

Micropayments for Wireless Communications

DongGook Park^{1,2}, Colin Boyd² and Ed Dawson²

¹Korea Telecom, Access Network Laboratory,
17 WooMyeon-Dong, SeoCho-Gu, 137-792, Seoul, Korea
dgpark6@kt.co.kr

²Queensland University of Technology, Information Security Research Centre,
2 George Street, GPO Box 2434, Brisbane, Queensland 4001, Australia
{c.boyd, e.dawson}@qut.edu.au

Abstract. Electronic payment systems for wireless devices need to take into account the limited computational and storage ability of such devices. Micropayment schemes seem well suited to this scenario since they are specifically designed for efficient operation. Most micropayment schemes require a digital signature and therefore users must support public key operations and, furthermore, a public key infrastructure must be available. Such schemes are not suitable for current wireless systems since public key technology is not supported. We examine the SVP micropayment scheme which overcomes this problem by using only symmetric key cryptography and relying on tamper resistance. Some limitations are observed in the SVP micropayment scheme and an enhanced scheme is proposed suitable for current generation wireless communications.

1 Introduction

Over recent years, there has been a significant increase in both the scale and the diversity of electronic transactions over the Internet. Electronic commerce (E-commerce) means electronic payment (E-payment) in a narrow sense but it may mean *electronic business* in a broader sense which also includes the exchange of information not directly related to the actual purchasing activities [GrFe99]. In this paper, the term *E-payment* will be used to describe purchasing activity itself between buyers and sellers. Secure electronic payments will not only make purchasing activities more flexible and convenient but also create as yet unimagined new markets [Wayn97].

As the integration of computing and communications continues, wireless computing devices are of increasing importance as devices to access the Internet and to make electronic transactions. Many E-payment schemes have been proposed, and a lot of them assume the use of today's well-established credit card business environment. The most well-agreed and dominant E-payment protocol is the SET (Secure Electronic Transaction) protocol, produced by Visa and MasterCard to be their standard for processing credit card transactions over networks like the Internet. This, and other similar schemes, use extensive cryptographic technologies, a lot of which are based on public-key cryptography, to satisfy high level security requirements such as nonre-

pudiation. These protocols are all appropriate for medium to large transactions (macropayments) of more than \$5 or \$10.

These macropayment protocols will be too expensive and time-consuming when applied to inexpensive transactions, 50 or 25 cents and less, because of the transaction charges of card companies and the computational cost of public-key signature/verification. They also place a heavy burden on the computational and storage capabilities of currently available wireless devices. Without appropriate cheap alternative schemes, the light-weight transaction market cannot be developed to its full potential. This market typically includes selling *inexpensive* information software, and services (e.g. directory search or games), usually delivered online, and is a prime market for wireless communications.

Several schemes have been proposed for micropayment. To reduce the computational and signalling burden down to a reasonable level which can be justified in micropayment environments, they try to avoid *public-key* cryptography partially or entirely. Their dependency on *on-line* access to banking/clearing systems is also small compared to macropayment schemes. In this paper, we focus on micropayment schemes because this category not only directly addresses the limited resources of mobile communications but also is the most reasonable option for applying to the light-weight E-payment by mobile users.

Figure 1 shows a general scenario in E-payment environments, adopted from [Ahuj96].

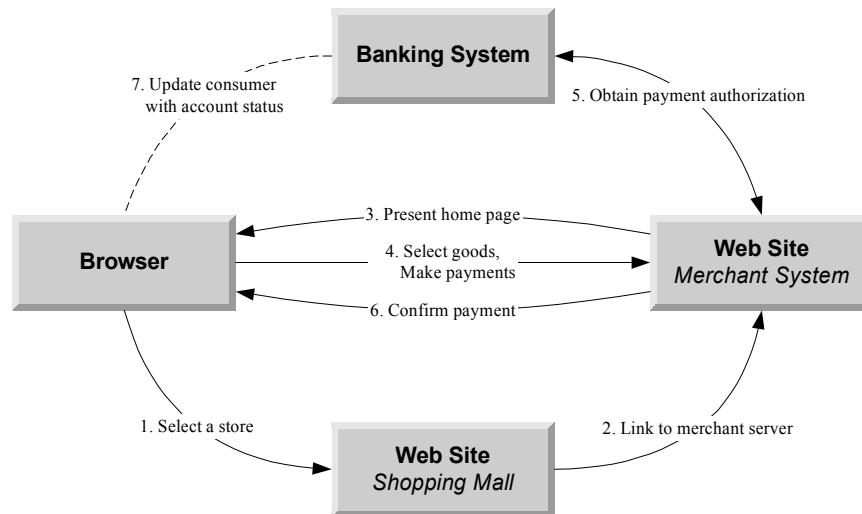


Figure 1: E-payment Environments

In this scenario, there are four elements or role players as follows.

- **A consumer** along with a Web browser uses the hyperlinks from the mall to access the merchant's home page.
- **A merchant** system residing on an online Web server with a connection to Web browsers over the Internet consists of the home page and related software to man-

age business.

- **An online shopping mall** may help direct consumers to the merchant server. It may pay to enlist with one or more well-known shopping malls.
- **A background banking network** supports electronic payments from consumers to the merchant. This network may include two types of banks:
 - **a merchant's bank** maintains the account for the merchant, authorizes and processes the payments. It may use on-line real-time link to the merchant so as to allow online authorization of consumer payments, and the link with the consumer's bank for verifying the transactions.
 - **a consumer's bank** manages the account for the consumer, and has an offline link to the consumer, such as via postal mail or e-mail.

These four role players take part in the following sequence of E-payment related activities.

1. The consumer accesses the shopping mall and selects a shop for purchasing certain items.
2. The shopping mall server accesses the merchant system for the selected shop.
3. The merchant system presents the store's home page to the consumer. It also includes information on the various goods available from this store.
4. The consumer selects the desired goods, interacts with the merchant's system, and makes the payments.
5. The merchant system accesses its bank for authorization of the consumer payment.
6. The merchant system informs the consumer that the payment is accepted and the transaction is completed. (At a later time, the merchant's bank obtains payment from the consumer's bank.)
7. The consumer's bank informs the consumer of the money transfer through mail such as a monthly report or online bank account.

2 E-Payment Mechanisms in Mobile Environments

The European ASPeCT project [ASPe96] has investigated security services for next generation wireless communications. The project included proposals for secure billing using hash based micropayments in combination with a digital signature scheme [ASPe97]. The digital signature serves a dual role as it is also used for authentication purposes during the establishment of a session key to secure the session data [HoPr98].

Provision of secure and trustworthy E-payment mechanisms will be the most critical factor for the success of E-commerce. Such a payment scheme must satisfy the following requirements [Ahuj96].

- Strong authentication of each party using certificate and digital signature
- Privacy of transaction using encryption
- Transaction integrity using message digest algorithms

- Nonrepudiation to handle disputes about the transaction

There are many classification methods for E-payment schemes, many of them rather orthogonal to each other. The following list shows an example of many classification criteria, most of which are described in detail in the report of the ASPeCT protocol [ASP97].

- Electronic purse/cash/credit
- On-line/off-line
- Credit-based/debit-based
- Software-based/tamper-resistant hardware
- Macropayment/micropayment

The public-key based security protocols for mobile users are not likely to be deployed in the early stage of future mobile communications such as IMT2000 [Buha97, ITU97]. They will be introduced into the systems when a fully-fledged public key infrastructure is available which may yet take a number of years. Therefore the assumption of limited use of tamper resistant devices by mobile users for E-payment in the near future is very likely and reasonable. Payment takes place using hashing mechanisms which are very cheap in computation while the broker can remain off-line. In mobile communication environments, there is already a well established infrastructure for billing users. This means that we do not need to establish extra clearing/banking infrastructure for mobile E-payment. A suggested model for billing users for micropayments is presented in Figure 2.

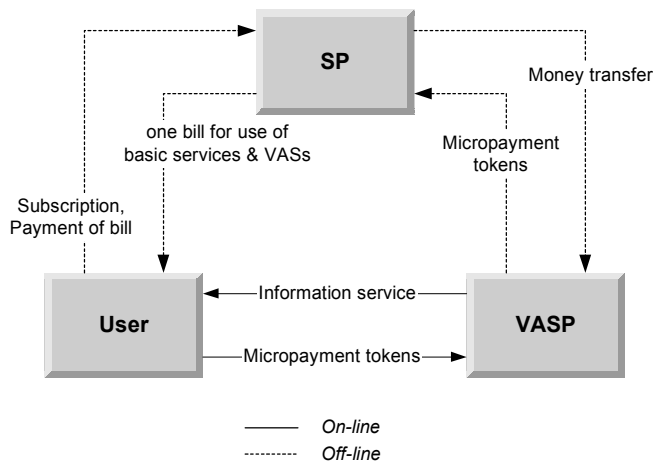


Figure 2: Billing of Micropayments

The role players in the mobile micropayment shown in Figure 2 comprise mobile users, service providers (SPs) and value added service providers (VASPs). Here, a SP plays the role of the broker in general micropayment environments. It bills the user for both basic and value-added services, and then redeems the relevant payment to the

VASP. Considering the light-weight nature of most transactions to be carried out through mobile communications, the VASP-SP interface will be usually off-line.

3 Micropayments using Hash Chains

The most widely studied and promising approach involves using a public-key signature together with a hash-chain. Four similar schemes have been proposed: PayWord [RiSh96], *iKP*'s micropayment [HSW96], Netcard [AMS95], and Pedersen's scheme [Pede95]. The basic idea is that a signature value generated using a public key operation is spread over many other cryptographic values derived by much more efficient one-way functions such as hash functions. In other words, the effect of a digital signature is reused many times over subsequent messages (containing preimages of a specific hash). This mechanism was originally proposed for use in an authentication scheme by Lamport [Lamp81]. The following description of the hash chain scheme is based on *PayWord* proposal of Rivest and Shamir [RiSh96].

3.1 Issuing user certificate

- The *user* U establishes an account with a *broker* B . U supplies personal details to B , such as a credit card number and delivery address, together with U 's public key, K_U . U 's aggregate charges will be charged to her credit-card number.
- The broker issues to U a PayWord Certificate, which is a signed statement by B containing:
 - broker's name B
 - user *name* U
 - user's IP-address
 - user's public key K_U
 - expiration date $ExpDate$
 - other information, possibly including user-specific information such as:
 - a certificate serial number,
 - credit limits to be applied per vendor,
 - information on how to contact the broker,
 - broker/vendor terms and condition.

The user's certificate has to be renewed by the broker regularly (e.g. monthly); the broker will do so only if the user's account is in good standing.

3.2 Typical scenario

The user's certificate authorizes the user to make Payword chains, and assures vendors that the user's passwords are redeemable by the broker. When the user U wishes to make a micropayment she clicks on a link to a vendor V 's charged web page.

- The user's browser determines whether this is the first request to V that day.

- For a first request, U computes and signs a *commitment* to a new user-specific and vendor-specific chain of payments c_1, c_2, \dots, c_N .
 - The user creates the payword chain in reverse order by picking the last payword c_n at random, and then computing

$$c_i = h(c_{i+1}) \quad \text{for } i = N-1, N-2, \dots, 0.$$
 Here c_0 is the root of the payword chain, and is not a payword itself. The *commitment* contains the root c_0 , but not any payword c_i for $i > 0$.
 - commitment $M = \{V, \text{UCert}, c_0, \text{Date}, \text{OtherInfo}\}$
 - commitment includes both identities of the user and the vendor, and so is both user-specific and vendor-specific.
- The user provides this commitment and her certificate to the vendor V, who verifies the signatures.
- The i -th payment (for $i = 1, 2, \dots$) from U to V consists of the pair (c_i, i) , which V can verify using c_{i-1} .
- At the end of each day, V reports to the broker B the last (highest-indexed) payment (w_l, l) received from each user that day, together with each corresponding commitment.
- The broker charges subscription and/or transaction fees.

Figure 3 shows the generation of hash-chain and commitment in the above scheme.

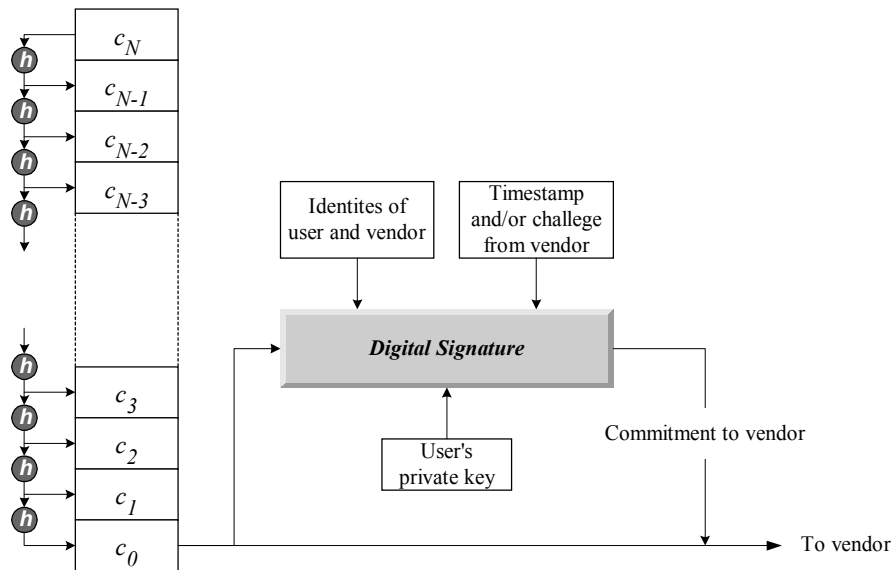


Figure 3: Hash Chain Protocol

3.3 Problems with Existing Hash Chains Schemes

There are a number of significant overheads which are implied by this model. We would like to emphasise that these are not currently present for most mobile users.

- The user must have the capability of public key operations in her mobile communications device.
- The user must have the ability to generate, or acquire, a suitable public key.
- There must be some mechanism for users to be able to revoke certificates when they are compromised, and for merchants to know that certificates have been revoked.

Wireless communications systems in the current generation use only symmetric key based cryptography [Mehr97, Moha96]. This is the main problem with the wireless application of existing micropayment schemes based on hash-chains. In Section 5 we will examine how to include hash chains into a symmetric cryptography setting so as to be able to benefit from the idea in the current wireless context.

4 SVP Scheme based on Tamper-Resistant Device

An alternative to use of a digital signature for micropayments is to employ a tamper-resistant device together with symmetric key cryptography. One such scheme called Small Value Payment (SVP) was proposed by Stern and Vaudenay [StVa97]. It aims to provide an even cheaper and more effective micropayment scheme than the approach using hash chains, by avoiding the use of asymmetric key cryptography. Instead, it requires the use of tamper-resistant devices both at the consumer and the merchant sides. We note that current mobile communications systems include use of a smart card which provides a degree of tamper resistance. The SVP scheme is illustrated in Figure 4.

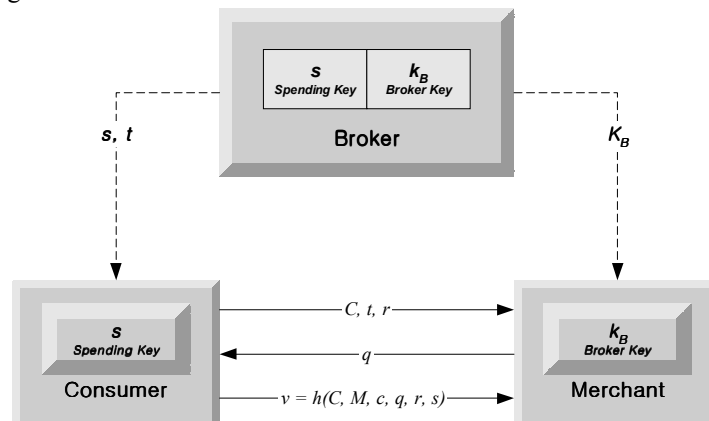


Figure 4: Small Value Payment Protocol

Initialization. The broker B generates its own secret key k_B and communicates it in a secure way to the device of each merchant, where k_B is a common value to all merchants. It also generates and computes a *random value* t and a *spending key* $s = \text{Mac}_{k_B}(C, t)$ for a consumer C , where s is unique to the consumer. In this equation Mac is a message authentication code which should have the property that it cannot be formed without knowledge of the key k_B and it is infeasible to find a different input (C, t) which gives the same output s . Both s and t are given by B to C as authorisation for C to spend an agreed amount of money.

4.1 Payment protocol

The payment protocol can be described as follows. In this description h is a hash function which can be regarded as a MAC operation with the spending key s as the MAC key.

C : consumer, M : merchant

1. $C \rightarrow M: C, t, r$ (r : random number chosen by C)

2. $C \leftarrow M: q$ (q : random challenge)

3. $C \rightarrow M: v = h(C, M, c, q, r, s)$ (c : microamount)

M : checks if $v = h(C, M, c, q, r, \text{Mac}_{k_B}(C, t))$,
keeps an account balance for the user and increases C 's account by c , and
(optionally) stores (t, q, r, v) if he is suspicious about this payment.

From the response in message 3, M is able to determine whether C is in possession of the spending key s . If so M knows that C was authorised to make payments associated with the value t . Note that there is no mechanism to prevent C using s any number of times. In this sense SVP is a credit based scheme in which C is trusted to pay the bills accrued from use of s .

4.2 Payment clearing

The merchant regularly sends the broker a statement of the amount of money spent by consumers, and the broker monitors to check if the accounts are consistent. If not, the broker requests a valid proof (C, c, t, q, r, v) of payment from M . If it cannot be provided, the broker just refuses the payment and records that there must be a problem with C or M . *If such a proof is released, the broker pays and checks if (M, q, r) has already credited to M .* If it has, the broker suspects the merchant to be dishonest. If not, the broker stores (M, q, r) in the (C, t) -records.

4.3 Problems with the SVP scheme

We have identified a number of problems with the SVP scheme which affect both the security and efficiency of a practical implementation in the wireless environment.

- There is no signature from the user, and thereby the scheme does not provide non-repudiation (the merchant and/or the broker can generate all the security parameters). This is why the scheme depends heavily on the use of tamper resistant devices. The compromise of only one tamper resistant device in the merchant side enables an attacker to impersonate other consumers.
- The shared secret key k_B between the broker and all the merchants must be the same, because the user's spending key is a function of the key k_B . Every merchant (more precisely, its tamper-proof device) in transaction with the customer must be able to compute the spending key. Stern and Vaudenay recognise this problem in their paper and suggested a solution in which the broker has several secret keys, a subset of which is shared with each merchant. Customers must then obtain multiple spending keys and provide a corresponding subset of spending keys to the merchant. This solution adds storage and complexity to the scheme, while compromise of a set of merchants keys can still allow spending at different merchants.
- The user and the VASP must execute the three-way challenge-response protocol for every micropayment, which is inefficient compared with the hash chain approach exchanging only one message (preimage of a hash chain).
- *Weakness in the message freshness*: the mechanism of replay-detection against the merchant is vulnerable to the following attack scenario:
 - Broker resets all the account records periodically, e.g., every month.
 - Merchant reuses the old parameters (used in the previous months).
 - Broker checks if (M, q, r) has been used before, but the check cannot be applied to all the transaction out of the manageable period.

The last problem with regard to replay attack can be easily fixed by adopting an additional commitment which is generated by the consumer and checked by the broker, and including date information in the commitment computation procedure. This prevents a merchant from cheating the broker with old payment data received from the user previously. We have included such a mechanism in the new scheme described in Section 5.

5 A New Scheme Using Tamper-Resistant Devices

Exploiting the advantages of both the hash chain and the tamper-resistance schemes, we have designed a new scheme. We can avoid both the expensive asymmetric cryptography even for the payment initialization, and challenge-response for each payment of microamount.

Figure 5 shows the required setting of this scheme assuming the use of tamper-resistant devices. The role players in this scheme are taken by those in mobile envi-

ronments: the user, the VASP, and the user's SP. There are three distinct kinds of shared secret keys:

- K_{US} between the user and the SP;
- K_{VS} between the VASP and the SP;
- K_{UV} between the user and the VASP.

In fact, the shared key K_{UV} is derived from the K_{VS} which is common to every VASP. Also, for simplicity of key management, the user-SP shared key K_{US} is computed using the user identity and a master key K_S of the SP.

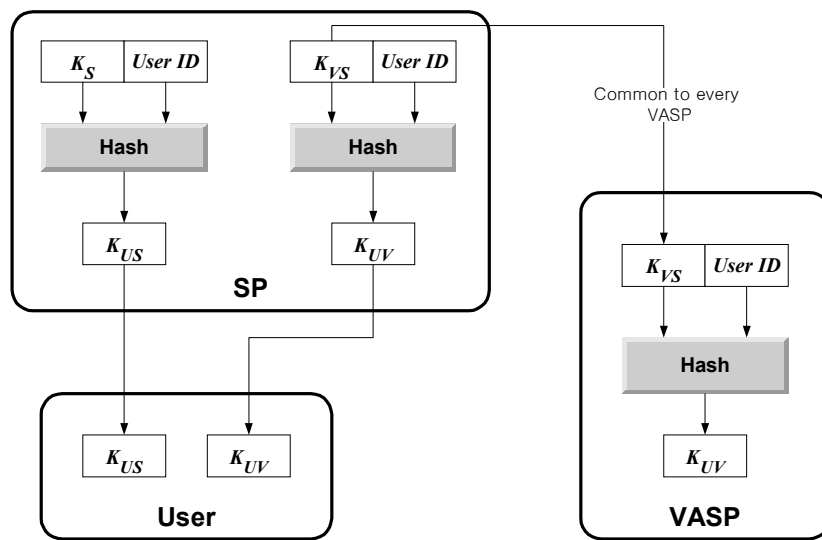


Figure 5: Enhanced Payment Scheme

The payment protocol assuming the use of hash chain is described in Figure 6. The user generates two separate commitments: one to the VASP, and another to the SP. The usage of pre-images of the hash chain is the same as in Figure 3. The computation of commitment for the VASP uses the shared key K_{UV} , the identities of the user and the VASP, random challenge r_V and time-stamp TS_V from the VASP, and the result of hashing c_θ . This commitment value is, in turn, input, together with the shared key K_{US} between the user and the SP, to the commitment generation procedure for the SP. Note that by including the time-stamp which may be simply the date (yymmdd), this scheme is secure against the replay attack by the VASP which was possible in the scheme described in the previous section. The burden of computing the hash chain, if any, may be alleviated by reusing the previously generated hash chain in such a way that the remaining preimage with the smallest index is used for the commitment generation. Summarizing, the setting of this scheme basically comes from the SVP mechanism proposed by Stern and Vaudenay, and the actual payment protocol from the hash chain setting.

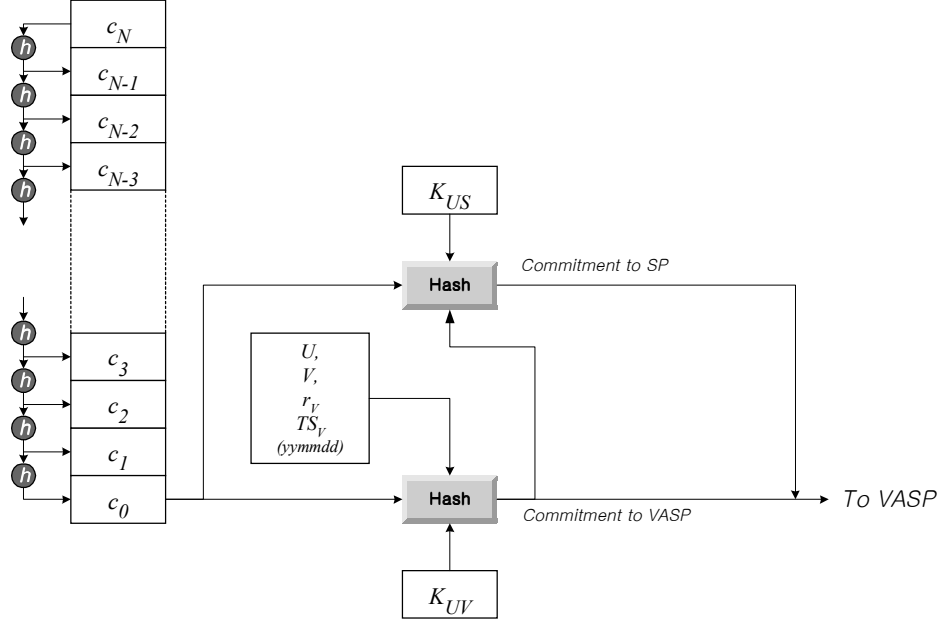


Figure 6: Payment Protocol

An example payment protocol set based on this enhanced scheme is shown in the following. We first summarise the goals of payment initialization protocol as follows.

- Mutual authentication between the user and the VASP
- Authentic and secure key establishment
- Mutual session key control
- Weak non-repudiation of the user to both the VASP and the SP based on shared keys
- Payment parameter initialisation

5.1 Payment initialization protocol

U : User, V : VASP, S : SP

1. $U \rightarrow V$: U, r_U
2. $U \leftarrow V$: $r_V, h(r_U, r_V, K_{UV}), ch_data, TS_V$
3. $U \rightarrow V$: $c_0, commitment_V, commitment_S$

U : $commitment_V = h(U, V, K_{UV}, r_U, r_V, TS_V, ch_data, c_0)$
 $commitment_S = h(commitment_V, K_{US})$

Protocol description

- *First message*: the user sends the VASP his identity U and a random challenge r_U .

- *Second message*: the VASP computes the common shared secret key K_{UV} using the user identity U and the share secret key K_{VS} , chooses a random challenge r_V and computes $h(r_U, r_V, K_{UV})$. It delivers to the user the random challenge r_V , $h(r_U, r_V, K_{UV})$, charging data ch_data and the time-stamp TS_V .
- *Third message*: upon receiving the second message from the VASP, the user computes $h(r_U, r_V, K_{UV})$, the value of which is compared with the received hash value from the VASP. The match of two values guarantees that the VASP has an authentic secret key K_{VS} . After that, the user computes the two commitments to the VASP and the SP using the secret keys K_{UV} and K_{VS} , respectively. The VASP checks the first commitment value by computing the same calculation as the user and comparing the result with the received value. If both values match, then it has confidence that the user has the correct shared secret key K_{UV} .

5.2 Payment protocol

U : User, V : VASP

1. $U \rightarrow V$: c_j ($j = 1, \dots, N$)

Protocol description

When the user and VASP need to exchange the actual payment data for a unit of charged service, the user sends the relevant preimage of the hash chain. Note that the three-way challenge-response messages are not used but a simple tick (a preimage of the hash chain) is delivered from the user to the VASP when required. Therefore this scheme achieves a significant improvement in terms of signalling load from the tamper-resistant device scheme proposed by Stern and Vaudenay.

5.3 Payment clearing

V : VASP, S : SP,

1. $V \rightarrow S$: $c_0, c_{j_max}, j_max, U, V, r_U, r_V, ch_data, TS_V, commitment_V, commitment_S$

Protocol description

After the transaction, the VASP stores the payment data for billing, which includes the user identity U , the user's commitments to the VASP and the SP, and the required data for the verification of the signature, i.e., $r_U, r_V, ch_data, TS_V, c_0$, the last received pre-image c_{j_max} , and the corresponding index value j_max , which equals the total number of ticks paid by the user in the transaction. The SP checks the $commitment_S$ field by computing the same calculation as the user and comparing the result with the received value. The confidence gained by this check is to ensure that the commitment could not have been formed by the VASP, even if the tamper resistance of the VASP's device has been compromised. For this reason, we claim that this new scheme provides a weak form of non-repudiation of the user data.

5.4 Comparison with SVP

Compared to the original SVP protocol there are two main advantages that we can claim.

- Firstly, the interactive three move protocol for every micropayment has been avoided. This can be an important issue for mobile communications where call charges are still large in comparison with Internet based communications. It also reduces delay and removes the possibility of incomplete payment protocols due to communications failures.
- Secondly, the key used at payment time is user specific and used in combination with a key shared only with the SP (broker). This means that compromise of a VASP (merchant) does not allow impersonation of other users. More specifically, an attacker who obtains a merchant key will be able to forge payments, but these payments will be exposed as forgeries when the payments are cleared at the SP. This will allow the broker key, K_{VS} , to be immediately updated. In contrast, knowledge of a merchant key in the original SVP scheme, allows forgeries to be made which are undetectable.

If we compare the disadvantages of the SVP scheme with our enhanced version we see that all disadvantages have been overcome except that there is still no signature to provide non-repudiation of user payments. However, even in this regard there is a significant improvement since only the broker itself is able to forge user commitments, and not merchants as in the original SVP scheme.

6 Conclusion

In the foreseeable future, mobile communication terminals will be a major method for electronic commerce, at least in transactions of small amounts. The well-studied and efficiency-proven hash chain scheme relies on the existence of digital signatures and an associated public key infrastructure. In this paper the alternative of using a tamper-resistant device has been explored. It has been shown that the SVP scheme has limitations for use in this environment. We have proposed an improved scheme which provides much reduced risk at no significant additional cost. We suggest that our enhanced scheme is suitable for implementation in current wireless communications systems.

References

- [Ahuj96] Vijay Ahuja, *Secure Commerce on the Internet*, Academic Press, 1996.
- [AMS95] Ross Anderson, Harry Manifavas, and Chris Sutherland, "A practical electronic cash system", *Personal Communication*, December 1995.
- [ASPe96] ASPeCT, *Initial Report on Security Requirements*, AC095/ATEA/W21/DS/P/02/B, February 1996.
- [ASPe97] ASPeCT, *Secure billing: evaluation report*, AC095/SAG/W25/DS/P/16/ 1, May 1997.

- [Buha97] K. Buhanal, et al., "IMT-2000: Service Providers' Perspective", *IEEE Personal Communications*, August 1997.
- [GrFe99] Marilyn Greenstein and Todd M Feinman, *Electronic Commerce: Security, Risk Management and Control*, McGraw-Hill, 1999, p. 2.
- [HoPr98] G. Horn and B. Preneel, "Authentication and payment in future mobile systems", *Computer Security - ESORICS'98*, Lecture Notes in Computer Science, 1485, 1998, pp. 277-293.
- [HSW96] Ralf Hauser, Michael Steiner, and Michael Waidner, *Micro-Payments based on iKP*, IBM Zurich Research Lab. Available as <http://www.zurich.ibm.ch/Technology/Security/publications/1996/HSW96.ps.gz>
- [ITU97] ITU, Recommendation ITU-R M.1223, *Evaluation of Security Mechanisms for IMT-2000*, 1997.
- [Lamp81] L. Lamport, "Password authentication with insecure communication", *Communications of the ACM*, 24(11), 770-771, Nov 1981.
- [MaMi98] K.M. Martin and C.J. Mitchell, "Evaluation of authentication protocols for mobile environment value-added services", *Journal of Computer Security*, to appear. Available online from http://isg.rhbnc.ac.uk/cjm/Chris_Mitchell1.htm.
- [Mehr97] A. Mehrota, *GSM System Engineering*, Artech House, 1997.
- [Mite95] C.J. Mitchell, "Security in Future Mobile Networks", *Second International Workshop on Mobile Multi-Media Communications (MoMuC-2)*, Bristol, April 1995. Also available online at <http://isg.rhbnc.ac.uk/cjm/SIFMW.ZIP>.
- [Moha96] Seshadri Mohan, "Privacy and Authentication Protocols for PCS", *IEEE Personal Communications*, October 1996, pp.34-38.
- [MPMH98] K.M. Martin, B. Preneel, C.J. Mitchell, H.J. Hitz, G. Horn, A. Poliakova, and P. Howard, "Secure billing for mobile information services in UMTS", in: S. Trigila, A. Mullery, M. Campolargo, H. Vanderstraeten and M. Mampae (eds.), *Intelligence in Services and Networks: Technology for Ubiquitous Telecom Services* (Proceedings of the Fifth International Conference, IS&N 98, Antwerp, Belgium, May 1998), Springer-Verlag (LNCS 1430), pp.535-548.
- [OjPr98] T. Ojanpera and R. Prasad, "IMT-2000 Applications", in *Wideband CDMA for Third Generation Mobile Communication*, T Ojanpera and R. Prasad (ed.), Artech House, 1998, pp. 65-76.
- [Pede95] T. P. Pedersen, "Electronic payments of small amounts", DAIMI PB-495, Computer Science Department, Aarhus University, August 1995.
- [Redl98] S.M. Redl et al., *GSM and Personal Communications Handbook*, Artech House Publishers, 1998.
- [RiSh96] R. L. Rivest and A Shamir, "PayWord and MicroMint: Two simple micropayment schemes", *Cryptobytes*, Vol. 2, No. 1, May 1996, pp7-11. Available from <http://theory.lcs.mit.edu/~rivest>
- [StVa97] Jacques Stern and Serge Vaudenay, "SVP: a Flexible Micropayment Scheme", *Financial Crypto '97*, pp.161-171, Springer-Verlag, 1997.
- [TAC99] The Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure, *Requirements for Key Recovery Products*, available at <http://csrc.nist.gov/keyrecovery>.
- [Wayn97] Peter Wayner, *Digital Cash: Commerce on the Net*, Academic Press, 2nd Edition, 1997.
- [Wien98] M. Wiener, "Performance Comparison of Public-Key Cryptosystems", *Cryptobytes*, Vol. 1, No. 2, RSA Laboratories, 1998.