Evaluating the Effectiveness of Using the Protection and Security of Information Systems in the National Organizations of Information Security

Abdelmajid Moh. Ali Alhwije

PhD,Candidate

Abstract- All organizations, staffs, foundations and universities in this age depend completely on information and data to convoy the technical and scientifically development, and as it's known today that this age we live in is called or known as the age of information or the age of technology , and we can say that having a greater amount of information means having control over several fields and the development of information systems has already done a huge qualitative leap in the field of information technology , it's preciseness , increasing it's productivity and exploiting machines for performing all works in foundations and some other organizations ,therefore foundations started aiming to get the biggest amount of information, thence negativity appeared in technology and penetration, piracy and data exchange in illegal way started to be called ; information technology crimes, as it is a phenomenon which has many effects over the political, martial, economical, and safety fields , therefore foundations, universities, organizations, information centers and some other administrations should protect their information and data from penetrating networks and information systems where they exchange these information and process them ,whether inside that foundation / center or through the world wide web.

Among these foundations which depend on information; research centers, information centers , universities , libraries and some other different foundations which have an informational uprising that should have been protected from piracy and theft . This study ought to evaluate the reality of using security and protection of information systems in the national organization of information security from stealing , penetration , messing up, robbery , or change which effects directly on the credibility of this foundation considering information and data the spinal column of this foundation .

Index Terms- protection, security, information systems, cryptography

I. Introduction

In today's business environment, security is a major problem in all areas. Hackers and invaders have done a number of successful attempts to lower top-level corporate networks and web services. Many methods have been developed for network infrastructures and Internet connections such as firewalls, encryption and virtual private networks. Discipline is a new addition to this technology. In recent years there have been methods of attack. Using intrusion detection methods, you can collect and use certain attack attacks and find out who is trying to attack the network or private hosts. Data collected in this way can be used for network security and for legal purposes. There are also much vulnerability in the market that contain various network holes, including firewalls that block unwanted signals and signaling systems (IDSs). This determines whether the device has attempted to use it. For this purpose, both commercial and open source products are available. Trusted security systems are needed to create trusted computing platforms (network-related components). In the design of the base system, a security policy has been developed, taking into account the measures taken to ensure the privacy and integrity of the system. The privacy situation in this context shows users access restrictions and is available to protect the data. Honesty means that the information in the system and system is working properly. Furthermore, the existence of the system must be maintained, it must remain unchanged while maintaining the integrity of the system, even if it operates at a user-friendly level.

II. Research problem

In as much as foundations , staffs , data centers , universities and some other administrations depend on information technology, increasing these techniques complexity , technological advance and information systems , all put these foundations , staffs and data centers , in more risks and expose them to stealing , and losing these important information puts foundations , staffs and information centers in a situation , especially if the security and protection of information systems application has been facing many difficulties, so this foundation would be more exposed to lose a maximum amount of their information and data, what makes them in a need for using security and protection of information systems .

III. Symmetric Cryptography

Symmetric key cryptography has two parts: power passwords and password blocking. Stream chips are like a one-pad, but it provides security for a relatively small and controlled key. The key extends for a long period of time, which is then used as a one-off platform.

Blocking is based on the coding code concept where the code identifies the key code. The privacy block algorithms can be very scary. Passwords that are internally blocked also use confusion and diffusion.

There is a two-way encryption algorithm. Of these algorithms AS / 1 and RC4.Bit are widely used today, while AS / 1 works on GSM mobile phones. The AS / 1 algorithm represent the class of hardware-based large stream chips. RC4s use multiple places as well as Secure Layer or SSL and it is almost the only one with the current password because RC4 is powerful in software.

Blocked password DES (because of the relatively simplified block encryption standards), all these are block passwords that need to be compared.

Stream ciphers

The current length passes through the n keys of the bits k and extends to the remote key current. This key is then handled by p-text p to create encrypted text with XOR-ed. Using the mainstream is the same as using a disposable password. The same key current is created with a stream password to open a password and XOR-ed encrypted text.

Stream encryption function Stream chip (k) = S, where the key is the switch and the C key flow. Encryption Formula:

$$Co = po \oplus so.c1 = p1 \oplus s1.c2 = p2 \oplus s2\ldots\ldots$$

Where P= po $\oplus$ p2.....is the plaintext. S= so $\oplus$ s2..... is the key stream and C=co $\oplus$ c2 ... .is the cipher text. To decrypt cipher text C, the key stream S is again used.

$$Co = co \oplus so.p1 = c1 \oplus s1.p2 = c2 \oplus s2\ldots\ldots$$

Provided that both the sender and receiver have the same stream cipher algorithm and that both know the key k.

A5/1

A5 / 1 - Current passwords used by mobile phones to protect privacy. This algorithm
There is an algebraic description. AS / 1 uses three linear feedback shift registers [...] or LFSRs with symbols (X, Y, Z. X , x1, x2, ... x18).

Registered Y 22 bits (y0, y1, y2….. y21) and Z 23 bits (z0, z1, z2, ….. z22). Thus, three LFSRs have a total of 64 bits.
It is no coincidence that the key is k - 64 bits. The key is used as the first filler for the first registrant. We are prepared to produce the main stream only after the three recipe has been given. However, we must first discuss X, Y and Z registers.
In step X the following are:

$$t = x13 \oplus x16 \oplus x17 \oplus x18$$
$$xi = xi-1 \quad \text{for } I = 18,17,16\ldots\ldots\ldots 1$$
$$x0 = t$$

Similarly, for registers Y and Z, each step consists of

$$t = y20 \oplus y21$$
$$yi = yi-1 \quad \text{for } i = 21,20,19\ldots\ldots 1$$
$$y0 = t$$

and

t= z7 ⊕ z20 ⊕ z21 ⊕ z22
zi= zi-1 for i=22,21,20……1
z0=t

Respectively.

If x, y, and z are three, the function returns 0 if x, y, and z are zero on Return 1.
Used for A5 / 1 hardware and for every hour to mix the value

M= maj(x8, y10, z10)
is computed. Then the registers x, y, and z step according to the following rules:

if x8= m then X steps
if y10= m then Y steps
if z10= m then Z steps

Finally, a key stream bit s generated as:

S= x18 ⊕ y21 ⊕ z22
This is then XORed with the plaintext (if encrypting) or XOR-ed with the cipher text (if decrypting).

RC4

RC4 codecs is unlike A5 / 1. For A5 / 1 RC4s it is optimized for software development and RC4 is the primary byte at each stage and A5 / 1 produce only one key stream.

The RC4 algorithm is very simple because it resembles a table that contains 256 bytes location. Whenever the basic validity of each input stream is created, the functional actuator is constantly changing, so the table always has its own place (0, 1, 2, ..., 255).
All RC4 algorithms are based on bytes. The first step in the algorithm triggers the spreadsheet with the key. This switch is i = 0, 1 ... N-1,

Table 4.1. RC4 initialization

```
For I = 0 to 255
S[i]=i
K[I]=key[I mod N]
Next i
J=0
For I = 0 to 255
J= (j+S[i] + K[i] mod 256)
Swap(S[i].S[j])
Next i
 I=j=0
```

Each button [i] is a byte and S (i) is a lookup table for each S [i]. Table (2) in the table shows the pseudo-code for the P-permutation of activation.

Interesting features in RC4 are that the key can be longer than 256 bytes. The key is used only to initiate P rights.

After the start-up phase, each key stage flask is given in accordance with the table (3) algorithm, which is the main stream. Byte is a byte with XOR-ed, open text (encryption), or XOR-ed, encrypted text (open passwords). The RC4 output can also be used as a pseudo-random digital generator for applications requiring pseudo random numbers of "cryptographic" (i.e. presumably).
The RC4 algorithm you can look for as a changing lookup table is smart and powerful software. However, the attack is available for specific purposes

RC4 [.............], but we cannot attack if we remove the first 256 bytes of bytes. This can be accomplished by adding up to 256 stages to the output stage, in which each step generates and interrupts the key byte after the table 3 algorithm.
RC4 is used in many applications, such as SSL. However, the algorithm is not very optimized for older and 32-bit processors.
Table 4.2. RC4 key stream byte

i = (I+ 1) mod 256
j = (j + S[i]) mod 256
Swap(S[i] .S[j])
t=(S[i] + S[j]) mod 256
KeystreamByte = S[t]

Block Ciphers

Blocks encrypted blocks blocking plain text in solid format and creates encrypted text in a solid size. The encrypted text is separated from the text. Repeat an F-type F functions.

Function F, which is dependent on the K and K buttons of the previous type, is referred to as round operations because it is used in each type, not in its forms.

Blocked items are security and efficiency. Developing secure passwords or powerful algorithms is not a challenging task, but it is surprising to design very secure and encrypted passwords.

Feistel Cypher

Feistel encoders are, in principle, general password design, but no special passwords, but Feistel passwords for block passwords. The Feistel P text is divided into the left and right pieces.
P =(LO. RO),
And for each round i =1,2 .... n new left and right halves are computed according to the rule

Li= Ri-1 (3.1)

RI=Li-l $\oplus$ F(Ri-l.Ki) (3.2)

That is the sub key for the round. The sub key is derived from the K key according to the keypad algorithm. Finally, C is the final outcome.
C = (Ln. Rn).
Feistline encryption is a barber that is, we have the password to decompile whatever F function. We resolve the equations 1 and 2 for R-1 and Li-1 and return the process
Ri-1 = Li
Li-I = Ri $\oplus$ F (Ri-1, Ki)
And the final results is the original plaintext P = (LO. RO).

All circular functions work in Feistel encryption if F's output is the correct number of bits. In particular, function F must not be altered. For example, for all Ri-1 and Ki F (Ri-1 Ki) = 0, we have "encoding" and "password" with this F but encrypted is not really safe. The advantage of Feistel encryption is that all security equations suspect circular activity. Thus, the analysis can focus on F.

DES

DES, the Data Encryption Standard was developed in the 1970's. The design is based on the Feistel code developed by IBM, based on the Focus Codes. DES is simply a simple block identifier.

By mid-1970s, the US government became clear that secure encryption was justified by the commercial need. Volume and sensitivity over time and digital data, the computer revolution grew rapidly. The National Secret Security Agency or NSA Secret Agent did not want to contact DES, but ultimately accepted the study and dissemination of Lucifer models. All of this was secretly made and the data became popular later. Most suspected that the NSA had set a "tailgate" for DES, so it could simply interfere with the password. Of course, the NSA's SIGINT operation and the general lack of trust in the government have raised such fears. But for 30 years, it has not been opened to the back door for intense cryptanalysis. However, these doubts started with DNA itself.

Lucifer was finally des, but not the least, and some of them were not so subtle. The biggest change is that the key length is reduced from 128 to 64 bits. However, eight 64-bit bits were thrown, so the actual key length is only 56 bits.

As a result of these modifications, the expected work required for a brute force exhaustive key search was reduced from 2^{127} to 2^{55}. By this measure, DES is 2^{72} times easier to break than Lucifer!

The obvious, suspicious thing is that the NSA has been involved in this case. However, subsequent cryptanalysis of the DES algorithm detected shocks that required less effort than tests 2^{55}. As a result, DES may have about 56 key keys because it may be a longer key.

Subtle modifications to Lucifer include change boxes or S-boxes. In particular, these changes led to a suspect in the back room. But time goes by, it seems clear that many years later the changes to the S boxes enhanced the algorithm by protecting unknown cryptanalyses.
In summary,

- DES 16 different Feistel passwords;
- DES has a 64-bit block length;
- DES uses a 56-bit key; Each DES-type contains a 48-bit sub key, and each sub key consists of a 48-bit 56-bit key.

IV. Hash Function

The spreading function (used in data structures and algorithms) takes lines from arbitrary lengths and shortens them into shorter rows. In data structures, these shortcuts can be used as an index in the table: hash function is too short. Fourthly, the hash function requires fewer contradictions (as in every table, only a few elements run out).

The cryptographic spreading function h (x) should provide:

- Packaging: any input x size, output length = h (x) is very small. In practice, the cryptographic spread function generates fixed size costs regardless of the feed length.
- Function: All inputs x, h (x) should be easy to calculate. When calculating H (x), the computational motion increases with x length, but not too fast.
- Unidirectional: x (x) = The value of y cannot be calculated taking into account any y value. Another way to say this is to overestimate the difficulty.
- Weak Impact Resistance: For x and h (x) it is difficult to find y-x such as y (x) = h (x).
- Greater crash resistance: It is difficult to find x and y xi-y and x (x) = h (y).

Output fields should be present because the input field is larger than the free space. For example, suppose that the spread function generates a 128-bit output. If the value of this estimate reaches any output, all access values are up to about 150 gigabytes on average, over 2^{22} or over 4,000,000. And copy 150-bit entries. Collision prevention features require that all of these conflicts (with all others) are difficult to find. Importantly, there are cryptographic hash functions.

Hash functions are very useful for security purposes. The important use of Hash is to calculate a digital signature. If Alice uses a "special" key for coding, that is, he calculates S = [M] Alis. If Alice M and Sni send it to Bob then Normal M = {S} can confirm the signatures by confirming Alice. However, if M is larger, [M] Alice pays an estimate that is not the bandwidth used to send the same size M and C.

Assume that Alice has a cryptographic spread function. M (M) file can be considered "fingerprint". This is less than H (M) Mbit. M. If M is different from one or more "min", it can be assumed that about half of h (M) and h (M ') can be expected. Alice S = [h (M)] under signing you can login and send Bob M and S. (M) = {SJ Alice.

What are the benefits of a signature (M) instead of M? For example, expensive private view features should only apply to small fingerprints (M) instead of the entire file. Greater M and more efficient h (M) the funds are so large. Additionally, when you send multiple attachments to Alice, the bandwidth is stored.

Non-Cryptographic Hashes

To understand a specific cryptographic hash function, first consider a few simple non-cryptographic hashes. Suppose the input data is

X = (XO, Xl, X2 .... , Xn-1)

where each Xi is a byte. We can define a hash function h(X) by

h(X) = (XO + Xl + X2 + - - - - + Xn-1) mod 256.

This, of course, impresses as the input of any size is compressed into 8 bits. But this would not be safe, because if we mix directly with 2x4 = 16. For example

h(10101010,0000,1111) = h(0000,1111,10101010) = 10111001.

The length of the hash is not very short, but has many algebraic structures. As an example of a non-cryptographic hash, look at the following. Again, data is written as bytes

X = (X0, XI, X2 ... Xn-1).

Here, we'll define the hash h(x) as

h(X) = nX0 + (n-1) X1 + (n-2)X2 + ... +2Xn-2 + Xn-1 mod 256.

Is this hash secure? At least it gives different results when two bytes are swapped, for example, h(0000001,00001111) $\neq$ h(00000000,00010001)= 00010001 .

Although this is not a trusted cryptographic hash, it is used successfully in a non-cryptographic program [...].

One of the common methods for non-cryptographic "hash" is a cyclical surveillance or CRC [...]. These calculations are basically a long time interval and the remainder is CRC. The default long term division is used to substitute the difference XR value.

By choosing this distributor, it's easy to find clashes and actually make collisions easier with any CRC system [...]. CRCs are sometimes used in applications that require cryptographic integrity (incorrect). For example, WEP [.....] uses cryptographic compositions to match the more consistent CRC checksum. CRC and its equalization methods are intended solely to detect transmission errors - not to disclose information unintentionally.

- Efficiency problems. The spreading function can be calculated by applying a single input to the input, while retaining certain data. It is also very powerful for large files.
- Applies to Hash functions. Today MD5 and SHA-1 are the most resilient for hash functions. Its capacity is 160 bits.

V. Popular Uses of Collision-Resistant Hash Functions

In practice, the password used to log on is required. If this file is stolen, all user passwords should be opened. In Unix, this problem solves the password only with the required passwords. That is, any input included on the desktop (usher h (pwdi)) with the lock-resistant hash function.

The structure of this structure, as we have seen, is a one-way approach to the conflict of the clash traditions. Therefore, getting a password file does not specify the passwords needed to log in. (Remember that Hw (pwdi) information does not help access the server, because the host waits for host pwdi and h (pwdi).)

VI. Conclusion

Our system generates enough keys; It can generate different keys for different applications; Supports withdrawal; Its security document is based on extensive research in software development and in statistical discussions under subordinates; And we have shown that it is less than half of the wrong diagnosis.

An advanced sophisticated system with two subsystems and a biometric separation system has been created to authenticate and create keys. The purpose of the first subsystem is to identify people based on biometric data. The validation of the service recognition system is carried out. The execution is controlled by parameter FRR (false encryption) and parameter difference (incorrect). The results are as follows: FRR = 0.37 and Far = 0%. Selected parts by IRSA-iris segmentation did not produce good results.

The second subsystem is responsible for developing a cryptographic key creation system. The maximum length of the key is 150 bits for the smallest FRRs and FARs. Performance and individual systems are certified with parameters FRA and LP. The results are as follows: FRR = 1.35 and Far = 0%.

Authentication and key systems have competed with Daugmans biometric key generations. In the "Biometric Effective Crypton" combination, the authors note that the key length of FRR = 0.47 and FAR = 0 is 140 bits.

VII. Further work

The main idea for future business is to develop systems that use biometric errors to create key PKI keys. He has thoroughly studied IBM's information acquisition methods and public key production mechanisms. Photos are in RGB format. Thus, in view of the large amount of data, the length of the normal PKI key is large. The results confirm the validity of the proposed solutions.
Another idea for the future is to develop a multimedia content protection system for biometric data using cryptographic protection. Using biometric information such as a key may prevent access to unauthorized use of copyrighted material. A combination of symmetrical and asymmetrical keys used for this purpose. The proposed method can fill the system to create a water cylinder.
The latest offer for the next job is the development of a digital content management system, DRM - Digital Rights Management. System-based and identification methods that incorporate DRM are based on iris biometric data systems. The victims of the system distinguish between protection and individuality. The purpose of the system is to separate customers from illegal users, so only authorized customers have access to digital content.

References

[1] R. Wildes. Iris recognition: an emerging biometric technology. Proceedings of the IEEE, Vol. 85, No. 9, 1997.

[2] Adnan Awad , research methodology , Jordan ,ubited Arab company for publishing , 2008 , Abdulhamid Basiony , protection from internet dangers, dar al-kutub for oublishing and distibution , 2003 .

[3] Andrew S Tanenbaum. "Distributed Systems Principles and Paradigms" . Prentice Hall, 2002.

[4] Andrew S Tanenbaum.(2003) "Computer Networks" . Prentice Hall, 4th edition edition.

[5] Apama Vattikonda and Ranjit Kumar Gampa.(2002. "Intrusion Detection In Wireless Networks,term paper.

[6] Arabic club for information . modern information systems , demascus ,national information center printing house , 2000.

[7] Aree Karim , managment of information systems in organizations , faculty of economic sand social sciences , Agad university , Norway , 2007 .

[8] Auer P. & Warmuth M, (1998). "Tracking the Best Disjunction. Machine Learning" 32:127-150.

[9] Base, Rebecca "Intrusion Detection Systems". Washington, DC: National Institute of Standards and Technology.

[10] Begzo Balka Guru ,security of information systems , readiness and auditor (case study) ethiopian ngos 2011 .

[11] Buhan, J. Doumen, P. Hartel, and R. Veldhuis, (2007) "Fuzzy extractors for cominuous distributions," in Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security (ASIACCS '07), pp. 353-355, Singapore.

[12] Cannady, J.,(1998), "Artificial Neural Networks for Misuse Detection," Proceedings, National Information Systems Security Conference (NISSC'98), October, Arlington,

[13] Cavoukian and A. Stoianov, (2007) "Biometric encryption: a positive-sum technology that achieves strong authentication, security and privacy".

[14] CERT Advisory CA-1998-01 "Smurf IP Denial-of-Service Attacks".

[15] CERT the U.S. Patent and Trademark Office

[16] Charlie Scott, Paul Wolfe, and Bert Hayes,. Snort for dummies, page 27. Wiley Publishing, Inc., Indianapolis, India (2004).

[17] CRESCENZO, G. D., GHOSH, A., AND TALPADE, R. Towards a theory of intrusion detection. In 10th European Symposium on Research in Computer Security ESORICS (2005), pp. 267-286.

[18] DENNING D. E. "An intrusion-detection model". IEEE Transactions on Software Engineering, Special issue on computer security and privacy vol. 13- 2, pp 222-232, (Feb. 1987),.

[19] Denning, Dorothy. (February, 1987). "An Intrusion-Detection Model". IEEE Transactions on Software Engineering, Vol. SE-13, No. 2.

[20] Dittrich, Dave. "NANOG ISPSec Meeting/DDoS BoF". 7 February, 2000.

[21] E. Wolff. Anatomy of the Eye and Orbit. 7th edition. H.K. Lewis & Co. LTD, 1976.

[22] Endorf C. F., Schultz E., Mellander J 9. (2005). "Intrusion Detection & Prevention",page,56,163.

[23] Endorf C. F., Schultz E., Mellander J, "Intrusion Detection & Prevention", page 69-70, (2005).

[24] Endorf C. F., Schultz E., Mellander J. "Intrusion Detection & Prevention", page,, 52. 2005.

[25] Endorf C. F., Schultz E., Mellander J. "Intrusion Detection & Prevention", page,, 60-63 2005.

[26] ESKIN, E., ARNOLD, A., PRERAU, M., PORTNOY, L., AND STOLFO, S. "A geometric Frame work for unsupervised anomaly detection: Detecting intrusions in unlabeled data. In Applications of Data Mining in Computer Security" (2002).

[27] F. Hao and C.W. Chan, "Private Key Generation from On-Line Handwritten Signatures," Information Management & Computer Security, vol. 10, no. 2, pp.159-164, 2002.

[28] F. Monrose, M.K. Reiter, and R. Wetzel, "Password Hardening Based on Keystroke Dynamics," Proc. Sixth A CM Conj Computer and Comm. Security (CCCS), 1999.

[29] F. Monrose, M.K. Reiter, Q. Li, and S. Wetzel, "Cryptographic Key Generation from Voice," Proc. 2001 IEEE Symp. Security and Privacy, May 2001.

[30] F.Hao, R.Anderson, J.Daugman, ,,Combining Crypto with Biometrics Effectively", IEEE Transactions on Computers, Vol.55, No.9, September 2006.

[31] GHOSH, A. K., AND SCHWARTZBARD, A. "A study in using neural networks for anomaly and misuse detection", In Proceedings of the 8th conference on USENIX Security Symposium Volume 8 (1999), SSYM'99, pp. 12-12.

[32] GUYON, I., GUNN, S., NIKRAVESH, M., AND ZADEH, L."Feature Extraction: Foundations and Applications" (Studies in Fuzziness and Soft Computing). Springer-Verlag New York, Inc., Secaucus, NJ, USA, (2006).

[33] H Venter and J Eloff. (2003). "A taxonomy for information security technologies". Computers and Security, 22(4):299-307.

[34] http:/ /www.academia.edu/l 959721/IJERA www.ijera.com.

[35] Hui Zhu; Bo Huang; Tanabe, Y.; Baba,T."Innovative Computing Information and Control", 2008.ICICIC apos; 08. 3rd International Conference on Volume,Issue,18-20 June2008,pp 509-509. [54] Iftikhar Ahmad, Sarni Ullah Swati, Sajjad Mohsin. "Intrusion Detection Mechanism by Resilient. Back Propagation (RPROP)" European Journal of scientific research,Volumel 7, No.4 2007,pp 523-530.

[36] Information Security Principles and Practice. Mark Stamp San Jose State University Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

[37] J. Daugman. Biometric personal identification system based on iris analysis. United States Patent, Patent Number: 5,291,560, 1994.

[38] Jack koziol. "Intrusion Detection with Snort", Sams Publishing, 800 East 96th Street,Indian 2003.

[39] Jack Koziol.(2003). "Intrusion Detection with Snort, Sams □ublishing, 800 East 96th Street, Indianapolis, Indiana 46240.

Juels and M. Sudan, (2002) "A fuzzy vault scheme," in Proceedings of the IEEE International Symposium on Information Theory, p. 408, Piscataway, NJ, USA.

Juels and M. Wattenberg, (1999) "A fuzzy commitment scheme," in Proceedings□-- 6th ACM Conference on Computer and Communications Security (ACM CCS '99), pp. 2 -36. Singapore

[40] Julie Greensmith and Uwe Aickelin. "Firewalls, Intrusion Detection Systems and Anti-Virus Scanners", Computer Science Technical Report,UK, 2005.

[41] Kerckhoffs' law, at http://en.wikipedia.org/wiki/kerckhoffs' law

[42] Kerckhoffs, La cryptographie rnilitaire, Journal des Sciences Militaires, vol. IX, pp. 5-83, January 1883, pp. 161-191, February 1883.

[43] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Richardson.(2004) CSI/FBI "Computer Crime And Security Survey," Computer Security Institute.

[44] LEE, W., AND STOLFO, S. J. A "framework for constructing features and models for intrusion detection systems". ACM Transactions on Information and System Security (TISSEC) 3, 4 (2000),pp 227-261.

[45] LEE, W., STOLFO, S. J., AND MOK, K. W. "A data mining framework for building intrusion detection models". IEEE Symposium on Security and Privacy O (1999), 0120.

[46] LIPPMANN, R. P., GRAF, I., WYSCHOGROD, D., WEBSTER, S. E., WEBER, D. J., and Gorton, S. The 1998 DARPA/AFRL Off-Line Intrusion Detection Evaluation. In In First International Workshop on Recent Advances in Intrusion Detection (RAID) Belgium.

[47] LUNT, T. F., and JAGANNATHAN. "A prototype real-time intrusion-detection expert System", In Proceedings of the 1988 IEEE conference on Security and privacy (1988), SP'88, pp 59-66.

[48] MITCHELL,T.M."Machine learning". McGraw Hill senes in computer science, McGraw-Hill,(1997).

[49] Mohamed Abdulhalim Saber managments of information systems, t1 , 2007, Alexandria. Dar al-Fikr, page 28 ,30 .

[50] Mohamed Dabas Elhamid and dr. Marco Ibrahim Nino, protection of information systems, Amman , Hamed library for publishing and distribution, 2007 , t1- page 34 .

[51] Najm Abdullah Alhamid (and others) .Managment information contemporary entrance , Amman , Dar Wael, 2005- page11.12.35.

[52] National Security Agency, at http://en.wikipedia.org/wiki/NSA

[53] NORTHCUTT S ."Network Intrusion Detection", an Analyst's handbook. New riders Publishing, Thousand Oaks, CA, USA, 1999.

[54] P. Ferguson and D. Senie.(2000). "Network ingress :filtering Defeating denial of service attacks" which employ IP source address spoofing agreements performance monitoring. RFC 2827.

[55] Proctor, Paul E (2001). "The Practical Intrusion Detection", Handbook. New Jersey: Prentice Hall.

[56] Q. Li and E.-C. Chang, (2006) "Robust, short and sensitive authentication tags using secure sketch, " in Proceedings of the 8th Multimedia and Security Workshop (MM and Sec '06), pp. 56-61, Geneva, Switzerland.

[57] R.J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, New York, [1 7] Wiley, 2001.

[58] Rafeeq Ur Rehman, 2003. Intrusion Detection with SNORT: Advanced IDS Techniques Using SNORT, Apache, MySQL, PHP, and ACID, Published by Prentice Hall.

[59] Rebecca Gurley Bace, "Technology series Intrusion Detection", (2000).

[60] Rebecca Gurley Bace. "Intrusion Detection, Macmillan technical publishing", page 29.2000.

[61] ROESCH, M. "Snort lightweight intrusion detection for networks", In Proceedings of the 13th USENIX conference on System administration, LISA '99, pp. 229-238, (1999).

[62] Rune Hammersland. "ROC m Assessing IDS Quality", Norwegian Information Security Lab,Gj0vik University College.

[63] S. C. Draper, A. Khisti, E. Martinian, A. Vetro, and J.S. Yedidia, (2007) "Using distributed source coding to secure fingerprint biometrics," in Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP '07), vol. 2, pp. 129-132, Honolulu, Hawaii, USA.

[64] Saeed Alqahtany , threats of information security and the ways of conforming them , Riyadh ,Naief arabic university for security scinces, 2008,(master degree).

[65] SAMUEL, A. L. "Some studies in machine learning using the game of checkers", IBM Journal of Research and Development, 3, 210-229.

[66] Saurabh Mahajan and Gurpadam Singh, (2007) "Reed-Solomon Code Performance for M-ary Modulation over AWGN Channel" International Journal of Engineering Science and Technology (DEST).

[67] Sumeet Dua, Xian Du.(2011). "Data Mining and Machine Learning in Cybersecurity",CRC Press.

[68] Sundaram A. "An introdution to Intrusion Detection",http://www.acm.org/crossroads/xrds2.html.

[69] T.C. Clancy, N. Kiyavash, and D.J. Lin, "Secure Smart Card-Based Fingerprint Authentication," Proc. 2003 ACM SIGMM Workshop Biometrics Methods and Application (WBMA), 2003.

[70] Thabit Abdullrahman Idris, managments of information systems in contemporary organizations- Alexandria, Dar al-Fikr 2005, page124.

[71] U. Uludae,. S. Pankanti, S. Prabhakar, and A. K. Jain, (2004) "Biometric cryptosystems: issues and challenges", Proceedings of the IEEE, vol. 92, no. 6, pp. 948-960.

[72] V. Bapuji and R. Naveen Kumar. (2012) "Soft Computing and Artificial Intelligence Techniques for Intrusion Detection System", Department of CSE, Jawaharlal Technological University (JNTUH), Hyderabad, India.

[73] VA, pp. 443-456.

[74] Varun Chandola, Arindam Banerjee, and Vipin Kumar , "Anomaly Detection": A Survey, Technical Report.

[75] Vetro and N. Memon, (2007) "Biometric system security" in Proceedings of the 2nd International Conference on Biometrics, Seoul, South Korea, August 2007.

[76] VIGNA, G., AND KRUEGEL. "Host-based Intrusion Detection Systems", handbook of Information Security. Wiley, December (2005).

[77] W. Boles, B. Boashash. A human identification technique using images of the iris and wavelet transform. IEEE Transactions on Signal Processing, Vol. 46, No. 4, 1998.

[78] WU, S. X., AND BANZHAF, W. Review. "The use of computational intelligence in intrusion detection systems", A review. Applied Soft Computing. 10, 1 (Jan. 2010), 1-35.

[79] Y. Dodis, L. Reyzin, and A. Smith, (2004) "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," in Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT '04), vol. 3027 of Lecture Notes in Computer Science, pp. 523-540, Interlaken, Switzerland.

[80] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, (2006) "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," Tech. Rep. 235, February 2006.

[81] Y. Seto, "Development of Personal Authentication Systems Using Fingerprint with Smart Cards and Digital Signature Technologies," Proc. Seventh_ Int'! Con[Control, Automation, Robotics, and Vision, Dec. 2002.

[82] Y.-J. Chang, W. Zhang, and T. Chen, (2004) "Biometrics-based cryptographic key generation," in Proceedings of the IEEE International Conference on Multimedia and Expo (!CME '04), vol. 3, pp. 2203-2206, Taipei, Taiwan.

[83] Yetmo Flasier , Frank Balas, protection of information managment and knowledge managment , technical university of Berlin,Germany. 2007.

AUTHORS

First Author – Abdelmajid Moh. Ali Alhwije , PhD,Candidate