7. DISCUSSION

An individual user's anonymity is ensured by minimising disclosure of information to other parties. Such information is the 'what' (data), 'who' (identity) and 'where' (location) of that user. The desired level of disclosure, in an ideal world, is zero. However, this is not always practical. There are elements within the telecommunications networks that 'need-to-know' certain information in order to perform their tasks e.g. an ISP needs to know 'who' for authentication, 'what' data is requested and 'where' to send the requested information. The non-disclosure of 'who' may be achieved with the use of pseudonyms and 'where' with the use of anonymous connection methods. However, the 'what' needs to be made known. Therefore some degree of anonymity can be achieved whilst meeting this 'need-to-know' requirement by unlinking the 'who/where/what' data. However, given time and continued use, any on-line identity will develop history and may then be subject to on-line profiling.

One way of avoiding the development of history associated with an on-line identity may be achieved by making the identity and history unlinkable. The greatest degree of privacy and anonymity might be achieved by unlinking identity and each transaction phase i.e. for each phase of a transaction (request, offer, order, payment and delivery) a new unlinkable identity is used. This has the drawback of being computationally expensive (how to manage an infinite number of unique and unlinkable identities for each individual user for every single transaction phase or step?) and unnecessary since if one complete transaction cycle (request through to payment/delivery) is linked to an identity then little can be discernible from this - a sample of one does not indicate a trend.

At present, non-disclosure of data is already achieved through the application of cryptographic methods (i.e. data confidentiality is achieved by the application of data encryption) and may therefore be viewed as a closed issue. There are also several methods for ensuring the non-disclosure of identity and the non- or partial-disclosure of location. However, a scheme that ensures anonymity through the prevention of on-line profiling by unlinking history (transactions processes) and user identity is novel work. Furthermore, such a scheme that does this and provides an anonymous

payment scheme, an on-line revocation mechanism for accountability, a non-repudiation service for dispute resolution and is suitable for implementation on UMTS mobile devices is a further contribution to the research areas of pervasive anonymity and mobile e-commerce.

8. CONCLUSIONS AND FUTURE WORK

Having reviewed the state of the art anonymity services and compared these to our ideal pervasive anonymity scheme we are able to list ongoing and future work. At present, there is no one single scheme that:

- provides anonymity for m-commerce transactions

and

- provides end--to--end (or pervasive) anonymity;

and

- provides on-line revocation with non-repudiation for accountability and dispute resolution;

and

- incorporates an anonymous payment scheme

and

- is robust and secure for transactions that are successful, those that are aborted and those that result in dispute;

and

- meets the performance constraints imposed by UMTS mobile devices and commercial telecommunications networks.

This list represents the Aims of this project.

Notes

[1] Approximately - converted from US dollars.

[2] Again, converted from US dollars

[3] E.g. receiver anonymity (anonymous browsing of the web), sender anonymity (anonymous publication on the web) and transaction anonymity (stocker broker systems, voting and auctions).

References

Buttyan et al (1999)
Levente Buttyan and Jean-Pierre Hubaux.
Accountable anonymous access to services in mobile communication systems.
Proceedings of the 18th IEEE Symposium on Reliable Distributed Systems, page 384, 1999.

Camenisch et al (2000)
J.~Camenisch and A.~Lysyanskaya*.
Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation.
Research report rz 3295 (93341), IBM Zurich Research Laboratory and *MIT, 2000.
(Found at http://www.zurich.ibm.com on 6 Dec 00).

CMU
Carnegie~Mellon University.
Netbill.
(http://www.ini.cmu.edu/NETBILL/home.html)

Chaum (1981)
David Chaum.
Untraceable electronic mail, return addresses and digital pseudonyms.
Communications of the ACM, 24(2):84, 1981.

Chaum (1985)
David Chaum.
Security without identification: Transaction systems to make big brother obsolete.
Communications of the ACM, 28(10):1030, 1985.

Cybercash
Cybercash.
(http://www.cybercash.com.)

Digicash
DigiCash.
Ecash by digicash.
(http://www.digicash.com/ecash/ecash-home.html).

E-gold
E-gold.
(http://www.e-gold.com).

IBM
IBM.
Ibm micro payments.
(http://www.hrl.il.ibm.com/mpay).

Jokela (1999)
Petri Jokela.
Wireless internet access using anonymous access methods.
IEEE 1999 International Workshop On Mobile Multimedia Communications (MoMuC'99), page 194, 1999.

Lacoste et al (1998)

G.~Lacoste et~al.
Semper - secure electronic marketplace for europe.
LNCS, (1854), 1998.

Marchal et al(1998)
B.~Marchal N.~Mikula B.~Peat, D.~Webber et~al.
Guidelines for using xml for electronic data interchange.
Open standard, XML/EDI Group, 1998.
(Home Page URL: http://www.xmledi.org).

Mondex
Mondex.
Mondex electronic cash.
(http://www.mondex.com).

Nicolle (2000)
Lindsay Nicolle.
Life by phone
The British Computer Society: The Computer Bulletin, 2(6):20, 2000.

OBI Consortium (1999)
OBI Consortium.
Open buying on the internet - technical specifications v2.1
Technical report, OBI Consortium, 1999.
(Found at www.openbuy.com, on 16 April 01).

Oppliger (1999)
R. Oppliger.
Shaping the research agenda for security in e-commerce.
Proceedings of the 10th International Workshop on Database and Expert Systems Applications, page 810, 1999.

Peat et al (1997)
B.~Peat and D.~Webber.
Introducing xml/edi - the e-business framework.
(http://www.geocities.com/WallStreet/Floor/5815/guide.htm), 1997.

Pipkin (1998)
D.~L. Pipkin.
Information Security - Protecting The Global Enterprise.
Prentice Hall, 2000.

Preneel (1999)
Bart~Preneel Joris~Claessens and Joos Vandewalle.
Solutions for anonymous communication on the internet.
Proceedings of the IEEE 33rd Annual International Carnahan Conference on Security technology, page 298, 1999.

Reiter et al (1998)
Michael~K. Reiter and Aviel~D. Rubin.
Crowds: Anonymity for web transactions.
ACM Transactions on Information and Systems Security, 1(1):66, 1998.

RosettaNet
RosettaNet.
Rosettanet overview.
(http://www.rosettanet.org found April 2001).

Shi et al (1997)
Qi~Shi Bob~Askwith, Madjid~Merabti and Keith Whiteley.

Achieving user privacy in mobile networks.
IEEE Proceedings of the 13th Annual Computer Security Applications Conference}, page 108, 1997.

Shi et al (2000)
Q~Shi N~Zhang and M~Merabti.
Anonymous public-key certificates for anonymous and fair document exchange}.
IEE Proceedings on Communications, 147(6):345, 2000.

Shields (2000)
Clay Shields and Brian~N. Levine.
A protocol for anonymous communication over the internet.
Proceedings of the 7th ACM Conference on Computer and Communication Security, page~33, 2000.

Syverson (1998)
P.F.~Syverson M.~G.~Reed and D.M. Goldschlag.
Anonymous connections and onion routing.
IEEE Journal On Selected Areas in Communications, 16(4):482, 1998.

Waidner (1998)
M.~Waidner.
Open issues in secure electronic commerce.
Research report rz 3070 (93116), IBM Zurich Research Laboratory, 1998.
(Found at http://www.zurich.ibm.com on 22 Nov 00).
