Science Arena Publications
Specialty Journal of Electronic and Computer Sciences
ISSN: 2412-7485
Available online at www.sciarena.com
2019, Vol, 5 (3): 1-9

Authentication and Encryption Mechanisms

Dina Daliri[1, 2]

[1] Master of Computer Architecture Engineering, Imam Reza International University, Mashhad, Iran.
[2] Bachelor of Computer Engineering-Software, Sajjad University of Technology, Mashhad, Iran.

Abstract: *Authentication is a process that occurs between the sender and the recipient so that in this process, either party or one of the parties must provide something to establish trust between the communications; after the authentication process was performed correctly and trust was created naturally, both parties will reach the communication goal and the server will service the client. The purpose of this research was to introduce the security structure and the authentication problem and their implementation mechanisms, such as the authentication mechanism based on the challenge and response approach, the mechanism based on a key distribution center, the authentication mechanism Nidham-Schroeder, the authentication mechanism with (Kerberos V5. Kerberos version Kerberos5) and authentication mechanism using public key encryption and review each of these methods.*

Keywords: *Security structure, Authentication, Encryption.*

INTRODUCTION

Today, in the age of communication, with the advancement of technology, control over the security of payment systems in e-commerce has become more complicated. Parallel to this advancement, encryption science has also provided good tools for security with its rapid growth. One of these tools can be private key encryption, public key, digital signing, and hash functions. These tools ensure the confidentiality of data, authenticity of users' identity and data, non-denial, secure e-commerce, multiple communications and tracking, and more. One of the aspects of exploitation in e-commerce is to forge a title. An encryption algorithm is referred to as an algorithm or mathematical function, which is to be used in encryption protocols due to the encryption properties required. The encryption algorithm is a comprehensive concept, and it is not necessary that any algorithm from this category be used directly for the encryption of information, but rather the existence of an encryption application. In the past, organizations and companies that needed encryption or other encryption services designed a unique encryption algorithm that over time, it became clear that sometimes there were great security weaknesses in these algorithms, which make it easy to break the password. For this reason, encryption based on hiding the encryption algorithm today is outdated, and new encryption methods assume that the full information of the encryption algorithm has been published, and what is hidden is just the password key. Therefore, the issue of authentication and non-denial is one of the fundamental principles of security in electronic exchanges.

Research literature

Symmetric key algorithm

Search for symmetric key algorithms, a class of algorithms, used for encryption using the same encryption keys for both text encryption and decryption. The keys may be similar, or there may be a simple switch between the two keys. The key in action represents a common secret between two or more parties that can be used to maintain private information. It requires both parties to have access to hidden keys; this is one of the main problems of symmetric key encryption of the symmetric key in comparison with public key encryption.
the symmetric algorithm uses a key for encryption and uses the same key to decrypt it. The most common form of use of this type of encryption is in smart cards and, of course, in most information security systems. The DES algorithm is a US state product that is nowadays widely known as a well-known international standard. The 64-bit data blocks are encrypted and decrypted by a single key, usually 56 bits long.
In these systems, both the encryption and decryption keys are the same or extracted by a very simple relationship, and encryption and decryption of information are also two inverted processes. Clearly, in this type of encryption, a common key must be defined between the two parties, because the password key must remain completely confidential.

Encryption DES

The DES data encryption standard is a mathematical algorithm used to encrypt and decrypt binary coded information, which encrypts data into inaudible data called CIPHER. Decryption from CIPHER returns it to the original data. The algorithm defines both encryption and decryption operations based on a binary number called the key. Data can only be recovered from cipher, which the key used for encryption is also used to decryption. The DES algorithm has two components.
Encryption algorithm: the published DES algorithm contains several replications of a simple deformation using both displacement and replacement techniques. This algorithm uses only one key for encryption and decryption, that's why it's called private key encryption. In this case, keeping the key confidential is very important for the sender and receiver of the message.
Encryption key: the DES key is an 8-byte sequence, each bit containing a seven-bit key and 1-bit of parity. During the encryption, the DES algorithm breaks the original text into 64-bit blocks. Characters are 16 times under the control of the key to deformation and eventually a 64-bit encryption text is generated. The key contains significant 56-bit and 8-bit of parity.

Asymmetric method encryption

Encryption algorithms with asymmetric keys use different keys for encryption and decryption. Many systems allow one of the keys to be published as a public key, while the other is kept private by the owner. The sender encoded the text message with the public key of the receiver, and the receiver decrypts it with his private key. In other words, only the recipient's private key can convert the encoded text to the correct initial text. That is, even the sender, although aware of the original message content, cannot use the encoded text for any receiver other than the sender's intended recipient, and it will not be meaningful. The most common asymmetric system is known as RSA and RSA uses two keys for encryption: a private key, public key.

Comparing the encryption of symmetric and asymmetric algorithms

Symmetric algorithms have higher speeds and asymmetric algorithms have better security. In the meantime, the system uses a combination of both algorithms. These algorithms are called hybrid algorithms. But if we look more closely at these two, then we will find that asymmetric algorithms and symmetric algorithms have two completely different nature and use, for example, in simple encryption that has a large amount of data, the symmetric algorithm is used, because the data is encrypted and decrypted at a higher rate. But in protocols that are used on the Internet, asymmetric algorithms are used to encrypt keys that require management.

DES algorithm

The overview of the algorithm in DES is the 64-bit length. The key also includes 64 bits, but in practice, only 56 bits are used, and the other 8 bits are only used to check parity. The algorithm contains 16 similar steps, each of which is called *round*. The text that is to be encrypted is initially exposed to an initial permutation

(IP). Then a series of complex actions key is performed on it and ultimately subjected to a final permutation (FP); FP and IP are inverse; the FP neutralizes the action performed by the IP. Therefore, the encryption aspect is not important and but was included in order to facilitate loading blocks in and out of mid-1970s 8-bit based hardware but slowed down the implementation of DES in the software. Before the main rounds, the block is divided into two 32-bit halves and processed alternately; this crisscrossing is known as the Feistel. The Feistel structure ensures that decryption and encryption are very similar processes and the only difference is that the subkeys are applied in the reverse order when decrypting. The rest of the algorithm is identical. This greatly simplifies implementation, particularly in hardware, as there is no need for separate encryption and decryption algorithms.

Key schedule algorithm

This algorithm is used to generate subkeys. Initially, 56 bits of the key are selected from the initial 64 by Permuted Choice 1 (PC-1) and the remaining eight bits are either discarded or used as parity check bits. The 56 bits are then divided into two 28-bit halves; each half is thereafter treated separately. In successive rounds, both halves are rotated left by one or two bits, and then 48 bits from the left half, and 24 from the right. The rotations mean that a different set of bits is used in each subkey; each bit is used in approximately 14 out of the 16 subkeys. The key schedule for decryption is similar, but the subkeys are in reverse order compared to encryption. Apart from that change, the process is the same as for encryption.

Security DES

The most basic attack for each token is to test all the possible values for the key. The length of the key determines the number of possible keys, and hence the feasibility of this method. There was the doubt that from the beginning and even before that DES was known as standard, there was enough key for DES. The key was IBM, the NSA reduced the key length from 128 bits to 64 bits and then to 56 bits, indicating that the NSA even at that time, it was also able to break the 56-bit keys. Various designs have been proposed for a machine that can break down the DES keys. In 1977, Diffie and Hellman proposed a machine costing an estimated twenty million dollars which could find a DES key in a single day. By 1993, Wiener had proposed a key-search machine costing 1 million dollars which would find a key within 7 hours. However, none of these early proposals were ever implemented and no implementations were publicly acknowledged. In 1997, RSA Company sponsored a series of contests, offering a $10,000 prize to the first team that broke a message encrypted with DES for the contest and this was done using the IDLE CYCLE idle time of thousands of computers on the Internet. The feasibility of cracking DES quickly was demonstrated in 1998 when a custom DES-cracker was built. The machine had a price of about $ 250,000, and the motivation of the team to invent the machine was to show that DES was breakable in practice as well as in theory. The machine finds a key in a little more than 2 days' worth of searching. The next confirmed DES cracker was the COPACOBANA machine built in Germany and unlike the EFF machine; COPACOBANA consists of commercially available, reconfigurable integrated circuits. There are 120 FPGA of type DIMM. Each of these modules includes 6 FPGAs. The use of reconfigurable hardware makes the machine applicable to other code-breaking tasks as well. One of the more interesting aspects of COPACOBANA is its cost factor; this machine can be built for approximately $10,000. The cost decrease by roughly a factor of 25 over the EFF machine is an example of the continuous improvement of digital hardware.

Replacement DES algorithms

Concerns about security and the short length key of DES in software motivated researchers to propose a variety of alternative block cipher designs, which started to appear in the late 1980s and early 1990s. These efforts led to the creation of designs such as CAST5, SAFER, NEWDES, IDEA, RC5, BLOWFISH, FEAL. Most of these designs kept the 64-bit block size of DES and could act as a DES replacement, although they typically used a 64-bit or 128-bit key. DES can be changed by using two keys (2TDES) or three key (3TDES) to make it safer. TRIPLE DES was introduced by one of DES's inventors.

Rayndal algorithm

Rayndal is a symmetric block cipher algorithm with a data length of 128, 192, 256 bits. Depending on the length of the key, the algorithm is independent of the length of the data format and the key length is 10, 12 or 14 rounds. Rayndal has a structure for key expansion, which, based on the number of rounds, produces a number of the subkey, which is added to the data format in each round. The algorithm consists of three important nonlinear transforms and a system security provider, and the latter are linear functions for increasing the expansion and mixing of the algorithm. This block cipher is not exactly the same as the encryption system, as it increases with the increase in the key length of the number of algorithm rounds. The runtime and speed of the algorithm depend on the length of the key.

The advanced standard of AES encryption

Until 2006, the only effective attack against the AES algorithm was the SIDE CHANNEL attack, and the NSA reviewed all five algorithms that reached the final stage, and after review, all of these algorithms were used to protect unprotected information America provides enough security. In June 2003, the US government announced that AES could be used to protect classified information and secret it. For super-secret information, the keys should be 192 or 256 bit long. This was the first time the NSA provided the public with the encryption method for encryption of super-secret information. The most common way to attack a block cipher is to try attacks that are diverse on passwords with a reduced number of rounds. AES is available for 10-round of 128-bit keys, for 192-bit keys of 12 rounds, and for 256-bit keys of 14 rounds. By 2006, the best attack was with 7 rounds for 128-bit keys, 8 rounds for 192-bit keys and 12 rounds for 256-bit keys. Some cybercriminals express concern about AES security. They believe that the margin of security is the interval between the rounds of the algorithm and the necessary rounds to break the password are low. There is also the risk that with the advancement of the algorithms mentioned, these algorithms can easily break through the key space. Breaking down a 128-bit key requires 2120 operations, which is very low compared to 2128. In fact, this today is completely impossible and impractical. The biggest attack that came with a comprehensive search on key space has led to the breakdown of the 65-bit RC5 key. So there is no worry about this. Other doubts about this algorithm are about AES's mathematical structure. Unlike most block cipher algorithms, AES has a regular algebraic definition. This structure has not resulted in any attack so far, but some researchers say that creating a code based on new hard assumptions is not risk-free. In 2002, a theoretical attack called XSL was introduced by Nicolas Courtois and Josef Pieprzyk. The two said there were weaknesses in this algorithm. Several specialists in Rheumatology discovered problems in the proposed mathematical structure of the attack and claimed that inventors of the attack are likely to make a mistake in their estimates. Whether the XSL attack can act against AES is a question that has not yet been answered, but the likelihood that the attack could actually be done is very small.

Several attacks are being carried out for some implementations known to be AES specific structures. In April 2005, D.J.BERNSTEIN stated that the CACHE TIMING attack could design a conventional day that was designed to provide time-setting information that was as effective as possible and uses the OpenSSL AES encryption method. The attack requires over 200,000 CHOSEN PLAINTEXTs. Some believe that this attack is not possible with an interval between one and more than a HOP on the Internet. In October 2005, ERAN TROMER, ADI SHAMIR, ARNE OSKIV published a paper explaining several CACHE TIMING attacks that could have been effective against AES. One of these attacks was able to get the key after 800 operations and within 56 ms, but to launch the attack; the attacker should run the program on the same system that uses AES.

Authentication

Authentication is the mechanism by which each entity, such as a server of banking or individual, examines whether its partner in a relationship is the same claiming to be with a third-party disruptive person who has put himself in place of the real side. For example, an application that acts as a server of financial and credit institution service provider must prove to the user who wants to use his institution's services to represent the

institution and also an application on the client side must prove that the real representative is the one who claims. In the world of data security, we deal with the term AAA, which means:
Authentication: is the mechanism by which the real or legal identity of individuals is proven.
Authorization: is the mechanism by which a person is personally identifiable with an entity whose identity has been obtained, that is the license and what to do in the system.
Accounting: is a mechanism that determines how much the process consumes resources of system and services, that is, for example, has sufficient credit or no?
In these three sections, the most important step is authentication, which makes the next two sections very simple.

Authentication mechanisms

This section examines the initial and basic mechanisms that are the foundation of future mechanisms.

1. **Authentication mechanism based on the challenge and response approach**

In this method, the service provider and client firstly agreed on a secret and symmetric key called the KAB (in person or by a third party), then each one by sending a the challenge string (random string) and get it encrypted (by KAB key) from the other side and decipher and compare it with the string they have already sent, authenticity of the other party's identity and so-called a session (data exchange) initiation (Figure 1).

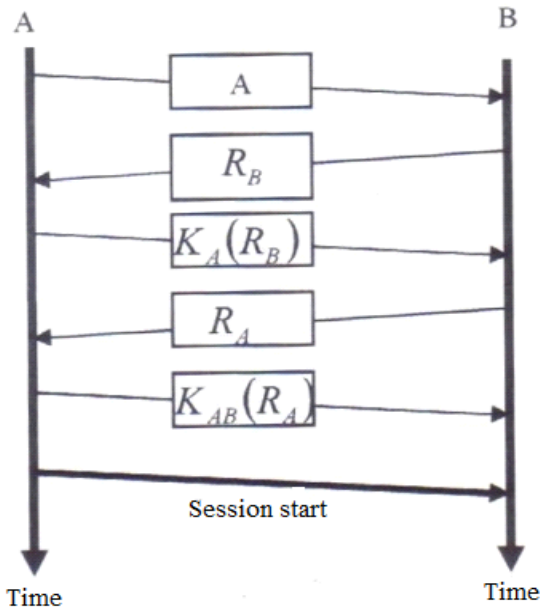

Figure 1: Two-step Authentication (Roger Needham et al., 1990)

One of the serious problems that this method faces is the "replay attack" on the part of the disruptive person. In this way, the disrupter as a client first sends a user ID A and a challenge string (RT) to a B server and its encrypted key response is received by the key (KAB (RT)) along with the server challenge string B (RB). Leaving the first session and setting up its second session as another client and the server string in the first session sends the RB back to itself and receives its encrypted response (KAB (RB)). Here it is returned to the first session and sends an encrypted response (RB) to the B server, completing the first session and exploiting the disturbance to the abuse phase. As you can see, this is a major security breach (Figure 2).

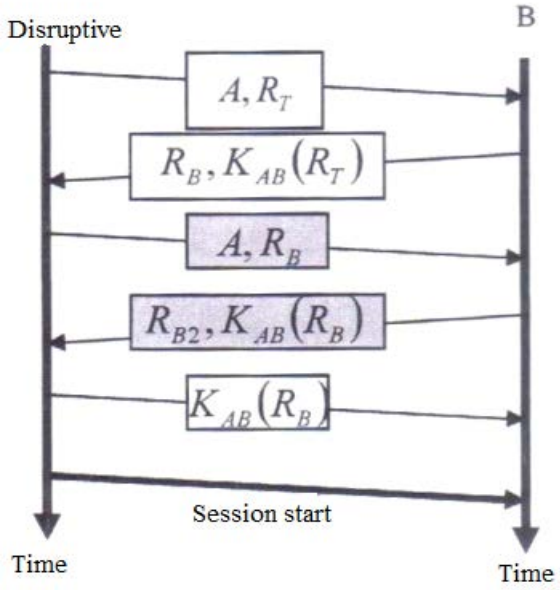

Figure 2: Replay attacks (Andrew, 2003)

There are several solutions to cover this security breach:

The first solution: is to design the system so that when the session information is viewed in a parallel session, the system interrupts both sessions.

The second solution: The parties to the transaction choose their own challenging strings from different collections so that there is no possibility of impersonation. For example, the session starts with even numbers, and the answer starts with odd numbers.

2. Mechanism-based on a key distribution center

Suppose that services provided by a bank or credit institution are such that the user must open at least one branch in the presence of an account and receive his or her secret key on a regular card or smart card, and then use its remote banking service. Obviously, the volume of the key for users is so high that it needs to be the center for storing and managing keys (as independent servers) that they call the KDC center. In the case of KDC, individuals will be authenticated to create sessions with each server only by KDC intervention and approval. First, user A firstly assigns his user ID (A) with the encrypted result, the server of the user ID (B), and the random session key with its own private key send to the KDC (i.e., A, KA (B, Ks). Because in the world only KDC has a dedicated user proprietary key (KA) A, only it can decrypt the message and after decoding, it realizes that user A intends to session with the B server. Then the KDC encrypts the ID of user A and the session key (Ks) with the B server key (i.e., Kn (A, Ks), and if the B server can log the message with its own private key (KB), it decides that this message was sent by KDC because only KDC has its own dedicated key. At this time, the KDC role is over, and the session is set up with the Ks key between the A and B parties (Fig. 3).

One of the most important risks in this way is the risk of a repeat attack. Because a third-party interrupt can intercept messages between user A and server B without any understanding of its exact content and then re-run them.

There are two solutions to deal with security breaches:

The first solution is to insert "timestamp" in order to detect the novelty of the message from old and repetitive messages. The second solution is to insert a nonce in each message, and the receiver will check for repeatability by receiving each message and referring to the file history file. The best solution is to combine the two top solutions. In

this way, only buffered receivable strings should be stored that have timelines, which would require less capacity than the receiver buffer.

3. Needham-Schroeder authentication mechanism

The protocol was introduced in 1978 with developing modern security techniques, by Roger Needham and Michael Schroeder. This protocol is also based on the concept of challenge and response and needs a key distribution center (KDC). Initially, user A sends its ID (A), B server user ID, and a random string of RA to the KDC center. The KDC center generates a data structure with the following five items and encrypts it with a user key A (KA (RA, B, Ks, KB (A, Ks)) and sends it:

The RA intended to restore it, is to ensure that the user A is satisfied that the message is current and not eavesdropped; the B server ID must be used during the session:

KB (A, Kx), which is the result of the encryption of the user ID A and the session key, which is encrypted with the secret key of server B, and naturally the user A and no one else can use it.

The above item that user A has to submit to the B server is called the ticket. The role of the KDC will end after the ticket is issued.

User A decrypts it with its secret key after receiving items from the KDC and sends the ticket to the server using Ks (RA2), which is the result of encryption of another random string with the session key.

The B server is the only one who can unblock the ticket. By decoding the ticket, the B server identifies the user A and gains the session key. By extracting Ks, server B can also decrypt the RAs value. Now, for the B server to authenticate itself to user A, the RAS random string is reduced to a unit and encrypted with the Ks key and sends RR to the user A along with the random string. Now, user A decodes Ks (RA-1) and adds a unit to it that its message is exactly in response to the current demand and is not duplicated. Note that because a single RAS unit is diminished, the message is not being eavesdropped and retransmitted by the interrupter. Eventually, user A proves the active presence of server B by reducing one unit of RB and encrypt it with the key Ks, and the server B assures that the third message does not belong to previous and repeated times (Fig. 4).

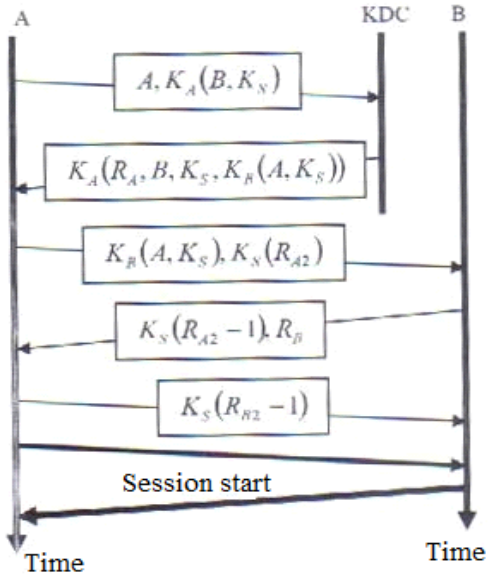

Figure 4: Needham-Schroeder Authentication Method (Stallings, 2005)

It is worth noting that the role of KDC in this protocol is very short and useful and will not cause traffic jams on the network. However, it should be carefully protected, since the collapse or infiltration of KDC will endanger all users and service providers. In this protocol, if the eavesdropper and Ks (which are usually

disposable and each time they change, and generally, people and software do not care about it), can trigger a repeat attack from the third stage.

4. Authentication mechanism with Kerberos

Kerberos belongs to the mid-80s. The fifth version of Kerberos also received the IETF in 2005 as a support Internet-based document. The main components in Kerberos are:

A. Server A (Authentication Server)

Each user at the first login stage, the login process, is required to prove his identity to this server.

B. Ticket Granting Server (TGS)

This server exported (tickets) for receiving any kind of service from servers at the quasi-level.

C. Server

After receiving the ticket, the server will provide a special service to the customer. The number of these servers is high.

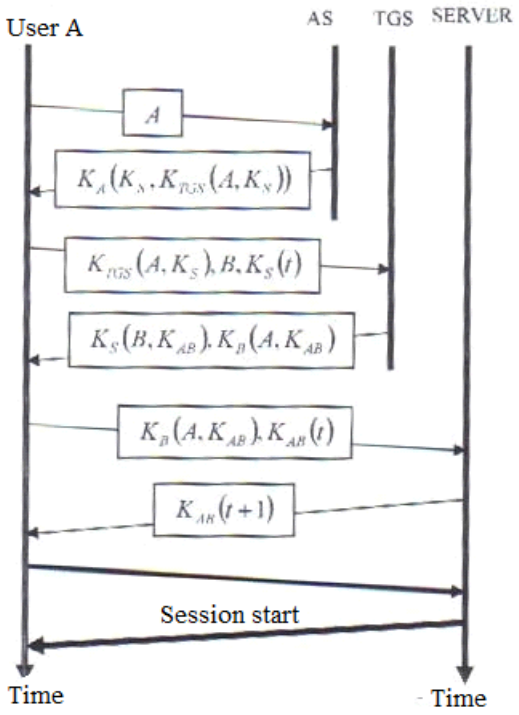

Figure 5: General of Kerberos Authentication Protocol (Kang et al., 2011)

In the fifth version of Kerberos, each ticket issued by the TGS server has the following contents:

1. User ID/Login ID 2. Symbolic Server Name 3. Client Machine Address 4. Key Session 5. Ticket Validity Time 6. Time Stamp

Advantages of the 5th version of Kerberos compared to previous versions:

- For Kerberos to be able to expand on a very large network, the entire network has been tried in a hierarchical manner in multiple domains, each domain for its own stylish TGS, AS server, which is responsible for users of their territory.
- In the fifth version, unlike previous versions, the ASN.1 notation language was used to describe the data and encode them. In the fifth edition, we tried to decode the DES dependency and allow symmetric encryption to be used in the system. The fifth version of Kerberos has been tested in an environment of over 28,000 users and its effectiveness has been proven.

As stated, Kerberos provides credibility and identity authentication services, and exchange session key KAB was raised between the user and the server. This key can be used by the user for the confidentiality and integrity of the communication. So the Kerberos system provides two types of messages. The KRB-PRIV

message is intended to protect the security (confidentiality) of the communication and KRB-SAFE message is to protect the integrity of communications.

5. Authentication mechanism using public key encryption

Whenever a public key can be accessed in a secure way, authentication can be implemented in a simpler manner based on the public encryption. For example, you can use digital certification and the PKI system to apply this method. The procedure for this method is as follows:

1. Initially, user A of the public-key distribution server requests to receive a B-server. Whenever a PKI-based system is established, it can validate it by obtaining a digital certificate issued to the B server, and then obtain the public key of the B server from within the certificate, with the help of it, encrypts the information and sends it to the B service.
2. User A submits its user ID and a random number of RA in a given data structure and with the help of the public key, the server will encrypt and send B server. Obviously, no one other than B can decrypt this message.
3. After decoding the third message, the server B extracts its user key A with its own private key and its challenge string, and because it needs a public key to respond to user A, so it asks for a public key distribution server or user A certificate.
4. After receiving public key or user certificate A, the conditions for sending encryption information are provided.
5. In this message, the B-server has three items: RA-A challenge string sent by the user ARB, its own challenge string KB, the session key to use it in symmetric encryption of the data in a given data structure and the result is encrypted with the public key by the user A and sends it back to it. Naturally, the only person who is able to decrypt and retrieve these items will be the user of A.
6. User A decodes the data first by examining the RA and comparing it with the challenge string to the conclusion that this response exactly matches its request or no. In this way, the new message is proven and a repeat attack is prevented. Now, by encrypting the RB with the session KB key, it must prove to the B server that it is also an active and actual user and the third message is not a duplicate message. This will start the session between B and user A with session key Ks.

In all of the proposed methods, the most commonly used mechanisms in computer networks and e-commerce are the combinations of Kerberos V5 and the use of public keys (asymmetric) such as RSA that increasingly increase the security of the Kerberos V5 method. The overall purpose of this article was to achieve secure methods to ensure correct communication and data exchange.

References

1. Andrew S. (2003). tanenbaum,Computer Network,Forth Edition,Prentice-Hall.
2. Kang, D. J., Lee, J. J., Kim, B. H., & Hur, D. (2011). Proposal strategies of key management for data encryption in SCADA network of electric power systems. International Journal of Electrical Power & Energy Systems, 33(9), 1521-1526.
3. Roger Needham, Michael Burrows,martin Abadi, (1990). A Logical of Authentication;ACM Transaction on Computer System,Vol8,No.1.
4. Stallings W., (2005). Cryptography and Network Security. 4th ed. Englewood Cliffs, NJ, USA: Prentice Hall.