IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

A New Secure Forward Digital Signatures based on Forecasting and Statistical Entropy of Key Exposures

Dr. Faris M. Al-Athari [1], Dr. Abdulameer Khalaf Hussain[2], Dr. Adnan Al-Helali[3]

Department of Mathematics, Faculty of Science, Zarqa University, Al-Zarqa, Jordan[1]

Department of Computer Science, Faculty of IT, Jerash University, Jerash , Jordan[2]

Department of Computer Science, Faculty of IT, Isara University, Amman, Jordan[3]

Abstract: A new method of forward digital signatures is proposed in this paper. All of the previous forward digital signatures depend on changing the private key periodically but they keep the public key. The proposed system will change both private keys and public keys that can be generated only by authorized users to enhance the authenticity of users. Another important proposal is that the expiration of that public key depends on the length of the document so the sender must compute the expired time of his/her document depending on its length. This method also can be used to change the private key depending on the expired date of the document but the public key is still fixed. In order to make this digital signature more efficient, the system must change the private keys in terms of their critical times that indicate the period of exposure of the keys by different attacks types. So the ability to change these keys do not depend on fixed periods as in most forward digital signatures but also depend on these critical times and the entropy of the information of the keys.

Keywords: Forward Digital Signature, Entropy, K-nearest Algorithm, Agreement.

I. INTRODUCTION

The concept of the forward security for all digital signatures is introduced to deal with an important problem which is the key exposure. To enhance digital signature the forward concept divides the whole time into discrete time periods. In the forward digital signatures, different secret keys are used to sign the messages in different time periods, while the public key is unchanged during the whole lifetime. The first forward signature was proposed by Anderson [1] . Then it formalized by Bellare and Miner [2]. Bellare and Miner also gave the definition of forward-secure signature scheme and its security. After these efforts, some of forward secure signatures schemes [3, 4, 5,6] were proposed. These last schemes had different trade-offs among key size, signing time and update time. These schemes in [5] had the ability to provide optimal signing and verifying algorithms at the expense of slower key update. Another scheme [6] could achieve fast key update but had slower signing and verifying algorithms. Malkin et al. [7] proposed generic forward-secure signatures with an unbounded number of time periods. Another construction which is Hierarchical ID-based cryptography could be used to build forward-secure signature schemes. Based on the hierarchical ID-based cryptography [8], some forward- secure signature scheme using bilinear maps were proposed in [9, 10, and 11]. Some proposals such as of Boyen et al. presented a forward- secure signature with untrusted update [12] in which the secret key is additionally protected by an extra secret that is possibly derived from a password and key update procedure can be completed by the encrypted version of signing key. Libert et al. [13] gave generic constructions of forward-secure signatures in untrusted update environments.

Forward-secure symmetric-key encryption was studied in [14] and forward-secure public key encryption was also studied in [15]. Forward-secure threshold signatures were researched in [16, 17, 18, 19]. Key-insulation [20, 12, 22, 23] and intrusion-resilient cryptography [24, 25, 26 27] can achieve a higher level of security than forward-secure cryptography. However, these methods were not able to apply to many scenarios.

Key-insulated signature schemes [24, 25] and intrusion-resilient signature schemes [26, 27] can achieve a higher level of security. However, one weakness of these schemes is that they require an additional device to communicate with signer, which makes them unable to be applied to many scenarios. Boyen et al. introduced the concept of forward-secure signature with untrusted up-date and proposed the first concrete scheme in [28]. In their scheme, the signing key is additionally protected by a second factor. The second factor in practice is a password provided by the user, which is used to encrypt the signing key. Key update procedure can be completed by the encrypted version of signing key; therefore, the password only comes into play for signing messages. They also left open the problem of adding untruted update to other existing forward-secure signature schemes. Subsequently, Libert et al. [29] gave generic constructions of forward-secure signatures in untrusted update environments by expanding MMM construction [30]. However, their method is not for designing a concrete scheme and has

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

great limitations because it needs two signatures and has a lot of additional expenses during setup and key generation. Therefore, how to construct more efficient concrete forward-secure signature schemes with untrusted update is worth researching.

Shannon entropy (p):=-$\sum p_i \lg p_i$, is often considered as a measure of the number of bits of uncertainty associated with a source which produces symbol i with probability p_i , where Ig=$\log_2$. This use, which began with Shannon's work on Information Theory, has become widespread in cryptology where it is often used outside it s original context. For example, suppose the symbol i is a key for some cipher and is chosen with distribution p_i . Key guessing attacks are discussed in [31].

We can measure how bad a key distribution is by calculating its entropy. This number E is the number of real bits of information of the key: a cryptanalyst will typically happen across the key with in 2^E guesses. E is defined as the sum of -$\sum p_K \log_2 p_K$, where p_K is the probability of key K.

II. RELATED WORKS

In [32], a new scheme was proposed which studied the continuously changing of private keys and showed that the attacker could not fake the older signature even if the private key is leaked out in some period of time. In this way this scheme makes sure of the security of signature of former phases. The validity of the new scheme is proved and the security is analysed in this paper.

A paper in [33] the authors proposed a technique to enhance the security of forward digital signature. In this enhancement scheme the private key and the public key changes at random intervals of time, if there is a communication between two users and if there is no communication then the keys will not be changed. By using this enhancement scheme the attacker cannot get the older or future signatures even if the private key is compromised. This scheme is more secure and it is proved practically.

Due to forward-secure-digital-signature's capability of effectively reducing loss caused by exposure of secret keys and significant in-application benefits of blind signature aiming at protecting senders' privacy, they have been hot spots for decades in the field of cryptography. In [34] the authors proposed an integration of forward secure digital signature and blind signature to resist forging attack.

Another paper showed some insecurity in Xu's forward secure multi-proxy signature scheme. There are two kinds of attacks on this scheme:

(1) anyone can forge some certain messages which to be sign and cannot detect by the signature verifier. (2) This scheme can't resist the dishonest signer forgery attack by forging its own public key. After that, the paper proposed two new forward-secure multi-proxy signature schemes based on discrete logarithm problem and quadratic residues. [35].

In most forward-secure signature constructions, a program that updates a user's private signing key must have full access to the private key. Unfortunately, these schemes are incompatible with several security architectures including where the private key is encrypted under a user password as a "second factor" of security, in case the private key storage is corrupted, but the password is not. The authors in [36] introduced the concept of forward-secure signatures with untrusted update, where the key update can be performed on an encrypted version of the key.

III.PROPOSED SYSTEM

In this system, we design a strong forward digital signature (FDS) that changes both the private keys (Ds) and public keys (Es). The private key will be changed according to a critical time (CT) which indicates the amount of period before espousing the key. The public key will be changed depending on two parameters: the length of the message sent (L) and the amount of information included within that message, i.e. entropy (H(x)) of this message. For this reason, the messages are sent with variable lengths.

To demonstrate the digital signature, the sender must send the message (M_1) to the receiver by encrypting the M_1 with length (L_1) by his/her private key (D_1) for the first time (T_1). So the structure of the first forward digital signature will be as follows:

$FDS_1=M_1^{D1} \bmod n \parallel L_1 \| T_1$, where n is the product of two large prime numbers p and q (n=p*q). Suppose that the forecasting or critical time for this message will be CT_1 , so the next forward digital signature will be in time of $T_2= T_1+CT_1$ and the sender must extract another private key by choosing the next two neighbours of previous p and q to be p_1 and q_1 and compute the next private key as following :

$$\Theta (n)=(p_1-1)(q_2-1)$$
$$D_2= E^{-1} \bmod \Theta (n)$$

The sender now encrypts the next variable length message (M_2) as follows:

$$FDS_2=M_2^{D2} \bmod n \parallel L_2 \| T_2$$

To change the public key (E) we must know the length (L) of the sent message or the ciphertext which represents the $Mi^{Di} \bmod n$ in each FDSi and the amount of information of that piece of FDS_i which represents the entropy ($H(x_i)$). So the new public key will take the decision gained from these two parameters and the receiver can choose the nearest one in the pool of available public keys.

In order to choose a new public key from a pool of public keys, we use the proper distance (d) from the old public key by using the K-nearest neighbour one. The pool of public keys is represented by the figure 1 with 3 alternative public key.

So K-nearest=Agreement (d_i) , where the distance d_i will be chosen according to an agreement among all authorized users rather than it is calculated according to the traditional k-nearest neighbour algorithm because agreement will provide more security.

DOI 10.17148/IJARCCE.2016.51119

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

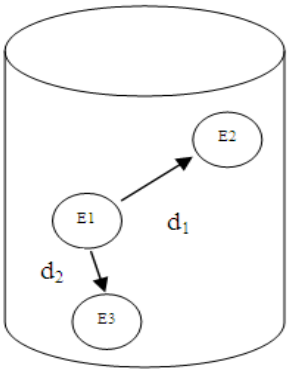

Fig.1. A Pool of Nearest Subsequent Public Keys.

Algorithm

Let D be the set of subsequent private keys; $D=\{d_1,d_2,\ldots\ldots,d_n\}$.

Let E be the pool of public keys associated with private keys.

Let FDS_i be the significant forward digital signature.

Let L_i be the length of message Mi

Let T_i be the time of each stage of changing the private key D_i

Let CT_i is the critical time needed to change the subsequent private keys

Let $H(x_i)$ be the entropy of message M_i

Sender Operation	Receiver Operation
Choose two large prime numbers p and q. Compute n=p*q Compute φ (n)=(p-1)(q-1) for i=1 to m $FDS_i = M_i^{Di} \bmod n \,\|\| L_i \| CT_i$ $CT_i+1=T_i+CT_i$	for j=1 to k E_i=K-nearest $(E_i \| L_i \| H(x_i))$

IV. RESULTS

Table 1 illustrates some of the results of this proposed system.

TABLE 1: Initial Information of Private and Public Keys

M (With Binary Representation and the Length of the message)	p	q	n	φ(n)	Public key	Private Key
120=1111000 L=3	3	11	3*11= 33	2 * 10 = 20	7	3
14530=11100011000010 L=5	7	13	7*13=91	6*12=72	5	29
1317226=10100000110010 1101010 L=9	5	11	5*11=55	4*10=40	27	37
6965774489=11001111100 11000101001000100110001 L=16	5	11	5*11=55	4*10=40	3	7
5978238=10110110011100 00111110 L=6	29	31	29*31=899	28*30=840	11	611

The next step is to calculate the nearest public keys for each item in table 1. In order to perform this task we must provide information about each message. In the binary representation of each message we take the number of one's and the number of zero's to include them as a part of calculation of the entropy contained in each message.

The new public key (Enew) is calculated as follows:

For simplicity suppose the numbers of one's is O ,the numbers of zero's is Z and the total binary numbers is T.

$$Enew = Eold + L + h(x)$$

Where Eold is the previous public key , L is the length of the message and h(x) is the entropy which is calculated as follows ;

h (x)=-(O *Round (log2 probability of O)+Z*(Round (log2 probability of Z)). According to these equations and the elements of table 1, the following calculations are illustrated as follows:

For m=120, L=3, the binary representation is 1111000, and number of one's is 4 so the first new public key ($E1_{new}$) is:

$$E1_{new}=E1_{old}+L+h(x)$$
$$= 7+3- (4\log_2 4/7+3\log2\ 3/7)$$
$$=10-(-7)=17$$

Then we check this new public key if it satisfies the public keys conditions which it must be between 1 and φ(n) and the greatest common divisor (GCD) of the new public key and φ(n) is 1 . In this case 17 satisfies the first condition in that (1<18<20), and the GCD (17, 20) is 1 so we take it as a new public key . if the GCD of the public key is not 1 so we choose the nearest public key in either the left side or the right side of that new public key.

After choosing the new public key , the new private key from this public key must be calculated according the function which states that the private key is the inverse of public key and φ(n) ; d= inv(E, φ(n). In this case d=inv (17,20)=13. So we get both a new public key (17) and a new private key d=13. We can apply the above steps to get the other public and private keys for each elements of table 1 as shown in table 2.

TABLE 2: Generation of New Public and Private Keys

Old public keys	No.of one's in the message	φ(n)	Length (L)	Round(H(x))= -(Olog2O/T+Zlog2Z/T)	The new public key	Nearest Public key= GCD(e, φ(n)=1)	The new Private keys
7	4	20	3	$-(4\log_2 4/7+3\log_2 3/7 \approx -7)=7$	7+3+7= 17	17	13
5	6	72	5	$-(6\log 24/14+8\log 211/4) \approx -(-3)=13$	5+5+13= 23	23	5
27	9	40	7	$-(9\log_2 9/21+12\log_2 12/21) \approx -(-20)=20$	27+7+20= 34	37	13
3	16	40	10	$-(16\log_2 16/33+17\log_2 17/33) \approx -(-32)=32$	3+10+32=45	47	23
11	13	40	7	$-(13\log_2 13/22+9\log_2 9/22) \approx -(-40)=40$	11+7+40=58	59	19

The new date of using the next private keys is calculated as the length of the message plus the number of zero's in the binary representation of each message. Note : we can use other parameters to calculate the next private keys depending on the agreement of participants in the communication. So if we suppose the first date of using the initial private key is 22 March 2015 so the next dates of each of the above private keys listed in table 2 is illustrated in table 3:Note: for initial date the period is zero.

The length and number of zero's in each element can be used to calculate the date of using the next date of that element.

DOI 10.17148/IJARCCE.2016.51119

Table 3 illustrates the complete results of how to get the periods of using the subsequent private keys.

TABLE 3: Periods of Subsequent Private keys

L	No.of zeros	Period	Next date
3	3	3+3=6	28 March 2015
5	8	5+8=13	6 April 2015
7	12	7+12=19	25 April 2015
10	17	10+17=27	22 May 2015

V. CONCLUSION

This proposed system enhances the security of forward digital signatures. First enhancement is that in addition to change the private keys to prevent against different attacks, this system also changes the public keys at the receiver side. Secondly, the procedure of changing the private keys do not depend on fixed periods but the changing depends on different secure parameters. The generation of public keys depends on two secure factors. First factor is the k-nearest of each public key relative to the next one stored in a secure pool of public keys. The second secure factor is that the agreement among participants about the distance that separates different public keys. So this procedure shows the first modification to the traditional forward digital signatures. The second modification is that the calculation of new public keys depends on different factors such as the length of the message and the amount of information included in each message. If the new public keys satisfies the conditions of correct public keys then it is accepted , otherwise the public key is generated using the k-nearest neighbour either left or right sides of the new calculated public keys. Finally, the periods of changing the private keys are not fixed and they depend on different secure parameters related to the properties of each message.

REFERENCES

[1] R. Anderson, "Two remarks on public key cryptology," Invited Lecture, In: the 4th ACM Conference on Computer and Communications Security, 1997.
[2] M. Bellare, S. Miner, "A forward-secure digital signature scheme," In: Wiener, M.J. (ed.) Advances in Cryptology-CRYPTO'99. LNCS, vol. 1666, pp. 431–448. Springer, Heidelberg, 1999.
[3] M. Abdalla, L. Reyzin, "A new forward-secure digital signature scheme," In: Okamoto, T. (ed.) Advances in Cryptology-ASIACRYPT 2000. LNCS, vol. 1976, pp. 116-129. Springer, Heidelberg, 2000.
[4] H. Krawczyk, "Simple forward-secure signatures for any signature scheme," In: the 7th ACM Conference on Computer and Communications Security. pp. 108-115. ACM Press, New York, 2000.
[5] G. Itkis, L. Reyzin, "Forward-secure signatures with optimal signing and verifying," In: Kilian, J. (ed.) Advances in Cryptology-CRYPTO 2001. LNCS, vol. 2139, pp. 499–514. Springer, Heidelberg, 2001.
[6] A. Kozlov, L. Reyzin, "Forward-secure signatures with fast key update," In: Cimato, S., Galdi, C., Persiano, G. (Eds.) the Proc of security in communication Networks. LNCS, vol. 2576, pp. 247-262. Springer, Heidelberg, 2002.
[7] T. Maklin, D. Micciancio, S. Miner, "Efficient generic forward-secure signatures with an unbounded number of time periods," In: Knudsen, L. (ed.) Advances in Cryptology-EUROCRYPT 2002. LNCS, vol. 2332, pp. 400-417. Springer, Heidelberg, 2002.
[8] C. Gentry, A. Silverberg, "Hierarchical ID-based cryptography," In: Zheng, Y. (ed.) Advances in Cryptology-Asiacrypt 2002. LNCS, vol. 2501, pp. 548- 566. Springer, Heidelberg, 2002.
[9] F. Hu, C. H. Wu, J. D. Irwin, "A new forward-secure signature scheme using bilinear maps," Cryptology ePrint Archive, Report 2003/188, 2003.
[10] B.G. Kang, J. H. Park, S.G. Halm, "A new forward-secure signature scheme," Cryptology ePrint Archive, Report 2004/183, 2004.
[11] J. Yu, F. Y. Kong, X. G. Cheng, R. Hao, G. W. Li, "Construction of Yet Another Forward-secure Signature Scheme Using Bilinear Maps," In: the second international conference on provable security (ProvSec 2008). LNCS, vol. 5324, pp. 83-97. Springer, Heidelberg, 2008.
[12] X. Boyen, H. Shacham, E. Shen, B. Waters, "Forward- secure Signatures with Untrusted Update," In: the 13th ACM conference on Computer and communications security. pp. 191-200. ACM Press, New York, 2006.
[13] B. Libert, J. Jacques, M. Yung, "Forward-Secure Signatures in Untrusted Update Environments: Efficient and Generic Constructions," In: the 14th ACM conference on Computer and communications security. pp. 266-275. ACM Press, New York, 2007.
[14] M. Bellare, B. Yee, "Forward-security in private-key cryptography," In: Joye, M. (Ed.) Topics in Cryptology-CT-RSA 2003. LNCS, vol. 2 612, pp. 1-18. Springer, Heidelberg, 2003.
[15] R. Canetti, S. Halevi, J. Katz, "A forward-secure public-key encryption scheme," In: Biham, E. (ed.) Advances in Cryptology-EUROCRYPT 2003. LNCS, vol. 2656, pp. 255-271. Springer, Heidelberg, 2003.
[16] M. Abdalla, S. Miner, C. Namprempre, "Forward-secure threshold signature schemes," In: Naccache, D. (ed.) Topics in Cryptology–CT-RSA 2001. LNCS, vol. 2020, pp. 441-456. Springer, Heidelberg, 2001.
[17] Z. J. Tzeng, W.G. Tzeng, "Robust forward signature schemes with proactive security," In: Kim, K. (ed.) Public-Key Cryptography (PKC 2001). LNCS, vol. 1992, pp. 264- 276. Springer, Heidelberg, 2001.
[18] H. Wang, G. Qiu, D. Feng, G. Xiao, "Cryptanalysis of Tzeng-Tzeng Forward-Secure Signature Schemes," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences E89-A(3), 822-825, 2006.
[19] J. Yu, F. Y. Kong, R. Hao, "Forward-secure Threshold Signature Scheme from Bilinear Pairings," In: Wang, Y., Cheung, Y., Liu, H. (Eds.) the Second International Conference on Computational Intelligence and Security. LNAI, vol. 4456, pp. 587-597. Springer, Heidelberg, 2007.
[20] Y. Dodis, J. Katz, S. Xu, M. Yung, "Key-insulated public key cryptosystems," In: Knuds en, L. (ed.) Advances in Cryptology-Eurocrypt 2002. LNCS, vol. 2332, pp. 65-82. Springer, Heidelberg, 2002.
[21] Y. Dodis, J. Katz, S. Xu, M. Yung, "Strong key-insulated signature scheme," In: Desmed t, Y. (ed.) Advances in Public key Cryptography-PKC 2003. LNCS, vol. 2567, pp. 130-144. Springer, Heidelberg, 2003.
[22] Y. Zhou, Z. Cao, Z. Chai, "Identity Based Key Insulated Signature," In: Chen, K., Deng, R., Lai, X., Zhou, J. (Eds.) the Second International Conference Information Security Practice and Experience (ISPEC 2006). LNCS, vol. 3903, pp. 226-234. Springer, Heidelberg, 2006.
[23] B. Libert, J. Quisquater, M. Yung, "Parallel Key-Insulated Public Key Encryption Without Random Oracles," In: Okamoto, T., Wang, X. (Eds.) Advances in Public Key Cryptography–PKC 2007. LNCS, vol. 4450, pp. 298-314. Springer, Heidelberg, 2007.
[24] Y. Dodis, J. Katz, S. Xu, and M. Yung, "Strong key-insulated signature scheme," in Proceedings of the Public-Key Cryptography , 2003, pp. 130-144.
[25] J. Weng, X. X. Li, K. F. Chen, and S. L. Liu, "Identity-based parallel key-insulated signature without random oracles," Journal of Information Science and Engineering Vol. 24, 2008, pp. 1143-1157.
[26] G. Itkis and L. Reyzin, "SiBIR: Signer-base intrusion-resilient signatures," in Proceedings of Cryptology – Crypto, 2002, pp. 499-514.
[27] Z. Gong, X. X. Li, D. Zheng, and K. F. Chen, "A generic construction for intrusion- resilient signatures from linear feedback shift register," Journal of Information Science and Engineering , Vol. 24, 2008, pp. 1347-1360.
[28] X. Boyen, H. Shacham, E. Shen, and B. Waters, "Forward-secure signatures with untrusted update," in Proceedings of the 13th

ACM Conference on Computer and Communications Security , 2006, pp. 191-200.
[29] B. Libert, J. Quisquater, and M. Yung, "Forward-secure signatures in untrusted up- date environments: efficient and generic constructions," in Proceedings of the 14th ACM Conference on Computer and Communications Security, 2007, pp. 266-275.
[30] T. Malkin, D. Micciancio, and S. Miner, "Efficient generic forward-secure signatures with an unbounded number of time periods," in Proceedings of Cryptology −Eurocrypt, 2002, pp. 400-417.
[31] Various .sci.crypt cryptography faq.sci.crypt.
[32] J. Hong ,"A New Forward-Secure Digital Signature Scheme , Anti-counterfeiting, Security, Identification", 2007 IEEE International Workshop on 2007.
[33] M .Rajasekhar, I.M.V.Krishna, and M.Samuel John , Security Enhancement of Forward Digital Signatures Using ECC, International Journal on Computer Science and Engineering 2010.
[34] Y. LIU , X. QIN and B. LI , " Forward-Secure Blind Signature Schemes Based on the Variants of ElGamal", China Communications » 2010, Vol. 7 Issue (4): 58-64 .
[35] Z.Jun ," Improvement of a Forward-Secure Multi-Proxy Signature Scheme ", Journal of Networks, Vol 6, No 9 (2011), 1272-1279, Sep 2011.
[36] B .Xavier , S.Hovav, S.Emily ,and W. Brent "Forward-Secure Signatures with Untrusted Update , Full version of an extended abstract published in Proceedings of ACM CCS 2006, ACM Press, 2006.

BIOGRAPHIES

Dr. Faris M. Al-Athari, is a professor of Mathematical Statistics and is currently working as professor in the college of science at Zarqa University, Jordan. He earned his PhD. from Wyoming University, USA, in 1983 and his master degree from North Carolina State University, USA in 1979. He taught at Baghdad University from October 1983 to September 1999, the Hashemite University, Jordan from October 1999 to September 2009 and joined Zarqa University in September 2009 up to date. He has published more than 40 papers in peer-reviewed articles. His teaching and research interests include the mathematical statistics, Regression and Linear Models, and Stochastic Processes; He got the prize of the best researcher in Zarqa University, Jordan.

Dr. Abdulameer K. Husain, Jerash University- Jordan. He has completed Master degree in computer science, university of Sadam, Iraq, in 1991 and his PhD in computer science, computer security from Al-Neelain University, Sudan. He has total 20 years teaching experience and presently working as Associate professor in Jerash University –Jordan. He has a prize of the best scientific book.

.

DOI 10.17148/IJARCCE.2016.51119