TEST Engineering & Management

July-August 2020
ISSN:0193-4120 Page No. 3949 - 3953

Impact of Kerberos Authentication Technology In Security Services Of Computer Networks

Rana Ali Salim
Fine Art institution, Ministry of Education – Baghdad –Iraq ; E-mail: raname78@yahoo.com

Article Info
Volume 83
Page Number: 3949 - 3953
Publication Issue:
July - August 2020

Article History
Article Received: *06 June 2020*
Revised: *29 June 2020*
Accepted: *14 July 2020*
Publication: *30 August 2020*

Abstract:
The literal codes used to send telegraph messages, using standard sequences "long or short dashes" that can be formed by dots or oblique signs, were used in most high-speed communications, where they can be formed through sounds as well, and it is one of the codes The devices do not read it and the person must decode it by himself. The international Encryption code also includes characters, and the previous table shows a list of codes corresponding to each letter, written from right to left. Encryption code was used anciently in wireless communications, telegrams, and marine navigation, as this code was based on a simple principle which is to convert electrical signals transmitted through lightning lines into long and short sound clips so that long sections are converted into a condition and short are points, which in turn are later translated into letters understandable words. use of Encryption code is now limited by some hobbyists, but you can also create a complete sentence using long or short dots and dashes corresponding to latin and letters.

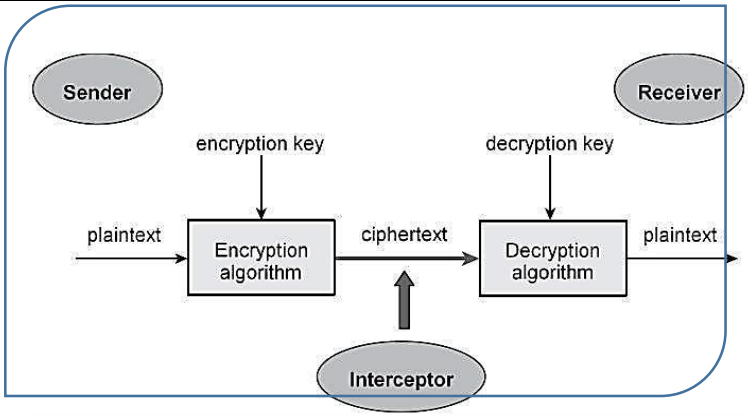
Keywords: *Asymmetric Authentication Systems, Certified Encryption, key to decrypt, Symmetrical Algorithm*

I.INTRODUCTION

Nobody denies the importance of encryption, especially with the spread of hackers and theft of personal information all over the world; The program that is in our hands is one of the programs that proved its worth and its amazing resilience in front of most attempts to break its encryption, and perhaps the most important feature of this program is that it uses a 128-bit key encryption, which prevents America from using it outside.

The certificate encryption process; obtain the certificate and the public and private keys from the CA; party that encodes the CA. data on the public key CA. for a receiver from itself or from the data. The encoder In the world of computing, encryption is the conversion of data from a readable form to a coded form that can only be read or processed after decoded. Encryption is the basic building block of data security and is the simplest and most important way to ensure that computer system information is not stolen or read by someone AAS who wants to use it for nefarious purposes. Individual users and large corporations use encryption, as it is widely used on the Internet to KD information may include anything from payment data to personal information.

Usually companies of all sizes use encryption to protect sensitive data on their servers and databases. The need for encryption In addition to the clear benefit of protecting private information from theft or hacking, encryption also provides a way to prove that the RSA to verify the origin of a message and ensure that it was not modified during the transmission.



They are the most difficult and needing to focus, because you play with letters more than you decode. The word 'digraph' in Latin means two letters that together form a single sound, which is what happens when decoding the digraph actually, where one writes the Latin or Arabic letters as pairs of letters and not Single letters, thus trying to encode each pair of letters with another pair.

As in the picture, the letters appear as pairs, each of which corresponds to one of the coded letters, and if you want to decode, you must draw a table of approximately five rows and five columns if you deal with the Latin language, and fill in the first blanks with the word "Key" or "Keyword" ", Which is the word that only you and your communicator must know and follow in Latin letters to fill in the table

II.LITERATURE REVIEW

The installation process is easy and he will ask you about the programs that he wil add himself to, such as Outlook, for example; have the option here to add whatever.

2.1 A study of J. G. Steiner, B. C. Neuman, and J. I. Schiller, To ware that after completing the setup, you must choose the your you that you created choose another; When choosing a new key, the program will ask you about your email shaping

TEST Engineering & Management

July-August 2020
ISSN:0193-4120 Page No. 3949 - 3953

this The key enter it and then you will be asked to enter the key and set the password.
2.2 A study of Stuart G. Stubblebine and Virgil D. Gligor, (On Message Integrity in Cryptographic Protocols, 2016). To display the enter it and confirm it here, and you can use a maximum of eight characters, preferably consisting of small and large letters, symbols and numbers, so that it is impossible to break them; like this (@ #%! * ||), and here is the process of forming your private key knowing that it allows you to configure more than one key. This is what distinguishes it from other similar encryption programs; can also change the password easily from Key Properties the program now.

3. Research and Information Collecting:
- Aims, Objective of Research:
1. Client should server don't initial encryption key; Whenever client authenticates itself to a new verifier.
2. To relies the authentication server for generate a new encryption key
3. To distribute it securely to both sides.

3.1 Kerberos Model:
When the other end receives the encrypted file, it must decrypt in the same way that the file was encrypted, i.e. assuming that the first party did the following to encode the file: use 13 type, B method, the second party must use the same method. When decrypting a file, in the file input field you put the encrypted file, and in the output file the file after decoding, do not forget that you must know the actual file extension of the decrypted file, before you can open it. The presence of the word SFX Extra Self in encryption programs means that there is no need to have a program to decrypt the file at the receiving end of the encrypted file. With this feature, the encrypted file is an exe file that can be decrypted by entering the password as shown in Fig,(1) and (2) below:

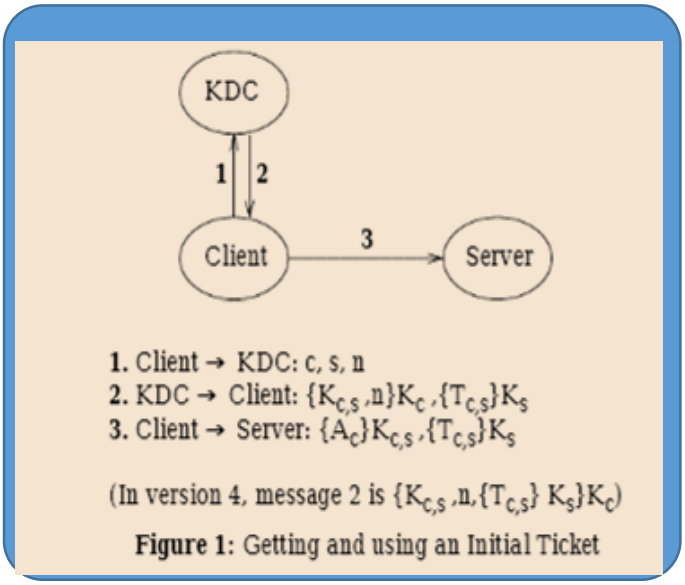


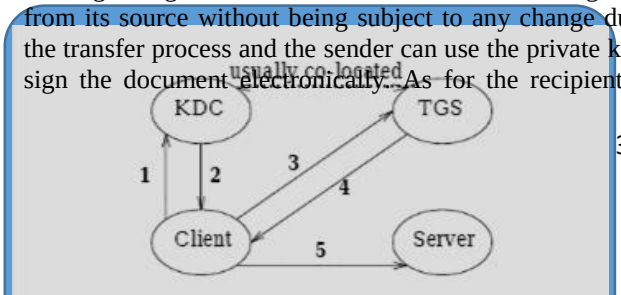
Figure 1: Getting and using an Initial Ticket

When the other end receives the encrypted file, it must decrypt in the same way that the file was encrypted, i.e. assuming that the first party did the following to encode the file: use 13 type, B method, the second party must use the same method. When decrypting a file, in the file input field you put the encrypted file, and in the output file the file after decoding, do not forget that you must know the actual file extension of the decrypted file, before you can open it. The presence of the word SFX - Extrat Self in encryption programs means that there is no need to have a program to decrypt the file at the receiving end of the encrypted file. With this feature, the encrypted file is an exe file that can be decrypted by entering the password and only. Some programs that support this feature: AxCrypt;

3.2 Initial Ticket Exchange, & Environmental Shortcome: With increased reliance risks over of it. the of giant espionage run and its allies in Britain and Australia. Recently, the United States passed a law authorizing spying on individual correspondence without legal permission, which increases correspondence companies, as full, safe and ideal service in the normal state, raised most important misuse.
3.3 Use of Encryption and Technical Deficiency: The message may be confidential and the sender and the recipient do not want their content to leak, and during the course may spy on it. Unfortunately, in the regular use of e-mail, any server through which the message passes through can spy on it, and even copy it, as simple as possible. *Impersonation: A person sends messages impersonating a person's name and to another person, and the messages reach the third person so he believes they are from the second person and treats them as such. Unfortunately, it is practically impossible to prevent anyone name anyone else as example, anyone modify that he uses to show his messages as if they were issued by the infidel Bush. *Changing was issued by authority, possible those who intercept it to amend it, for example, cause an effect on the future. Also, this threat is present in the case.

III.METHODOLOGY

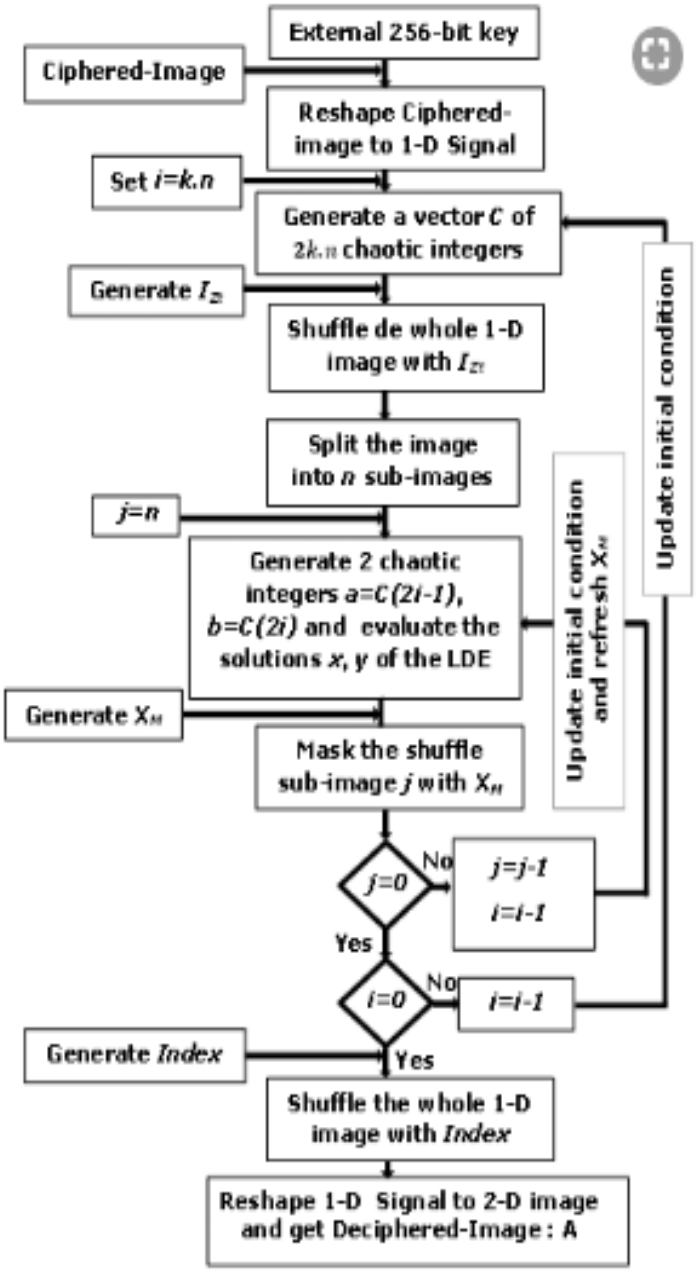
The digital signature is used to ensure that the message came from its source without being subject to any change during the transfer process and the sender can use the private key to sign the document electronically. As for the recipient, the



Published by: The Mattingley Publishing Co., Inc.

July-August 2020
ISSN:0193-4120 Page No. 3949 - 3953

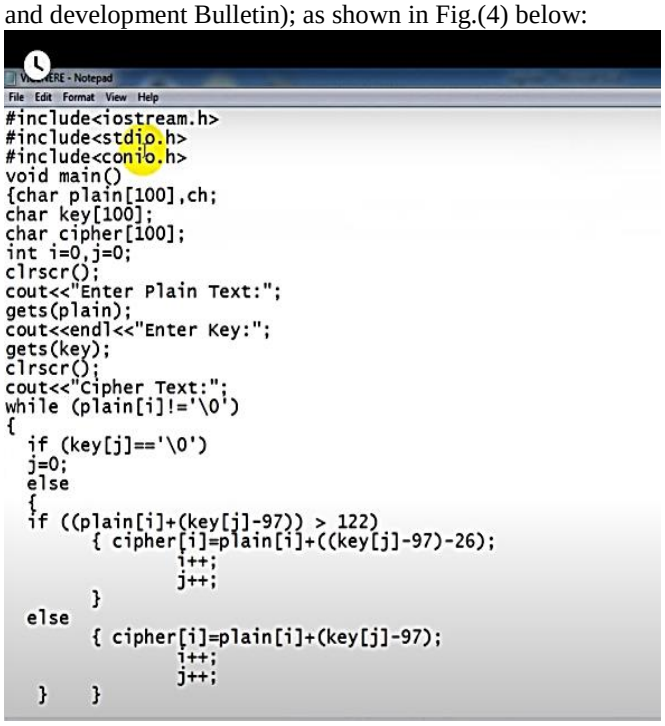
signature is verified by using the appropriate public key; as shown in fig.(3) below:



3.1 Authentication and Reply Detection: More than one way in which one can create different passwords, so that each of us creates his own word that expresses his personality a lot, whether it is a comic password that expresses his sarcasm, or whether a password in different languages is written in the languages he can master However, there is a whole life behind passwords or behind the concept of encryption in the first place. We have brought you the most popular methods humans have used to communicate with codes.

Hide the meanings of important messages has been around for thousands of years, and so they found many complex ways to encrypt their messages and hide their meanings, so that the way to solve or decipher the code varies depending on the complexity of the code itself.

3.2 Network Address: There is a difference between the code and writing the code, in the case of the code, every word written in it symbolizes another code or another example, whereas in writing the code, every letter in the code symbolizes another letter Or to a different code, except that the code is encoded and the code is encoded differently. It used methods of deciphering codes and symbols to understand Greek and hieroglyphic myths (the ancient Egyptian language), the most famous of which was the "Rosetta Stone" for example, and it is the stone that gives the key to modern understanding of the hieroglyphic language after its discovery in the city of "Memphis" in the Egyptian Delta and its translation for the first time from French scientist "Champollion transmission. (Quoted from the trade and development Bulletin); as shown in Fig.(4) below:

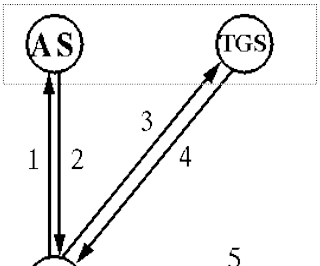


```
#include<iostream.h>
#include<stdio.h>
#include<conio.h>
void main()
{char plain[100],ch;
char key[100];
char cipher[100];
int i=0,j=0;
clrscr();
cout<<"Enter Plain Text:";
gets(plain);
cout<<endl<<"Enter Key:";
gets(key);
clrscr();
cout<<"Cipher Text:";
while (plain[i]!='\0')
{
  if (key[j]=='\0')
  j=0;
  else
  {
  if ((plain[i]+(key[j]-97)) > 122)
        { cipher[i]=plain[i]+((key[j]-97)-26);
                i++;
                j++;
        }
  else
        { cipher[i]=plain[i]+(key[j]-97);
                i++;
                j++;
   }    }
```

Fig.(4): Intact alterd during transmission

IV.RESULTS AND DISCUSSION

Most technology works; as mentioned earlier, the public key can be given to more than one user, assuming that the p. k., sent an unencrypted regular message that has public key How can the receiving party ensure, in this case the sending party when sending its message using the digital signature using the private key encrypts the signature only and not the message and then at the receiving party, In addition, this expectation is important to ensure that the message is intact, by doing a comparison of certain characteristics in the message to ensure that it has not been altered during the transfer process, which obvious noticed in Fig.(5) below:



Published by: The Mattingley Publishing Co., Inc.

July-August 2020
ISSN:0193-4120 Page No. 3949 - 3953

of regular use of e-mail. *Sending harmful or annoying content: such as viruses or malicious software of all kinds, or spam or advertisements paving online scams.

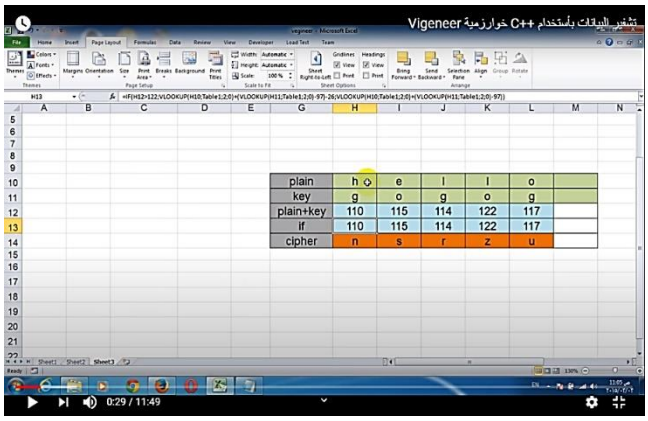


Fig.(6): Explore of Virus kinder detection process

Encryption has been used around protect its secret messages, and this use reached its climax during periods of warfare; For fear that sensitive messages will fall into the enemy's hands. Julius Caesar was one of the most famous ancient professions in cryptography, as he developed a cipher algorithm named after him Caesar Cipher; army chiefs.

Several encoding machines appeared, including the Enigma machine. In the early days of its appearance, the computer was method communications, that cryptographic research, and developing an a matter of controversy, and despite the reservations of the US government over its belief that companies and private institutions do not need coding systems, it has achieved a wide spread in the markets have been coding, highlighting process; as shown in Fig.(7) below:

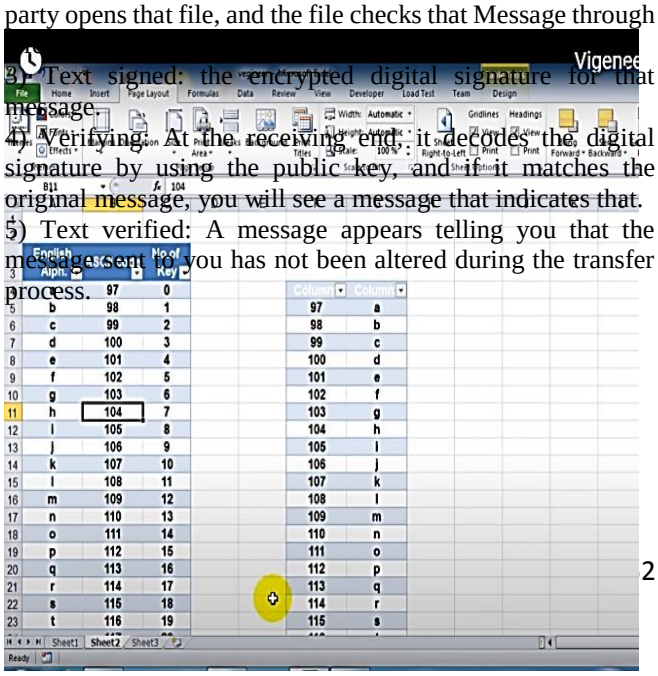
Among the most prominent institutions that contributed to this field is the National Institute of Standards and Technology- NIST, formerly known as the US National Bureau of Standards; this institute developed a standard called the Data Encryption Standard. (Data Encryption Standard- DES). This standard is based on the Lucifer algorithm algorithm, which uses a 56-bit encryption key, and requires that both the transmitter and receiver have the same secret key. The government used this official standard; and banks approved it to operate ATM machines.

V.CONCLUSION

These risks are all there is, and no one knows who will take advantage of them, when they might do so and for what reason. Even if you do not have enemies willing to pay for your harm, you may fall victim to a freak or a stinking seducer who prides himself on spying on your mail. Because of the nature of the Internet's work, it is often not possible to predict the path the message takes from the sender to the recipient, so whatever the technical security precautions the sender and the recipient, and the mail servers that use them, the possibility of the message being subjected to abuse on the road remains a possibility:

1) The text original: the unencrypted message, which will be sent normally to the receiving party.

2) Signing: the digital signature of the message by using the private key to encrypt the signature only, the digital signature can be sent as a file attached to the original message which is also in the form of an attached txt file, and then the receiving party opens that file, and the file checks that Message through



3) Text signed: the encrypted digital signature for that message.

4) Verifying: At the receiving end, it decodes the digital signature by using the public key, and if it matches the original message, you will see a message that indicates that.

5) Text verified: A message appears telling you that the message sent to you has not been altered during the transfer process.

July-August 2020
ISSN:0193-4120 Page No. 3949 - 3953

```
Public Function XOR_Encrypt(ByVal Input As String, ByVal pass As String) As Strin
    Dim out As New System.Text.StringBuilder
    Dim u As Integer
    For i As Integer = 0 To Input.Length - 1
        Dim tmp As String = Hex(Asc(Input(i)) Xor Asc(pass(u)))
        If tmp.Length = 1 Then tmp = "0" & tmp
        out.Append(tmp)
        If u = pass.Length - 1 Then u = 0 Else u = u + 1
    Next
    Return out.ToString
End Function
Public Function XOR_Decrypt(ByVal Input As String, ByVal pass As String) As Strin
    Dim out As New System.Text.StringBuilder
    Dim u As Integer
    For i As Integer = 0 To Input.Length - 1 Step +2
        Dim tmp As String = Chr(("&H" & Input.Substring(i, 2)) Xor Asc(pass(u)))
        out.Append(tmp)
        If u = pass.Length - 1 Then u = 0 Else u = u + 1
    Next
    Return out.ToString
End Function
```

REFERENCE

[1]. S. M. Bellovin and M. Merritt. Limitations of the kerberos authenication system. *Computer Communication Review*, 20(5):119-132, October 1990.

[2]. G. A. Champine, D. E. Geer, Jr., and W. N. Ruh. Project Athena as a distributed computer system. *IEEE Computer*, 23(9):40-51, September 1990.

[3]. S. Chokhani. Towards a national public key infrastructure. *IEEE Communications Magazine*, 32(9): 70-74, September 1994.

[4]. Computer Emergency Response Team. *Ongoing network monitoring attacks*. CERT Advisory CA-94:01, 3 February 1994.

[5]. CyberSafe Corporation. Deploying Kerberos for large organizations. Technical Report 94-47, CyberSafe Corporation, 1605 NW Sammamish Rd, Suite 310, Issaquah, WA 98027-5378 USA.

[6]. D. E. Denning and G. M. Sacco. Timestamps in key distribution protocols. *Communication of the ACM*, 24(8):533-536, August 1981.

[7]. W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644-654, November 1976.

[8]. B. Jaspan. Kerberos users' frequently asked questions. Periodically posted to Usenet newsgroup comp.protocols.kerberos, April 1994.

[9]. S. T. Kent. Internet privacy enhanced mail. *Communications of the ACM*, 36(8):48-60, August 1993.

[10]. J. T. Kohl and B. C. Neuman. The Kerberos network authentication service. Internet RFC 1510, September 1993.

[11]. J. T. Kohl, B. C. Neuman, and T. Y. T'so. The evolution of the Kerberos authentication system. In *Distributed Open Systems*, pages 78-94. IEEE Computer Society Press, 1994.

[12]. J. Linn. Generic security service application program interface. Internet RFC 1508, September 1993.

[13]. R. M. Needham and M. D. Schroeder. Using encryption for authentication in large networks of computers. *Communication of the ACM*, 21(12):993-999, December 1978.

[14]. B. C. Neuman. Proxy-based authorization and accounting for distributed systems. In *Proceedings of the 13th International Conference on Distributed Computing Systems*, pages 283-291, May 1993.

[15]. B. C. Neuman and S. G. Stubblebine. A note on the use of timestamps as nonces. *Operating Systems Review*, 27(2):10-14, April 1993.

[16]. R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 21(2):120-126, February 1978.

[17]. R. K. Smart. The X.509 extended file system. In *Proceedings of the ISOC Symposium on Network and Distributed System Security*, February 1994.

[18]. J. G. Steiner, B. C. Neuman, and J. I. Schiller. Kerberos: An authentication service for open network systems. In *Proceedings of the Winter 1988 Usenix Conference*, pages 191-201, February 1988.