NEW TECHNIQUE TO SOLVE KEY EXCHANGE PROBLEM

Dr Ghazi. I-Raho[1], Adham mohsin saeed[2]
[1]Department of MIS, Amman Arab University, Jordan -Amman
[2]Computer Engineer Dept, Al-Rafidain University College, Iraq, Bagdad
[1]larsa_rr@hotmail.com, [2]alshamary.adham@yahoo.com

Abstract- Key exchange has been solved using authentication protocols which add more computations and ciphering processes as the key is ciphered mostly using public key cryptosystems. In our proposed solution there would be no additional ciphering and Moreover Our proposed solution depends on mixing the cipher key with ciphered block in ciphering key in a way that only the legitimated receiver can easily extract the ciphered data and the cipher key and decipher to get the plain text.

Key words- key broadcast, Rijndael algorithm, key exchange.

I. INTRODUCTION

The development of software systems inevitably involves the security of the data which may be used in different stages of an automated system. A large proportion of software research has been devoted to securing software and systems which includes system data. Industrial reality however suggested that practitioners and their customers live with the threat of security breaches that might take place. Security is considered a fundamental aspect of any information technology system, as a result of growing system penetration and electronic fraud concerns, and certain fundamental trends [Ford1994]. However cryptographic knowledge has grown to the point that an algorithm to protect international commerce and communications [Landau2000].

Theoretically secure systems are based on the fact that there are multiple solutions to a cryptogram. Another problem is that cryptographic systems become impractical when a large number of users are involved [Leung1978]. Cryptography has been mainly concerned with the problem of private secure communication between two parties. However a number of cipher algorithms significantly solve this problem as these algorithms use certain secret keys. In commercial data networks, there is a need for many pairs of users to communicate in privacy. The classical method of distributing secret keys over a secure channel to each user pair becomes very expensive and alternative means have to be explored [Leung1978].

Symmetric cryptography in the sense that either the same piece of information cipher key is held in secret by both communicants, or else that each communicant holds one from a pair of related keys where either key is easily derivable from the other [Simmons1979].

In secret key cryptography, system must combine two elements: private secret *key (cipher key),* known only to the authorized communicants, and an *algorithm* which operates on this private secret cipher key and the message (plaintext) to produce the ciphered message (ciphered text) [Bellare1998]. The authorized receiver, knowing the cipher key, must be able to recover the ciphered text (decrypt the ciphered message); either an unauthorized receiver or an adversary should not be able to deduce either the message or the unknown cipher key. The cipher key as defined here is very general: It is the total equivocation of everything that is kept secret from an opposing cryptanalyst [Simmons1979].

II. A SECURE SYSTEM LOG-IN PROCEDURE

The object of secure communications has been to provide privacy or secrecy, to hide the contents of a publicly exposed message from unauthorized recipients [Simmons1979].

This method used in computer system for checking the authenticity of users involves, it the use of passwords. Each user should have been assigned an account number when user first joins the system. User should also choose a password which he /she keeps secret as part of the system and should be hidden from other users. There is limitation with this approach as if an intruder who obtains the password can gain easy access to all the accounts in the system. Moreover clever cryptanalysts can predict the password to break the system as end users will choose weak keys as long as they are allowed to [Schneier1994], so it is actually difficult to prevent the adversary from guessing a value for the password and using this value in an attempt to impersonate a player [Bresson2003]. Password is preferred to be more than 15-character long, passwords to exploit the serious human engineering problem since users do not easily remember random 15-character long passwords [Leung1978].

III. CLASSICAL CRYPTOGRAPHY SYSTEM

The classical design of the cipher system as described in [Leung1978] is shown in figure 1 aims to transmit the encrypted text to the receiver privately over an insecure channel to the legitimate receiver. In this model both sender and legitimate receiver know the secret cipher key as sender sends it over secure channel.

IV. THE ENCRYPTION/DECRYPTION CHANNEL [SIMMONS1979]

The encryption channel also consists of a transmitter who wishes to send a message M to a receiver. However the channel is assumed to be under observation by a hostile adversary. Cryptographic theory seeks to devise codes that cannot systematically be distinguished from purely random bit strings by the adversary. The statistical communications channel of the coding/decoding model has been replaced by a game theoretic channel; nature has been replaced by an intelligent adversary. The adversary can have one or more of the following purposes:

a) To determine the message M.

b) To alter the message M to some other message *M'* and have *M'* accepted by the receiver as the message actually sent.

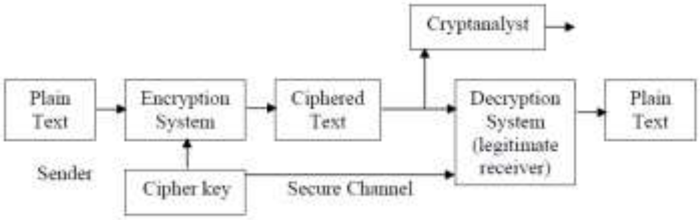

Figure 1: Classical Secret System [Leung1978]

c) To make-believe to be the transmitter.

V. MANAGING THE KEYS SHOULD ACHIEVE THE FOLLOWING GOALS: [WOOL2000]

- **Flexibility:** application should have the ability to use as many different keys as can be possible. Moreover user may share in knowledge to determine part of this key. Legitimated receiver should not suffer to receive the secure message. Further it should encrypt messages of arbitrary length and use a single block-cipher key [Rogaway2003].
- Another aspect of a cipher scheme's flexibility is the ability to make the packaging simple and understandable by user. Moreover, the system should use many cipher keys as every block may be ciphered using different cipher key.
- **Security: the security is very important** as adversary is a major concern, so all the process and scheme parts should be done in secure. So we can ensure that it will not be easy to attack and break the cipher key of the application and the data. In addition it should be strong enough to resist any tampering trials.

VI. RIJNDAEL ALGORITHM

It is well known to all of us, the importance of cryptography, moreover the cryptanalysis is growing rapidly in parallel to try and catch up with fast changing cryptography. Furthermore National Institute for Standards and Technology (NIST) always renews its standard algorithms in public, which encourages both cryptographers and cryptanalysts to improve their algorithms and techniques. This means that Rijndael algorithms is very important since it is considered as US government official algorithm, this would make it an interesting research field for both cryptographers and cryptanalysts. It is surprising that research papers and reports, which discuss Rijndael algorithm are limited seven areas: performance comparison between the finalist algorithms, attacking, hardware implementation and algebraic structure. Therefore only two papers to the best of our knowledge discuss the algorithm in details, giving examples with explanations [Gladman2003] and [AESpage].

It is obvious that there is a shortage in software engineering analysis and programming papers in this field moreover, the programs presented are just implementations for *16 bytes* in hexadecimal. This also will not be able to cipher one block unless it is converted to hexadecimal and added to the source program. This is only useful to beginners in this field. However the real software application for this important algorithm was explained by [RashedAjlouniJune2004] and [RashedAjlouni12004].

As we see, there are many gaps in this field which can be filled by our proposed system "Intelligent Encryption Decryption System".

VII. PROBLEM

The need of private secure communication arises whenever there are many parties or adversaries who can receive the private information. So it is necessary to have conventional ciphers, which allow private communication only among parties who have already exchanged secret keys [Leung1978].

The secret keys are used in the encryption process to introduce uncertainty to the unauthorized receiver, which can be removed in the process of decryption by an authorized receiver using his copy of the key or the "inverse key" This means, that if a key is compromised, further secure communications are impossible with that key [Simmons1979].

In secret key cryptography, the problem is how to distribute the shared secret key. The real problem is that both parties need secure communications to achieve key exchange operations [Bellare1998]. Gong [Gong1994], uses one way function and polynomial interpolation to broadcast secret keys and suggests reducing the use of secure keyed one-way hash functions as he comments that it is unclear whether his protocol techniques can be beneficial when clients do not share secrets with the server but instead register their public keys. In Eschenauer and Gligor's scheme, key distribution consists of three phases, namely key pre-distribution, shared-key discovery, and path key establishment. The two nodes discover if they share a key, i.e. each node broadcast in clear text, the list of identifiers of the keys on their key ring. This approach does not give an adversary any attack opportunity that he does not already have [Eschenauer2002]. Wool uses ExtHeader such that cryptographic header information is attached to each program [Wool2009] in TV broadcast, he supposes that programs would be split into n blocks and ciphered by the same key. Parnerkar, Guster and Herath present a framework that uses hybrid crypto algorithms for key distribution. A triple DES with a 168-bit key is used to generate the secret key. This secret key is transferred with the help of public key cryptography [Parnerkar2003].

Parnerkar, Guster and Herath proposed integrating public-key cryptography and digital certificates to strengthen transmission security. The process was implemented by using a handshaking protocol providing mutual authentication between two participants. It would be able to send the public key to the server via secured email or on a diskette [Parnerkar2003].

VIII. PROPOSED SOLUTION

Broadcasting the cipher key can be solved by mixing the cipher key with ciphered block in special way that only the legitimated receiver can extract both cipher key and ciphered block to be able to do the inverse cipher phase and get the plain text. The proposed system can resist a cryptanalytic attack involving an unlimited amount of computation.

IX. CONCLUSION

In this paper the problems with current cryptography systems has been highlighted. It has also been shown that all systems still have noticeable problems in both generating secure key that is prone to known and unknown attacks by adversary. It is suggested in this paper to implement different algorithms which will show simple methods that can be used to generate keys. Finally a new and novel algorithm should be designed, which will combine a mixture of both ciphered data blocks and ciphering key in a single file, which will be called output file or ciphered file. This will be created in an intelligent manner, which will add a higher level of security the ciphered data. A complete set of algorithms for both ciphering and deciphering for each proposed solution should be built and mathematical, it is proved.

REFERENCES

[1] [Ford1994] W. Ford, Standardizing Information Technology Security, Standard View Vol. 2, No. 2, , 2000, pp:64 -71.

[2] [Landau2000] Susan Landau, Designing Cryptography for the New Century, Communications of the ACM May 2000/Vol. 43, No. 5 pp: 115-120

[3] [Leung1978] C. Leung, Some Open Problems in Cryptography, Proceedings of the 1978 annual conference, December 1978, pp: 471- 475.

[4] [Bellare1998] M. Bellare, R. Canetti and H. Krawczyk, A Modular Approach to the Design and Analysis of Authentication and Key Exchange Protocols,

[5] Proceedings of the thirtieth annual ACM symposium on Theory of computing, May 1998, pp: 419-428.

[6] [Simmons1979] G. Simmons, Symmetric and Asymmetric Encryption, Computing Surveys, Vol. 11, No. 4, December 1979, pp: 306-330.

[7] [Schneier1994] B. Schneier, Designing Encryption Algorithms for Real People, Proceedings of the 1994 workshop new security paradigms, 1994, pp: 98-101.

[8] [Wool2009] A. WOOL, Key Management for Encrypted Broadcast, ACM Transactions on Information and System Security, Vol. 3, No. 2, May 2000, pp 107–134.

[9] [Rogaway2003] P. Rogaway and J. Black, OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption, ACM Transactions on Information and System Security, Vol. 6, No. 3, August 2003, pp:365–403.

[10] [Gladman2003] B. Gladman, A Specification for Rijndael, The AES Algorithm 2003, B. Gladman's AES related home page http://fp.gladman.plus.com/cryptography_technology/

[11] Brian Gladman. AES Source Code Implementation. At http://fp.gladman.plus.com/cryptographytechnology/rijndael/index.htm

[12] [AESpage] NIST 2001a. Federal Information Processing Standards Publication (FIPS PUB) 197. NIST, AES page available via http://www.nist.gov/publications.

[13] [RashedAjlouniJune2004] A. Abdali Rashed, Naim Ajloni, an extended Rijndael Block Cipher Using Java, the 2004 International Conference on software Engineering Research and practice, Las Vigas, Nevada USA, June 2004, 21-24.

[14] [RashedAjlouni12004] A. Abdali Rashed, Naim Ajlouni, RASAN Java Encryption Decryption System, submitted to Canadian Journal of Computer Science.

[15] [Gong1994] Li Gong, New Protocols for Third-Party-Based Authentication and Secure Broadcast, Proceedings of the 2nd ACM Conference on Computer and communications security, 1994, pp: 176-183.

[16] [Eschenauer2002] L. Eschenauer and V. Gligor, A Key-Management Scheme for Distributed Sensor Networks, Proceedings of the 9th ACM conference on Computer and communications security, 2002, pp:44-47.

[17] [Parnerkar2003] A. Parnerkar, D. Guster, J. Herath, Secret Key Distribution Protocol Using Public Key Cryptography, The Journal of Computing in Small Colleges, Vol. 19 No. 1, October 2003, pp:182-192.