Forward-Secure Signatures for Unbounded Time Periods in Mobile Computing Applications

N.R.Sunitha
Department of Computer Science
Siddaganga Institute of Technology
Tumkur, Karnataka ,India

B.B.Amberker
Department of Computer Science
National Institute of Technology
Warangal, Andra Pradesh, India

Prashant Koulgi
Department of Computer Science
Siddaganga Institute of Technology
Tumkur, Karnataka ,India

Summary
Messages transmitted in untrusted mobile environments may be secured by signing them using Digital Signature algorithms. Forward-Secure Digital Signatures enable the signer to guarantee the security of messages signed in the past even if his secret key is exposed today. We present a Forward-Secure like signature scheme with the following features: The verifier Bob can verify messages signed by Alice without himself being able to forge such signatures. If an adversary (may be service provider himself) gains access to either Bob's (verification) key or Alice's (present signing) key, nevertheless he cannot forge Alice's past signatures. When compared to other existing forward-secure schemes, our scheme can be used to sign for unbounded number of time periods with minimum secret key size and signature size.

Keywords
Mobile Computing, Forward Security, Identification Scheme, Blum-William's Integer, Digital Signature.

1. Introduction

The world of mobile computing [1] presents many unique challenges and opportunities for a researcher to provide high level security for mobile computing applications. Security is especially important in mobile computing because wireless transmissions can be sent and received by unknown parties. Also the communication media is accessible to everyone. Thus an unauthorised person can gain access to all information transmitted across mobile devices. The very portability of a mobile device is its greatest vulnerability and the easiest to exploit in terms of security. This has led to extensive consideration of security issues in mobile computing [2,3,4].

One way to provide security is to apply digital signatures on the messages sent. A Digital Signature is an electronic signature that can be used to authenticate the identity of the sender of a message and to ensure that the original content of the message that has been sent is unchanged. Also the sender cannot repudiate the message sent. Digital Signatures are easily transportable, cannot be initiated by someone else and can be automatically time stamped. A digital signature is specified by a key generation algorithm, a signing algorithm and a verifying algorithm. Here *A,* sender of message, will use key generation algorithm to generate a pair of matching public key and secret key, and makes the public key known to the receivers. In order to send a message, the sender will generate a signature on it by signing the message with the secret key using the signing algorithm. This signature is sent to the receiver. The receiver can use the verifying algorithm to confirm that the message is indeed from *A* using the public key. But digital signatures are vulnerable to leakage of secret key. If the secret key is compromised, any message can be forged. To prevent future forgery of signatures, both public key and secret key must be changed. Notice, that this will not protect previously signed messages: such messages will have to be resigned with new pair of public key and secret key, but this is not feasible. Also changing the keys frequently is not a practical solution.

To address the above problem, the notion of forward security for digital signatures was first proposed by Anderson in [5], and carefully formalised by Bellare and Miner in [6] (see also[8,10,11,12]). The basic idea is to extend a standard digital signature scheme with a key updation algorithm so that the secret key can be changed frequently while the public key stays the same. Unlike a standard signature scheme, a forward secure signature scheme has its operation divided into time periods, each of which uses a different secret key to sign a message. The key updation algorithm computes the secret key for the new time period based on the previous one using a one way function. Thus, given the secret key for any time period, it is hard to compute any of the previously used secret keys. (It is important for the signer to delete the old secret key as soon as the new one is generated, since otherwise an adversary breaking the system could easily get hold of these undeleted keys and forge signatures.) Therefore a receiver with a message signed before the period in which the secret key gets compromised, can still

Manuscript received May 5, 2007.
Manuscript revised May 20, 2007.

trust this signature, for it is still hard to any adversary to forge previous signatures.

In this paper we present a Bellare-Miner type signature scheme for a slightly modified adversarial model. Our model corresponds to applications where there is a single verifier, and it is not to this verifier's advantage to itself expose the key used by it for verification. If the verification key gets exposed the verifier will request the signer to revoke all keys. Therefore at any point an adversary can only obtain either the verification key or the signing key of a particular time period, but not both. We guarantee that, if the scheme we present is employed, an adversary in possession of such information will be unable to forge signatures for an earlier time period.

As Mobile Computing applications run in untrusted environments, the above model helps mobile device users to transmit information securely. To send authenticated information to Bob using her mobile device, Alice can sign her messages using the secret keys of our scheme. Bob, who is given the Verifier Key *VK* by Alice, can use this key to verify messages signed by Alice. But Bob cannot forge Alice's signatures. If either the signing key of some time period (which is with Alice) or the verification key (with Bob) is exposed, all keys are revoked. If an adversary (may be the service provider himself) acquires either of these keys, still he will be unable to produce fraudulent messages signed as by Alice for any time period before the time of exposure.

Let us place our scheme in the context of two previous papers [6,9] on forward security. In [9] Malkin, Miccianco and Miner presented a strategy for building a forward secure signature scheme from any standard digital signature scheme given as building block, via the use of certification chains. If the Fiat-Shamir scheme of [7] is used as the building block, this strategy produces secret keys and (forward-secure) signatures in the j^{th} time period of size $2l^2+2lk+lk(\log l+\log t)$ bits each, as against a secret key of size lk bits and signatures of l^2+lk bits in the basic Fiat-Shamir scheme itself (k and l are parameters chosen such that exhaustive search over l-bit strings, and factoring k-bit numbers, are considered infeasible).

The main contribution of Bellare and Miner in [6] is a scheme for signing with forward security based on the Fiat-Shamir of [7], in which (as against as in [9]) the sizes of secret keys and signatures stay the same as in the underlying signature scheme (of [7]).

The scheme of [6] has a fixed lifetime: a parameter T has to be provided as an input to the design procedure, consequent to which the secret key in the scheme designed cannot be updated more than T times while retaining security. On the other hand, in the schemes designed as in [9] (as indicated in the title of that paper) the secret key can be updated an (effectively) unbounded number of times.

In the scheme we present in this paper, we allow the secret key to be updated any number of times, which is as in [9]. And yet, the signature and key sizes stay the same as in the Bellare-Miner scheme of [6].

In section 2 we describe our scheme, in section 3 we compare our scheme with other existing forward-secure signature schemes and in section 4 we discuss the security of our scheme. Lastly in section 5 we conclude.

2. Description of our scheme:

Following are the algorithms used in our scheme: We introduce one change, in the manner of public key generation; and we modify the signing and verification procedures to accommodate this change.

Key generation

The base secret key $SK0 = (S_{1,0}, \ldots, S_{l,0}, N, 0)$ (where $S_{i,0} \xleftarrow{R} Z^*_N$ and N is a Blum-Williams integer). We calculate the key given to the verifier as $PK = (U_1, \ldots, U_l, N)$ with

$$U_i = S^3_{i,0} \bmod N, \; i = 1, \ldots, l \qquad (1)$$

Secret Key Updation

The secret key $SK_j = (S_{1,j}, \ldots, S_{l,j}, N, j)$ of the time period j is obtained from the secret key $SK_{j-1} = (S_{1,j-1}, \ldots, S_{l,j-1}, N, j-1)$ of the previous time period via the update rule

$$S_{i,j} = S^2_{i,j-1} \bmod N, \; i = 1, \ldots, l \qquad (2)$$

It is obvious that now, the base secret key may be updated any number of times without at some point obtaining the verifier's key. Further the secret key in no time period can be computed from knowledge of the verifier's key (for if this were possible then such a secret key and the verifier's key can be combined to derive cube roots of the components of the verifier's key, hence the factorisation of N). As a consequence our scheme can be used to generate signatures for any number of time periods.

Signature Generation

A signature <j, (Y,Z)> in time period j for the message M will be calculated as

$$Y = R^3 \bmod N \qquad (3)$$

where $R \xleftarrow{R} Z^*_N$ and

$$Z = R \prod_{i=1}^{l} S^{ci}_{i,j} \bmod N \quad (4)$$

with $c_1, \ldots, c_l = H(j, Y, M)$ (5)
being the *l* output bits of a public hash function.

Signature Verification

As for verification, a claimed signature <j, (Y,Z)> for the message M in time period j is accepted if

$$Z^3 = Y \prod_{i=1}^{l} U_i^{2^j c_i} \bmod N \quad (6)$$

where $c_1, \ldots, c_l = H(j, Y, M)$, and rejected otherwise. Notice that since

$$Z^3 = R^3 \left(\prod_{i=1}^{l} S_{i,j}^{c_i} \right)^3 \bmod N$$

$$= Y.\left(\prod_{i=1}^{l} S_{i,0}^{2^j c_i} \right)^3 \bmod N$$

$$= Y \prod_{i=1}^{l} U_i^{2^j c_i} \bmod N.$$

a signature by an honest signer with the secret key will be accepted.

3. Comparison with other schemes

Here we compare our scheme with noted forward-secure schemes like MMM scheme and Bellare-Miner Scheme. We have used the Fiat Shamir signature scheme as the underlyimg signature scheme. Following is the observation with respect to secret key size, signature size and life time.

Scheme	Secret Key size	Signature size	Life Time
MMM Scheme	**$2l^2+2lk+lk(\log l + \log t)$**	**l^2+lk**	**Unbounded**
Bellare-Miner Scheme	**lk**	**l^2+lk**	**T**
Our Scheme	**lk**	**l^2+lk**	**Unbounded**

Thus our scheme can be used to sign for unbounded number of time periods with minimum secret key size and signature size.

4. Security of our scheme

Recall that, unlike as in [6], we consider scenarios where the adversary is allowed knowledge (apart from signatures on messages in time periods of its choice) only of either the signing key for some time period *j*, or of the key with the verifier. Establishing the security of our scheme comes to showing that in the former case it cannot forge signatures in any time period. That the former claim is true is the content of the security proof of [6]; we are only left with having to prove the latter claim.

For this, just as in [6] we will show that a polynomial-time adversary who, given the verifier's key (and signatures on messages in time periods of its choice), can forge signatures in some time period, can be used to factor Blum-William's integer, and hence cannot exist. As in [6] our proof breaks into two parts : a proof that the underlying identification scheme, i.e., where the *l* bits $c_1, \ldots, c_l$ are not produced as in (5) by a hash function but are challenge bits provided to the signer (in this context called the prover) by the verifier, is secure; and a check that this security is preserved in the signature scheme where c1, . . . , cl are obtained via a hash function in the manner shown in (5). Lemma 6.1 of [6] applies to the situation we are considering; by this lemma, once it is shown that the underlying identification scheme is secure it will follow that the signature scheme is secure. We are therefore left only with having to prove the security of the identification scheme.

Suppose there is an adversary who, from knowledge of the verifier's key, can purportedly impersonate the signer in some time period k: we will make use of this impersonator to factor the given Blum-William's integer N. For this we choose *l* numbers

$S_{1,0}, S_{2,0}, \ldots, S_{l,0} \xleftarrow{R} Z^*_N$ for the base secret key and calculate the verifier's key $VK = (U_1, \ldots, U_l, N)$ from these as

$U_i = S^3_{i,0} \bmod N, \quad i = 1, \ldots, l.$

V K is exposed to the adversary. Suppose it claims to be able to impersonate the signer in the time period k. We run the adversary on two different challenge vectors $c_1, \ldots, c_l$ and $c'_1, \ldots, c'_l$; let <k, (Y,Z_1)> and <k, (Y,Z_2)> be its corresponding responses. Since these are successful impersonations, from (6) we have

$$Z^3_1 = Y \prod_{i=1}^{l} U^{2^k c_i} \bmod N \quad (7)$$

and

$$Z^3_2 = Y \prod_{i=1}^{l} U^{2^k c_i\,'} \bmod N \quad (8)$$

That is, the adversary has managed to provide us with Z_1 and Z_2 such that

$$Z^3_1 \prod_{i=1}^{l} U_i^{2^k c_i'} = Y \prod_{i=1}^{l} U_i^{2^k c_i} \cdot \prod_{i=1}^{l} U_i^{2^k c_i'} = Z^3_2 \prod_{i=1}^{l} U_i^{2^k c_i} \quad (9)$$

or

$$(Z_1 \prod_{i=1}^{l} S_{i,0}^{2^k c_i'})^3 = (Z_2 \prod_{i=1}^{l} S_{i,0}^{2^k c_i})^3 \quad (10)$$

by substituting for U_i in terms of $S_{i,0}$ (here and subsequently, all computations are assumed to be performed modulo N).Thus the adversary has supplied us with

$Z_2 \prod_{i=1}^{l} S_{i,0}^{2^k c_i'}$ as a cube root $(Z_1 \prod_{i=1}^{l} S_{i,0}^{2^k c_i'})^3$.

Since the former number has three cube roots, the probability that

$$Z_1 \prod_{i=1}^{l} S_{i,0}^{2^k c_i'} \text{ is different } Z_1 \prod_{i=1}^{l} S_{i,0}^{2^k c_i}$$

is 2/3. In this event we obtain the two factors of N as

$$p = \gcd(Z_1 \prod_{i=1}^{l} S_{i,0}^{2^k c_i'} - Z_2 \prod_{i=1}^{l} S_{i,0}^{2^k c_i}, N) \text{ and } q = N/p.$$

5. Conclusion

Forward-Secure Digital Signatures enable the signer to guarantee the security of messages signed in the past even if his secret key is exposed today. Our new forward-secure scheme ensures forward-security and permits to sign for unbounded number of time periods. When compared to other existing forward-secure schemes, our scheme has minimum secret key size and signature size.

Our scheme is built on Fiat-Shamir signature scheme. Further this research work can be continued by building efficient forward-secure schemes based on basic signature schemes like RSA or ElGamal.

References

[1] Martyn Mollik: Mobile and Wireless Design Essentials: Wiley Publishing Inc., USA, First edition 2003.

[2] Borisov et. al., N.: Intercepting Mobile Communications. In: Proc. of Mobicom 2003.

[3] Shiuh-Jeng Wang: Anonymous Wireless Authentication on a Portable Cellular Mobile System, IEEE Transactions on Computers, vol. 53, No.10 (2004).

[4] Rendon,J.: Protecting Phones, Handhelds from Attack, SearchMobileComputing.com, (2004).

[5] Anderson, R.: Invited Lecture, Fourth Annual Conference on Computer and Communications Security, ACM, (1997).

[6] Bellare, M., Miner, S.: A Forward-Secure Digital Signature Scheme. In: Wiener, M. (eds.): Advances in Cryptology-Crypto 99 proceedings, Lecture notes in Computer Science, Vol. 1666. Springer-Verlag, (1999).

[7] Fiat, A., Shamir, A.: How to prove yourself : Practical solutions to Identification and Signature problems. In: Odlyzko, A. (eds.): Advances in Cryptology-Crypto 86 proceedings, Lecture notes in Computer Science, Vol. 263 Springer-Verlag, (1986).

[8] Hans Delfs, Helmut Knebl: Introduction to Cryptography - Principles and Applications, Springer-Verlag, Berlin, Heidelberg, New York (2002)

[9] Malkin Tal, Miccianco Daniele, Miner, S.: Efficient Generic Forward Secure Signatures with an unbounded number of time periods, Proceedings of EuroCrypt 2002, Lecture notes in Computer Science, Vol. 2332 Springer-Verlag, 400-417.

[10] Abdalla,M., Reyzin,L.: A New Forward-Secure Digital Signature Scheme. In: ASIACRYPT 2000, LNCS 1976, pp. 116-129. Springer-Verlag, (2000),116-129.

[11] Krawczyk, H.: Simple forward-secure signatures from any signature scheme. In: Proc. of the 7th ACM Conference on Computer and Communications Security (CCS 2000), ACM, (2000), 108-115.

[12] Itkis, G., Reyzin, L.: Forward-secure signatures with optimal signing and verifying. In:

CRYPTO'01, LNCS 2139, Springer-Verlag, (2001), 332-354.

[13] Kozlov, A, Reyzin, L.: Forward-Secure Signatures with Fast Key Update In: Security in Comm

N.R.Sunitha obtained her M.S. from Birla Institute of Technology, Pilani, Rajasthan, India. She is presently working as Research Scholar and Faculty in the Department of Computer Science & Engineering, Siddaganga Institute of Technology, Tumkur, India.

B.B.Amberker obtained his Ph.D from the Department of Computer Science ¥& Automation, IISc., Bangalore, India. He is presently working as Professor in the Department of Computer Science & Engineering, National Institute of Technology, Warangal India.

Prashant Koulgi obtained his Ph.D from the department of Electrical and Computer Engineering, University of California, Santa Barbara, CA 93106-9560 USA. He is presently working as Visiting Professor and also involved in the Research activities of the Department of Computer Science & Engineering, Siddaganga Institute of Technology, Tumkur, India.