tures “, H. Alexander ,A. Robert and Z. Tanja, Anonymous Submission to ACM MIST 2017, Due 4 August 2017, Dallas, Texas2017. ACM ISBN 978 .

[9] “FIPS PUB 186]: Digital Signature Standard (DSS), 1994-05-19”.csrc.nist.gov.

[10] “FIPS PUB 186-1: Digital Signature Standard (DSS), 1998-12-15” (PDF).csrc.nist.gov. Archived from the original (PDF) on 2013-12-26.

[11] “FIPS PUB 186-2: Digital Signature Standard (DSS), 2000-01-27” (PDF).csrc.nist.gov.

[12] “FIPS PUB 186-3: Digital Signature Standard (DSS), June 2009”(PDF). csrc.nist.gov.

[13] “FIPS PUB 186-4: Digital Signature Standard (DSS), July 2013”(PDF). csrc.nist.gov.

[14] W. David W. Kravitz Archived January 9, 2013, at the Wayback Machine.

[15] Werner Koch. “DSA and patents”

[16] “Wayback Machine”. 26 August 2009.

[17] S. Saumya and A. Himanshu” Digital Signature Combined with Subliminal Channel and its Variants “ , International Journal of New Technology and Research (IJNTR) ISSN:2454-4116, Volume-3, Issue-6, June 2017 Pages 09-19.

[18] J.Jason and K.Ridha, “Exploring Covert Channels “ , System Sciences (HICSS), 2011 44th Hawaii International Conference on ,2011.

[19] H. Loïc and R. Aline , “ On the differences between Covert Channels and Interferences” , Workshop on Games , Logic and Security , 2010.

[20] W. Jingzheng , W. Yongji , D. Liping and L. Xiaofeng , “ Improving performance of network covert timing channel through Huffman coding” , Mathematical and Computer Modeling Volume 55 , Issues 1-2, January 2012, Pages 69-79.

[21] Dai-Rui Lin , Chih-I Wang, Zhi-Kai Zhang and D.J. Guan , “ A digital signature with multiple subliminal channels and itsapplications “ , Computers and Mathematics with Applications 60 (2010) 276284 .

- Compute u1≡ ht mod q= 53.8 mod 23= 424 mod 23 = 10
- Compute u2 r≡t mod q = 12.8 mod 23= 96 mod 23 = 4
- Compute v=($g^{u1}y^{u2}$ mod p) mod q= (266^{10}*2100^{4} mod 2347) mod 23= 12
- Since v=r , so it is accepted that the message was signed by the user, associated with the public key y.

CONCLUSION

The proposed system modifies the original DSA subliminal channel to enhance the security of the algorithm and increase the hidden layer of the subliminal . By appending a salt to the original message , the new system provides more diffusion to the message and then we can get a more secure to the message . Also , the proposed system agrees on a secure hidden piece of information . This agreement factor is inserted in the message signature which is agreed securely and without transferring through the network . So , these two modifications , adding salting and agreement factor , are considered important suggestions to provide a more powerful subliminal channel.

REFRENCES

[1] G.J. Simmons, The prisoner's channel and the subliminal channel", in Advances in Cryptology, Crypto' 83, pp.51-67, Plenum Press, New York and London, 1984.

[2] G.J. Simmons, "The history of subliminal channels", IEEE Jour. on sel. Areas Comm., Vol.16, No.4, pp.452-462, 1998.

[3] G.J. Simmons, "A secure subliminal channel", in Advances in Cryptology, Crypto' 85, LNCS 218,pp.33-41, Springer-Verlag, 1985.

[4] G.J. Simmons, "Subliminal communication is easy using the DSA", in Proc. EUROCYPT 93, LNCS 765, pp.218-232, Springer-Verlag, 1993 .

[5] J.K. Jan and Y.M. Tseng, "New digital signature with subliminal channels based on the discrete logarithm problem", ICPP Workshop 1999, pp.198-203.

[6] G J Simmons. The subliminal channel and digital signatures. In Proc.of the EUROCRYPT 84 workshop on Advances in cryptology: the-ory and application of cryptographic techniques, pages 364{378, New York, NY, USA, 1985. Springer-Verlag New York, Inc.

[7] K. Timo , " Subliminal Channels in Cryptographic Systems " , Seminar Topic: Covert Channels and Embedded Forensics , 2009.

[8] "A Subliminal Channel in EdDSA: Information Leakage with High-Speed Signa-

- Publish the triple (p,q,g)

2. Key Generation

- Choose the authentication key x = 1468, so that the verification key y can be computed as follows :

$y \equiv g^x \bmod p = 266^{1468} \bmod 2347 = 2100.$

- Publish the of y.

3:Sigining

- The message m is 1337 and as hash function we chose for simplicity a modulo reduction by 107.
- Concatenate m with salting ss=3 to get M=1337||3
- The hash of M is computed $h \equiv 13373 \bmod 107 = 105$
- Choose randomly a session key k= 17 and compute inverse of k , which is k^{-1} as $kk^{-1} \bmod q=1$. So from this rule we get $k^{-1}= 19$.
- Compute $r \equiv (g^k \bmod p) \bmod q = (266^{17} \bmod 2347) \bmod 23 = 12$
- Compute the signature $s \equiv k^{-1} (h+xr) \bmod q = 19(53+1468.12) \bmod 23=3$
- Concatenate s with agreement factor =5 to get S=s||ag=3||5
- Send the triple structure (M=13373 , r=12,S =35)

4: Verification

- At the sender , he/she receives triple structure (M=13373 , r=12,S =35)
- Extract M and S to get m=1337 and s=3
- He/she also compute $h \equiv 1337 \bmod 107 = 53$
- Compute s^{-1} from $ss^{-1} \bmod q = 3.8 \bmod 23 = 24 \bmod 23=1$, so $s^{-1}=8$
- Compute $t \equiv s^{-1} \bmod q = 8 \bmod 23 = 8$

- Let h be a hash function and module f
- Compute h= M mod f
- Choose randomly a session key k such that there is an inverse to k , k^{-1} such that k^{k-1} mod p=1
- Compute r≡(g^k mod p) mod q
- Compute the signature s≡k^{-1}(h+xr) mod q
- Choose an agreement factor , ag
- S=s||ag
- Send the triple (M,r,S)

4: Verifying

- After receiving the triple (M,r,S) do the following :
- ✓ Extract ss from M to get m only
- ✓ Extract ag from SS to get s
- Compute again h= m mod ff
- Compute t=s^{-1} mod q
- Compute u1=ht mod q
- Compute u2= rt mod q
- Compute v= ($g^{u1}y^{u2}$ mod p) mod q
- If v=r so the message is accepted as one is signed by the user , accompanied with the public key y

RESULTS

1: Setup

- Let p = 2347, q = 23 and the an element z = 1979.
- Computing g≡$z^{(p-1)/q}$ mod p = $1979^{(2347-1)/23}$ mod 2347 = 266

steps . The original DSA algorithm (broad channel) establishes a subliminal channel between sender and receiver by sharing an authentication key , x . One party has the ability to use and calculate k= m' which is considered as a subliminal channel (where m represents the message) . So for this reason it is not possible to recover m' unless one knows the value of x , or he/she can detect that information that the subliminal channel is being used , even if the enemy has any knowledge of the subliminal message.

In the side of sender , he/she can substitute the value of k by m' and calculate r as before $r \equiv (g^{m'} \bmod p) \bmod q$ and $s \equiv m r^{-1} (h+xr) \bmod q$ .The inverse of m' exists , this is because the modulus is prime and any non-zero element of GF*(q) has a multiplicative inverse . If the receiver knows x , then he/she can compute m' by :

$$m' \equiv s^{-1} (h+xr) \bmod q$$

The first modification is to salt (ss) wih the selected message m . This needs to compute the length of the original message (lm) in order o be extracted in the receiver side. The second modification is add an agreement factor (ag) in the signing step especially when we compute the value of the signature s.

Following the modified algorithm of subliminal channel using DSA :

1: Set-Up

- Select two prime numbers p and q .
- Select an element z
- Compute the generator $g \equiv z^{(p-1)/q} \bmod p$
- Publish (p,q,g)

2: Key Generation

- Choose an authentication key , x so that , the verification key , $y \equiv g^x \bmod p$
- Publish y

3: Signing

- Choose a message m
- Choose a secure salting ss to m
- M=m||ss

ogy (NIST) proposed DSA for use in their Digital Signature Standard(DSS) and adopted it as FIPS 186 in 1993 [9]. Four revisions to the initial specification have been released: FIPS 186-1 in 1996, [10], FIPS 186-2 in 2000,[11] FIPS 186-3 in 2009, [12] and FIPS 186-4 in 2013[13] .

DSA is covered by U.S Patent 5,231,668, filed July 26, 1991 and attributed to David W. Kravitz, [14] a former NSA employee. This patent was given to "The United States of America as represented by the Secretary of Commerce, Washington, D.C.", and NIST has made this patent available worldwide royalty –free . ClausP. Schnorr claims that his U.S patent 4,995,082 (expired) covered DSA; this claim is disputed [16] DSA is a variant of the ElGamal signature scheme.

RELATED WORK

In [17] , a discussion of subliminal channel with two digital signature schemes constructed on discrete logarithms and threshold subliminal channel where message can be recovered with the help of t users among the authorized user .

A model is proposal to understand the communication of subliminal channel . The proposed model is used effectively to scout the relationship among covert channels, steganography and watermarking.The objective is providing a best realization of subliminal channel communication in an attempt to develop investigative support for confidentiality [18].

In [19] a discussion is made to see how covertchannels can be seen as games, where a pair of players u, vwins against the system if it succeeds to maximizing the average of covert information sent from a player , u to a player , v in infinite numbers of runs. The problem of finding out the best possible strategy (i.e. the strategy that maximizes the outflow of information) is still an open matter in the field of numerical communications.

A paper presented the of Huffman coding method in order to make a compression of the transmitted data . This is done by taking the advantage of redundancy and exploring the performance of network timing channel depending on two factors , the channel capacity and covertness .This paper made experiment to check how the network delays and the Huffman coding scheme affect the capacity and covertness [20].

In [21] we find a paper presented two methods to embed multiple subliminal messages into one-time signature schemes (OTSSs) proposed by Lamport in 1971. This scheme can provide more than one independent subliminal message and also the numbers of subliminal messages and receivers are larger than that of the subliminal messages in previous schemes.

PROPOSED SYSTEM

In order to enhance the security of subliminal channel , this system proposes more than one modification . The original algorithm includes four steps , set up step , key generation step , signing step and verifying step . The medications will be in signing and verifying

the signer›s secret key but the length of the digital signature generated in their proposed schemes is too long . Also Jan and Tseng had proposed another two new digital signature schemes with subliminal channels [5].

A prisoner problem is an important example to explain the idea of subliminal channel in cryptography . Before the prisoners are arrested , they agree on a certain schemes in such a way that the warden has no knowledge about this agreement. The two prisoners want to exchange information and communicate and the only way is the warden. The prisoners must not use the encryption because the warden wants to read all communication or he will not deliver the message. They decide to sign the outcome of a fair-coin toss and use the signature of the authentication system to hide their communication. The warden accepts the use of an authentication system, but insists on an encoding rule . related to the outcome, such that he/she can verify the signature.

For simplicity a three bit message is used and the warden only accepts an even parity message when head is the outcome of the coin toss and at tail an odd parity message. The eight (23 = 8) possible messages are now sorted into two unique sets. Both sets contain two even and two odd parity messages, e.g., s1 = {000,101,010,111} and s2= {110,011,100,001}. With these sets the following eight keys can be constructed (details follows) [7].

	Head		Tail	
Key	S_1	S_2	S_1	S_2
1.	000	011	111	100
2.	000	011	010	001
3.	000	110	010	100
4.	000	110	111	001
5.	101	110	111	100
6.	101	100	010	001
7.	101	011	010	100
8.	101	011	111	001

When using subliminal channel in digital signature , it provides an effective way to securely leakage of information from inside a system to a third party outside. Information can be hidden in signature parameters in a way that both, network operators and legitimate receivers, would not notice any suspicious traces [8].

The Digital Signature Algorithm (DSA) is a Fedral Information Processing standard for digital signatures. In August 1991 the National Institute of Standards and Technol-

ABSTRACT

This paper presents a modified method to DSA subliminal channel. The proposed system intends to add more hidden layers to the original subliminal channel. The first modification is to insert a secure salting which is a piece of information to provide confusion to the system. The salting is appended to the message before the signing procedure of DSA algorithm. The second modification provides more hidden and secure layer especially for the signature of the message.

الملخص

تقدم هذه الورقة البحثية طريقة محورة لقناة الاخفاء دي أس اي . يهدف النظام المقترح الى اضافة طبقات اخفاء الى قناة الاخفاء الاصلية . يشمل التحوير الاول حشر معلومة سرية تسمى التمليح حيث توفر خلط لمعلومات النظام . يضاف التمليح في اخر الرسالة قبل عملية التوقيع في خوارزمية دي أس أي . يوفر التحوير الثاني طبقة اكثر اخفاءا وسرية وخاصة في توقيع الرسالة.

Keywords : Subliminal Channel , DSA algorithm , Agreement , Salting .

INTRODUCTION

A subliminal channel is considered a covert type of communication channel in order to send a message to an authorized receiver. The property of this message is that it cannot be discovered by any unauthorized receiver. Simmons is the first one who invented the concept of subliminal channel to be used as an effective tool in conventional digital signature schemes [1] . The subliminal channel has several applications. For example, a credit card provider can hide the card holder›s credit [2] .

Simmons explained In 1985, that in any digital signature scheme in which α bits are used to communicate a signature that providesβ bits of security against forgery, where α>β , the remainingα- β bits are potentially available for subliminal communication[3]. Also, Simmons gave a definition which implies that if the subliminal channel uses all, or nearly all, of the α- β bits, then the subliminal is known as broadband, while if it uses only a fraction of the bits, it is called a [4].

In addition to the work of Simmon , Both of Harn and Gong had proposed two types of schemes that have the ability to provide a digital signature with a broadband subliminal channel with a property that is it does not require the subliminal receiver to share

A Subliminal Channel in DSA
Using Agreement Factor and Salting

Dr. AbdulameerKhalaf Hussain

Alsalam University College - Iraq

قناة اللاوعي الاخفائية في طريقة
دي أس أي باستخدام عامل الاتفاق والتمليح

ا.م.د. عبد الامير خلف حسين

كلية السلام الجامعة

رئيس قسم هندسة تقنيات الحاسبات