Application of Data Authentication and Modification of Das's Remote System Authentication Scheme using Smart Card

Chandan Koner*
Chandan Tilak Bhunia**
Ujjwal Maulik***

Abstract

Remote systems authentication schemes need more research and investigation due to increasing of hackers and attacks with the increasing volume of wired and wireless traffic. All of the popular remote system authentication schemes provides only entity authentication, not provides any data authentication. Recently Das proposed a flexible remote systems authentication scheme using smart card [6] that checks authenticity of user as well as remote server but provides only entity authentication, not provides any data authentication.

In this paper, we show that Das's scheme is not withstand the alternation data attack, reverse XOR attack and adversary system attack. We have applied Data authentication cryptography technique to the Das's scheme that serves as entity authentication as well as data authentication. We show that how application of Data authentication cryptography technique in Das's scheme enhances the security and efficiency of Das's technique and defenses alternation data attack, reverse XOR attack and adversary system attack.

Keywords: Data Authentication, Entity Authentication, Remote user, Remote system, Smart card.

1. Introduction

In Remote system authentication, Remote system checks the authenticity of the remote user when the user starts to access the system. Remote password authentication scheme using smart card was first proposed by Chang and Wu [3] in 1993. After that, several new remote user password authentication schemes with smart card have been proposed. Remote user authentication using smart card, introduced by Hwang and Li [4] in 2005, is an application of ElGamal's [5] cryptosystem. After that, few public-key based authentication techniques have been invented and developed. But all of the techniques check only the authenticity of user but can not check the authenticity of system. In 2006, Das [6] developed a flexible remote user authentication scheme using smart card that authenticates user as well as remote system.

In all of the above techniques, the remote system checks the authenticity of remote user by the entities (e.g. password, smart card etc) of user before the transmission of user message. After the transmission of user message, the authentication of remote user is not checked by the remote server. So an intruder can alter user message in the transmission of user message. This motivates us to develop a scheme that will serve as data authentication as well as entity authentication. In this paper, we show that Das's

*Bengal Institute of Technology and Management, Dwarnda-731236, Birbhum, W.B., India.
**Bengal Institute of Technology and Management, Dwarnda-731236, Birbhum, W.B., India and I.C.T.P, Italy.
***Jadavpur University, Kolkata-700032, India.

scheme is vulnerable to different attacks and we have applied Data authentication cryptography technique (Digital Signature) [1, 2] to the Das's scheme. So that Modified Das's scheme will serve as entity authentication as well as data authentication and will not suffer from those attacks. We analysis that how the performance of Das's scheme is increasing by applying the data authentication scheme.

2. Review of Das's Remote System Authentication Scheme

Das's Remote System Authentication Scheme authenticates the user as well as the remote system by the user's entities. The user chooses a password (PW_i). The user has no private or public key but the remote system has a primary secret key (x) and a secret number (y). This scheme consists of three phases: registration phase, authentication phase and password change phase.

In the registration phase, the user U_i submits PW_i to the remote system (RS) for registration. The RS computes $N_i = h(PW_i,ID_i) \oplus h(x)$ and personalize a smart card with the parameters h(.), N_i, $h(PW_i)$, ID_i and y.

The authentication phase is divided into two parts, namely the User authentication and the RS authentication.

In user authentication phase, U_i insert his smart card and submits ID_i and PW_i. The smart card checks PW_i and ID_i with the stored ones in smart card. If they are correct, the smart card computes $DID_i = h(PW_i,ID_i) \oplus h(y \oplus Tu)$, where Tu is timestamp of U_i 's system and $C_i = h(N_i \oplus y \oplus Tu)$. Send (DID_i, C_i, Tu) as login request to the RS. RS receives the login request at time Ts and authenticates the U_i by the following way. If the time interval between Tu and Ts is the expected valid time interval for the transmission delay, then RS computes $h(PW_i,ID_i) = DID_i \oplus h(y \oplus Tu)$ and $C_i^* = h(h(PW_i,ID_i) \oplus h(x) \oplus Tu \oplus y)$. If $C_i^* = C_i$, the user is authentic.

In RS authentication phase, RS computes $X_i = h(h(PW_i,ID_i) \oplus h(x) Tu \oplus Ts^*)$ where Ts* is timestamp of RS's system and sends (X_i, Ts^*) to the user. Let the user receives the response at time Tu*. If the time interval between Tu* and Ts* is a valid time interval then computes $X_i^* = h(N_i \oplus Tu \oplus Ts^*)$. If $X_i^* = X_i$, then the RS is authentic.

3. Cryptanalysis of Das's Technique

In this section, we discuss a cryptanalysis of Das's remote system authentication scheme. Das showed that, although his technique is secured from replay, stolen verifier, impersonation, guessing and denial-of-service attack but his technique is still vulnerable to reverse XOR attack and adversary system attack. We demonstrate these attacks.

Alternation data attack: As the remote system checks the authenticity of user before the transmission of message. Remote system does not apply any authentication checking process on user message. So an adversary can change user message in the transmission of message. Hence Das's scheme is suffer from alternation data attack.

Reverse XOR attack: During the registration phase, the secret key x has to be applied. Now based on the reversible property of XOR operation, if the primary secret key of remote system (x) is hacked, user password (PWi) is guessed and mode of hash function is leaked, then nonce, Ni can be easily obtained. Hence Das's scheme is vulnerable to the reverse XOR attack.

Adversary system attack: Suppose the processors in remote system and card reader are very hasty and the transmission of data between user and server is happening in very speedily. In this type of communication, the timestamp of user Tu in user authentication phase and the timestamp of server Ts* in remote system authentication phase will be equal. During remote system authentication phase, remote system sends X_i [$= h(Ni \oplus Tu \oplus Ts^*)$ or $h(h(PW_i,ID_i) \oplus h(x) \oplus Tu \oplus Ts^*)$] to the user over a public channel. As Tu and Ts* are same so $X_i = h(N_i)$. Again suppose an adversary has stolen the user smart card for one time and just extract the Ni and mode of hash function is known to him so he can easily compute Xi which is h(x). Now if the adversary is also a user and accessing another server then he can send X_i to the user by that illicit sever over the public channel before the original server sent. Then user can easily certify that server as an authentic server and communicates with that illicit server. The adversary, thus, can trick the user by connecting him with a wrong server. Das's scheme is therefore insecure from the adversary system attack.

4. Modified Das's Remote System Authentication Scheme (application of Data Authentication)

Modified Das's Remote System Authentication Scheme is mainly divided into two parts, namely, Entity Authentication Phase and Data Authentication Phase. The Entity Authentication Phase checks the authenticity of the remote user by user password. The Data Authentication Phase checks the authenticity of the remote user by applying cryptography (Digital signature) on the user sending message. The Entity Authentication Phase is further subdivided into four parts, namely, User Enrollment Phase, User Login Phase, User Accessing Phase and Remote System Authentication Phase. Data Authentication Phase is also subdivided into three parts, namely, Key Generation Phase, Data Sending Phase and Data Receiving Phase.

4.1. Entity Authentication Phase

User Enrollment Phase: In this phase, the user registers to the remote system RS. The user chooses a password PW and submits it to the RS. After receiving enrollment request, the remote system performs the following operations.

(i) Computes, $N = h(PW \oplus ID \oplus E) \oplus h(x)$, where x is a primary secret key of RS and E is the encryption key generated by remote system by applying RSA algorithm.
(ii) Personalizes a smart card with the parameters <N, PW, ID, E>
(iii) Sends the smart card to the user in a secure channel.

4.2 User Login Phase

When the user wants to login to the remote system then the following steps are executed. This part is executed only once when the user wants to login to the remote server. User inserts his smart card and keys his identity ID and password PW'. The smart card verifies the entered ID and PW' with the stored ones in smart card. If the ID is correct and PW and PW' are same, the smart card executes the following steps,

(i) Computes, $D = h(PW \oplus ID \oplus E) \oplus h(y \oplus Tu)$
(ii) Computes, $C = h(N \oplus Tu \oplus y)$
Then send (D, C, Tu) as login request to the remote system. After receiving the login request, the remote system authenticates the user the following steps,
(iii) Computes, $h(PW \oplus ID \oplus E) = D \oplus h(y \oplus Tu)$
(iv) Computes, $C^* = h(h(PW \oplus ID \oplus E) \oplus h(x) \oplus Tu \oplus y)$

If $C = C^*$, the remote system accepts the login request and gives permission to the user to send the data.

4.3 Remote System Authentication Phase

The correctness of remote system is checked in this phase and executed when authenticity of user is passed correctly.

(i) Computes, $X = h((h(PW \oplus ID \oplus E) \oplus h(x) \oplus h(Tu)) \oplus h(Ts)$
(ii) Send (X, Ts*) to the user over a public channel.
The smart card computes $X^* = h((N \oplus h(Tu)) \oplus h(Ts)$ and checks whether $X = X^*$ or not. If $X = X^*$, then remote system gives the permission to access.

4.4 Data Authentication Phase

Key Generation Phase

This phase is executed after receiving the enrollment request by the receiver in parallel with user enrollment phase. In this phase the remote server executes the following steps,

(i) Generates Encryption Key (E) and Decryption Key (D) by RSA algorithm.
(ii) Personalizes a smart card with the parameter E and the other parameters <N, PW, ID>.
(iii) Sends the smart card to the user in a secure channel.

4.5 Data Sending Phase

After getting the permission from the remote server, smart card performs the following operations.

Let the user message M is continuous bit string. Smart card divides M into different blocks each size of 160 bits. Let the blocks are M_1, M_2,…… M_n. At first smart card sends M_1 and the Digital Signature of M_1 (First calculates the Hash of M_1 then encrypts it by E). Then smart card sends M_2 and Digital Signature of it. Next sends other left blocks and digital signature of them sequentially. During the sending time if smart card receives any reject signal from remote system for a particular block then smart card sends that block and digital signature of it to the remote system without any delay.

4.6 Data Receiving Phase

After receiving the first message block M_1 and the Digital Signature of M_1 from the user, the remote server executes the following steps

(i) Decrypts the Digital Signature of M_1 by D and calculates the hash of M_1.
(ii) Compares the two results. If they are same, confirms that M_1 is come from authentic user. If they are not same, rejects M_1 and sends a reject signal to the user to send M_1 again.

Remote server receives the message blocks (M_2,……, M_n) one by one sequentially and the above operations for each message blocks.

5. Security Analysis of Modified Das's Scheme

We analysis that how Modified Das's scheme is protected from the various security parameters. We discuss the defense of the scheme from the various attacks by which previous scheme is suffered.

5.1 Alternation data attack: In Modified Das's scheme the remote system checks the authenticity of user on user message after the transmission of message. If an adversary alters the authentic user message during the transmission of message, the remote system can easily identify it. Hence Modified Das's scheme is not suffer from alternation data attack.

5.2 Reverse XOR attack: In this authentication scheme, $N [= h(PW \oplus ID \oplus E) \oplus h(x)]$ is computed in the registration phase. If PW is guessed and mode of hash function is leaked by an adversary, he never gets N because N is a function of four parameters PW, ID, N and x. Hence Modified Das's scheme is undoubtedly not vulnerable to the reverse XOR attack.

5.3 Adversary system attack: In remote system authentication phase, remote system sends $X [= ((h(PW \oplus ID \oplus E) \oplus h(x) \oplus h(Tu)) \oplus h(Ts)]$ to the user over a public channel. For a very first system where Tu and Ts are same X will not be equal to the h (N). So if an adversary extracts the N by stoling the user smart card for one time and mode of hash function is known to him then he never gets X. So the user always authenticates a correct server. Hence Modified Das's scheme is firmly secured from the adversary system attack.

6. Result and Discussion

Suppose user Password and ID are that user submits in the User enrollment phase,

User Password (PW): User'sAuthentication

User Identifier (ID): Identity of Remote User

Suppose Remote system generates Encryption and Decryption key by RSA algorithm in the following way,

Let, two large prime numbers P=13 and Q=19. So, $N = 13 \times 19 = 247$
Encryption Key (E) = 31 and Decryption Key (D) = 7

Suppose User sends a message of 1600 bits to the Remote server,

User Message : "Authentication in sending information is a great research challenge.Remote system authentication is a process by which a remote system gains confidence about the identity of the communicating partner."

User sends a message block of 160 bits to the Remote system in one session. The blocks are M_1, M_2,….., and M_{10}. Each of them are size of 160 bits because the total size of M is1600 bits.

User Message Set (M):

M_1 = 41757468656e7469636174696f6e20696e 207365
M_2 = 6e64696e6720696e666f726d6174696f6e206973
M_3= 20612067726561742072657365617263683696368
M_4 = 616c6c616e67652e52656d6f7465207379737465

M_5= 6d2061757468656e7469636174696f6e20697320
M_6= 612070726f6365737320627920776869636820 61
M_7= 2072656d6f7465207379737465 6d2067696e73
M_8= 20636f6e666964656e63652061626f7574207468
M_9 = 65206964656e74697479206f662074686520636f
M_{10}= 6d6d756e69636174696e6720706172746e65722e

Smart card and Remote system apply Hash function on each message block M_i to obtain HM_i (Hash of M_i) in one session. HM_i is also size of 160 bits.

Hash Set (HM) of M obtained in Data Authentication:

HM_1= 42e743957f49558a4d6e6e36d840c4c828b50402
HM_2= a85f2c4bdc021e6f8b624812624e14eaa9fc7b31
HM_3 = 41142e9c38c0a3017ec833b8d0dd3fd27e15071e
HM_4 = 6ce258cf7eab54ebbd886744682f00b2dbaf561d
HM_5= 528fe2d161c85b6d5d9e8f71c5d03b4873c760ac
HM_6 = 653f5061485490489238187a94e0f4fa73c9bc15
HM_7 = 96b7acf35835acd82241df00efe2f3b2d0164380
HM_8= e0770291fa97e762e4d0fd7c3e5e49a8662e10b0
HM_9= 0e6bef8147b1f2f720613a1df368d41034a0f84b
HM_{10}= 4c3f17baad4ca60d96c31ac9aaa19a94da7bce85

Smart card encrypts HM_i by E to obtain DM_i (Digital Signature of M_i). DM_i is also size of 160 bits.

Digital Signature Set (DM) of M obtained in Data Authentication:

DM_1= c4a659b0cd0506e24d7c7c18534076cb4f33c7c1
DM_2= e95f634bdcc11ed63d47a29747753a9c8270d731
DM_3 = 413a546838e7c9017ecb81a7d0dd50737eae2d1e
DM_4 = ba4958a87e4c2eebe3216744ea2c00b2b8554692
DM_5= 040d49d162cb8f15cee80d7166d088a2d252e5ac
DM_6 = 1750b462a22e90a2e0385d0856b91d3ed2a36fae
DM_7 = 95b7ac305869ac53c8419a007d4930b2d0cc5902
DM_8= 1df5c132b912a64713d08920245e05e9c55451bc
DM_9= 286b7db53bd587004862149230ea93514ea001ab
DM_{10}= ab50daeed4abc05b95a91aa3aab1295665d77785

7. Experimental Analysis of Data Authentication

We analysis the results of Das's scheme and Modified Das's scheme by two directions, Graphical analysis and Character analysis. Graphical analysis compares the result of Das's scheme and Modified Das's scheme by bit to bit in different session. Character analysis compares the result of Das's scheme and Modified Das's scheme by character to character.

7.1. Grphical Analysis

In this section, we compare and analysis the bit variations between the User Message block (M_i) and Digital Signature of that Message block (DM_i) in different session. Increasing of variant bits means increasing the probability of authentication success of the scheme.

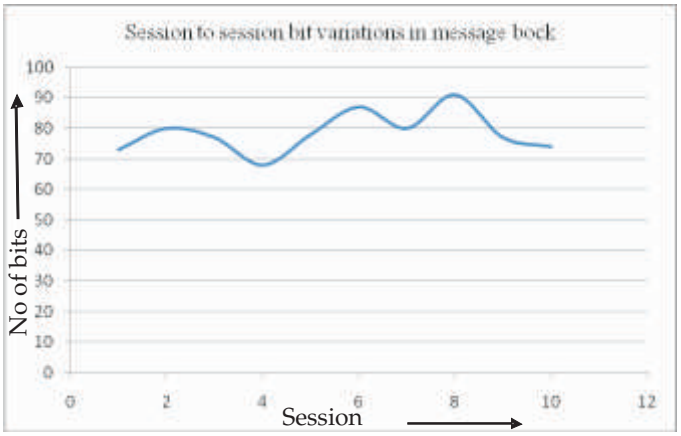

Fig : Plot of bit variations between M_i and DM_i with different session

The above graph shows that bits are variable in every session. The graph also shows that maximum no of bit variation occurs in session 8 and minimum no bit variation occurs in session 4. In session 8, 91 bits are variable out of 160 bits so the probability of authentication success is 91/160 and in session 4, 68 bits are variable out of 160 bits so the probability of authentication success is 68/160.

So, we can conclude that our scheme increases the probability of data authentication success. As data authentication enhances the performance of the remote system authentication scheme so our scheme will be pioneer of data authentication in remote system authentication.

7.2 Character Analysis

In this section, we compare and analysis the characters between the User Message block (M_i) and Digital Signature of that Message block (DM_i) using two parameters: Redundant Character and Redundant Pair Character. Redundant character measures by same character if they are in same position in M_i and DM_i. Redundant Pair character measures by same character if they are in consecutive position in both Mi and DM_i.

Redundant Character: There are only 19 characters are redundant out of 200 characters. So the probability of redundant character is 19/200.

In case of Das's scheme, every character is redundant character. So the probability of redundant character is 1. The probability of Redundant character increases the probability of authentication failure.

So, the probability of authentication failure of Modified Das's scheme is very less than the Das's scheme. Comparing by redundant character, we conclude that Modified Das's scheme is more efficient than the Das's scheme.

Redundant Pair Character: There is only 1 redundant pair character out of 100 pair. So the probability of redundant pair character is 1/100.

In case of Das's scheme, every pair of character is redundant pair character. So the probability of redundant pair character is 1. The probability of Redundant pair character increases the probability of authentication failure.

So, the probability of authentication failure of Modified Das's scheme is very very less than the Das's scheme. Comparing by redundant pair character, we state that Modified Das's scheme is more efficient than the Das's scheme.

8. Conclusion

In Modified Das's Remote System Authentication Scheme, we have applied the Data authentication cryptography theory to invent an efficient Remote System Authentication scheme which provides entity authentication as well as data authentication. We shows that the efficiency of our proposed scheme is more than previous scheme.

Characteristics of the scheme are,

(i) This scheme enjoys the advantages of Data Authentication as well as Entity Authentication.
(ii) Authenticity of user is verified on not only the entitiy (e.g. password, smart card etc) of user but also the user message by the server.
(iii) Instead of sending raw user message, Digital Signature of user message is sent to the server.
(iv) Simple one way hash function and XOR operation are only used.
(v) User authenticity as well server authenticity is checked efficiently.
(vi) Many users with same login identity can not able to log in.
(vii) Any user password database is not required in remote sever.

9. References

1. *C. T. Bhunia, Information Technology Network and Internet, New Age International Publishers, India, 5th Edition (Reprint), 2006.*
2. *Atul Kahate, Cryptography and Network Security, Tata McGraw Hill, India, Sixth Reprint, 2006.*
3. *C. C. Channg and T. C. Wu, Rmote password authentication with smart cards, IEEE Proceeding-E, Vol. 138, no. 3,pp. 165-168, 1993.*
4. *M. S. Hwang and L. H. Li, A new remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, pp. 28-30, February 2000.*
5. *T. ElGamal, A public key based cryptosystem and a signature scheme based on discrete algorithms, IEEE Transactions on Information Theory, Vol. 31, No. 4, pp. 469-472, 1985.*
6. *M.L.Das, Flexible and Secure Remote Systems Authentication Scheme Using Smart Cards. HIT Transaction on ECCN, Vol. 1, No.2, pp.78-82, April 2006.*