A NOVEL SECURE E-CONTENTS SYSTEM FOR MULTI-MEDIA INTERCHANGE WORKFLOWS IN E-LEARNING ENVIRONMENTS

Shadi R. Masadeh[1],Bilal Abul-Huda[2]andNidal M. Turab[3]

[1]Dept. of Computer Networks, ISRA University, Amman, Jordan
masadeh@ipu.edu.jo
[2]Computer Information Systems Dept.,Yarmouk University, Irbid, Jordan
abul-huda@yu.edu.jo
[3]Department of computer science, ISRA University, Amman, Jordan
Nedalturab@ipu.edu.jo

ABSTRACT

The goal of e-learning is to benefit from the capabilities offered by new information technology (such as remote digital communications, multimedia, internet, cell phones, teleconferences, etc.) and to enhance the security of several government organizations so as to take into considerations almost all the contents of e-learning such as: information content, covering most of citizens or state firms or corporations queries. Content provides a service to provide most if not all basic and business services; content of communicative link provides the citizen and the state agencies together all the time and provides content security for all workers on this network to work in securely environment. Access to information as well is safeguarded. The main objective of this research is to build a novel multi-media security system (encrypting / decrypting system) that will enable E-learning to exchange more secured multi-media data/information.

KEYWORDS

E-content, E-protection, Encryption and Decryption, Security of E-content, multi-media.

1. INTRODUCTION

Many universities have to use wireless networks to provide their academic staff as well as their students with wireless access to facilitate nomadic access to university systems and internet. But all that is broadcasted over the air, so any eavesdropper, with proper equipment can have the access to the information that is transmitted over the air. These Wireless Networks needed to be secured in order to protect the multi-media data and or the multi-media information they transmit over the air between the users and access points, so the designers worked a light weight securing system they called WEP (Wired Equivalent Privacy).

The objectives of E-learning project are: first, increase the productivity, efficiency and effectiveness of university institutions. Second, save time and effort in the movement and wait. Third, keep transactions and access to any student from any university institution faster and finally, in this paper we provide content security for all users on this network to work secured environment and access to their information in a safe and secure manner.

An example as a current use of wireless networks in educational institutions is the Al-Hussein Bin Talal University (AHU). Al-Hussein Bin Talal University has an E-learning network sponsored by the Computer Center, to provide faculties with a new learning approach that could be

DOI : 10.5121/ijcnc.2013.5510

developed at later stages to provide a portal for professors to access instructional and examinational materials. The ComputerCenter is utilizing a wireless network that connects to some faculties as a pilot project to fathom the efficiency of the project. This imposes security vulnerability in that the network is using conventional wireless protection schemes (WEP, WPA, and WPA-PSK). The main objective of this research paper is to introduce a new encryption system that, in addition to the well known systems, will make it hard for the code crackers to get the data or the information. This system was implemented and tested in AHU.

2. RELATED WORK

The history of cryptography dates back to the earliest recorded instances of man. About 1900 BC an Egyptian scribe used non-standard hieroglyphs in an inscription. Kahn lists this as the first documented example of written cryptography (Menezes,Oorschot and Vanstone , 2008). Cryptography is both the lock and the combination (or key) that can be used to help protect your data. There are a variety of cryptographic methods and keys. Together, themethod and the key determine cryptographic security (Menezes,Oorschot and Vanstone , 2008).

The advent of computer technologies in both software and hardware necessitated the development of more advanced encryption methods, so the NSA requested the data security organizations to come up with a new encryption system to replace the old DES. In the year 2000 the NIST selected the Rijndael to be the winner and to become the new AES (Advanced Encryption Standard with 128 bit block and 256 bit key). Many versions of the Rijndael system were designed to provide many levels of security ranging from medium to most secured (128 – 256 bits) depending on the level of security needed. The new communication systems are utilizing the AES encryption which includes Microwave Networks, Cellular and Wireless Networks. (Ferguson and Schneier, 2003), (Schneier, 2001).

The magic of secrecy enticed enthusiasts into cracking the code in order to see what others are hiding from them, so they devised code breaking techniques, even the new AES has been attacked , and in many cases breakers got the data.

The rest of this paper is organized as follows: Related Work is described in Section 2. The Case Study and its Description are discussed in Sections 3 and 4. Current Challenges facing the organization are discussed in section 5. Solutions and Recommendations are showed in section 6. Finally Conclusion and Discussion are drawn in section 7.

3. CASE STUDY

In a wireless networks security applications, the system security technique is the process of ensuring that both the stored and transmitted multi-media data and information is secured either during transmitted or afterward. The transmitted multi-media data or information should be encrypted before transmission.

The AHU faculty of Information Technology is totally depending on wireless networks. The academic staff has free access to the internet as well as the AHU E-Learning system using a unique usernames and passwords to their accounts.

The wireless network system facilitates the academic staff access to the faculty staff and student data-base, the usage of E-Learning systems for updating E-Courses materials, online contact with students and preparing the E-Exams for students. The faculty wireless network consists of an

application server in the computer center, WEP data security system, access points (4-5 points in each floor) and, portable staff laptops. The systems main disadvantage is sending the pre-shared security key over the air, where anyone can simply 'hack' the system.
The new encryption method should be installed in:

1- Computer center application server.
2- Access Points.
3- Academic staff's portable computers.

The current wireless E-learning network at the faculty of information technology (FIT) at Al-Hussein Bin Talal University (AHU) is relatively effective in the sense that the faculty is intended to adopt the blended learning techniques at faculty classes. However, from a security point of view, the system has serious problems in the area of secure e-content delivery network connectivity as it is shown in the Figure (1) below.

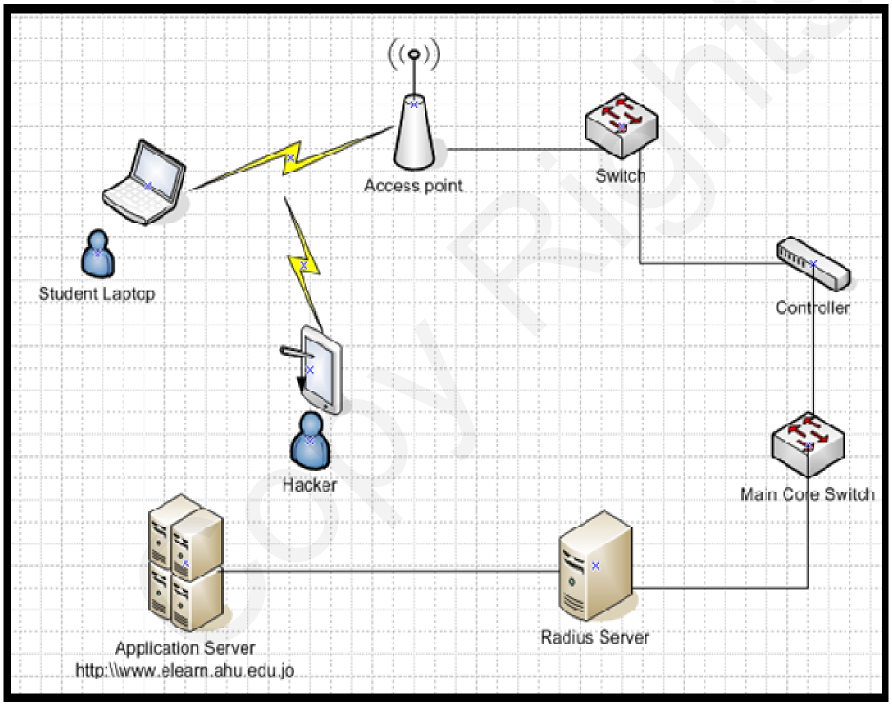

Figure 1: The network setup and the unsecured area of wireless E-Learning network of AHU Faculty of science and Information Technology (FIT).

The unsecured connection security issue can be summarized as follows:In the connection between the professor's notebook/laptop and the access point; the connection is encrypted using some widely used encryption systems and transferred over the air. When a hacker accesses the E-learning site/portal, the connection and the transferred multi-media data/information is sent over the air, and could be easily cracked using advanced methods. This means that the multi-media data/information integrity and confidentiality is jeopardized with simple software.

4. CURRENT CHALLENGES FACING THE ORGANIZATION

The main challenges facing the wireless network at the AHU are the security concerns. The wide-spread Access Points (APs) make it difficult to assure the security of system. The wireless system provides the academic staff, employees, and students with a remote access to the faculty students database files, Internetand Online E-Learning courses.

The main security issues that must be assured are the Confidentiality, Integrity, and Availability of the system data and resources. Therefore, the new security system must satisfy the following activities:

- Checking the ICT application environment for any sever-level vulnerabilities.
- Ensuring roles and privilege levels were respected.
- Evaluating use of cryptography for multi-media data at rest and in transit.
- Validating user input for malicious multi-media data/information that could result in loss of integrity or confidentiality of multi-media data/information.
- Anti-automation and end-user protection measures.

5. SOLUTION AND RECOMMENDATIONS

As a solution of threats facing the wireless network security using in AHU computer center we introduced a new encryption system for the transferred data/information. In our research we can summarize our proposed system in the following steps:

- ✓ Encryption Side:

Step1: Open file for reading digitized multi-media data or information.

Step2: Open file for writing ciphered multi-media data or information.

Step3: Read multi-media dataset as blocks.

Step4: Embedded Watermark into multi-media dataset.

Step5: Set 2 arrays to hold plain digitized multi-media data or information text and cipher digitized multi-media data or information text.

Step6: Hold input and output bytes or blocks in unmodified format.

Step7: Read-in 4 bytes or blocks from digitized multi-media data or information file.

Step8: keep reading until end of plain digitized multi-media data or information file.

Step9: read in one byte at a time and add it to the plain digitized multi-media data or information file array.

Step10: If the number of bytes in the plain digitized multi-media data or information file of array is 4 then encrypt the bytes from 0 to 3 (4 in total) and put them in cipher text array.

Step11: Repeat Step10 until end of array.

Step12: Write the cipher digitized multi-media data or information file array to encrypted or ciphered file.

Step13: Reset buffers P and S.

Step14: Encrypt the block (64-bit block).

- ✓ Decryption side

Step1: Open file for reading ciphered multi-media data text.

Step2: Open file for writing plain digitized multi-media data text.

Step3: reset the byte counter and start reading 4 bytes into ciphered digitized multi-media data array.

Step4: Repeat Step3 until end of ciphered multi-media data text file.

Step5: decrypt the bytes from 0 to 3 (4 in total) and put them in plain digitized multi-media data of array.

Step6: Read-in 4 bytes from decrypted file.

Step7: If the number of bytes in the ciphered digitized multi-media data array is 4 then decrypt the bytes from 0 to 3 (4 in total) and put them in digitized multi-media data array.

Step8: Repeat Step 7 until end of array.

Step9: Decrypt the block (64-bit block).

Step10: Extract Watermark from multi-media dataset.

Step11: Show multi-media dataset.

5.1 Proposed Encryption Algorithm

The following modified algorithm is used to explain our approach as follows:

1. Open file fpin for reading plain digitized multi-media data or information text

2. Open file fpout for writing ciphered multi-media data cipher text

3. Read dataset as blocks.

4. Embedded Watermark into dataset as shown above section 4.

5. set 2 arrays to hold plain digitized multi-media data or information text and ciphered multi-media data text using calloc function

6. unsigned int p[4],s[4]; /* to hold input and output bytes in unmodified format */

7. Read-in 4 bytes from file 1 into array and keep reading until end of plain digitized multi-media data or information file.

8. while (!feof(fpin)){ /* since we don't know the size of input file */

9. ch=getc(fpin); /*read in one byte at a time */

10. P[i++]=ch; /* add it to the cipher digitized multi-media data or information file plain text array */

11. If (i>3){ /* if the number of bytes in the cipher digitized multi-media data or information file plain text array is 4 then */

12. S[0]=(encrypt(p[3] using public key Bi[0]); /* encrypt the bytes from 0 to 3 (4 in total) and put them in cipher text array */

13. s[1]=(encrypt(p[2] using public key Bi[1]);

14. s[2]=(encrypt(p[1] using public key Bi[2]);

15. s[3]=(encrypt(p[0] using public key Bi[3]);

16. putc(s[2],fpout); /* write the ciphered digitized multi-media data cipher text array to output file (encrypted file) */

17. putc(s[0],fpout);

18. putc(s[3],fpout);

19. putc(s[1],fpout);

20. I=0; /* reset the byte counter and start reading 4 bytes into digitized multi-media data plain text array

21. reset buffers P and S using calloc function

22. } /* end of bytes reading loop */

23. if I > 0 /* there is more input to process digitized multi-media data array (plain text)

24. } /* end of while loop, at the end of input file digitized multi-media data array (plain text file) */

25. Encrypt the block (64-bit block)

5.2 Proposed Decryption Algorithm

The proposed decrypting algorithm is depicted as follows:

1. Open file fpin for reading ciphered digitized multi-media data text.
2. Open file fpout for writing digitized multi-media data of plain text.
3. set 2 arrays to hold digitized multi-media data of plain text and ciphered digitized multi-media data of cipher text using calloc function
4. unsigned int p[4],s[4]; /* to hold input and output bytes in unmodified format */
5. Read-in 4 bytes from file 1 into array and keep reading until end of ciphered digitized multi-media data of cipher text file
6. while (!feof(fpin)){ /* since we don't know the size of input file */
7. ch=getc(fpin); /* read in one byte at a time */
8. p[i++]=ch; /* add it to the ciphered digitized multi-media data cipher text array */
9. if (i>3){ /* if the number of bytes in the ciphered digitized multi-media data cipher text array is 4 then */
10. s[0]=(decrypt(p[3] using private key Bi[0])); /* decrypt the bytes from 0 to 3 (4 in total) and put them in digitized multi-media data plain text array */
11. s[1]=(decrypt(p[2] using private key Bi[1]));
12. s[2]=(decrypt(p[1] using private key Bi[2]));
13. s[3]=(decrypt(p[0] using private key Bi[3]));
14. putc(s[2],fpout); /* write the digitized multi-media data plain text array to output file (decrypted file) */
15. putc(s[0],fpout);

16. putc(s[3],fpout);
17. putc(s[1],fpout);
18. I=0; /* reset the byte counter and start reading 4 bytes into ciphered digitized multi-media data cipher text array
19. reset buffers P and S using calloc function
20. } /* end of bytes reading loop */
21. if I > 0 /* there is more input to process ciphered digitized multi-media data cipher text .
22. } /* end of while loop, at the end of input file ciphered digitized multi-media data array (cipher text file) */
23. Decrypt the block (64-bit block)
24. Extract Watermark from multi-media dataset.
25. Show multi-media dataset

6. CONCLUSION AND DISCUSSION

Through the compilation of all university activities and information services, interactive and reciprocity in one location on the web site is the official university web site from which to do the following:

1. Linking the average various organs of the university for all of the university services, and computerized automatically to anywhere in the world and safely.
2. Completion of the university to the adoption of the various activities of information and communication networks remotely.
3. The idea of E-learning basis to take advantage of all the possibilities offered by information technology (such as digital communications, multimedia, internet, cell phones, teleconferences, etc.) and to improve the performance of various government institutions so as to include all the contents of E-government such as:
    1. Information content, covering most if not all queries of faculty members, students or state firms or enterprises.
    2. Content provides a service to most if not all basic services and business services.
    3. Content of communication link provides citizens and the state agencies together almost all of the time.
    4. Provides content security for all workers on this network to work securely and access information in safeguarded environment.

Possible limitations of our algorithm are the CPU computation time and the power consumption. These limitations can be considered as a future work.

In this paper we propose a novel multi-media security system (encrypting / decrypting system) that will enable E-learning to exchange more secured multi-media data/information.

ACKNOWLEDGEMENTS

The authors are grateful to the Al- Isra University, Jordan, for the Full Financial support granted to this research project.

REFERENCES

[1] I. Fluhrer, S.Mantin, I.Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4",(**2001).**

[2] B. Schneier, "Cryptography, Security, and the Future," Communications of the ACM, v. 40, n. 1, 1997 p. 138. http://en.wekipedia.org/wiki/automation.

[3] N.Ferguson , B.Schneier," Practical Cryptography". New York: J. Wiley & Sons**, (2003**).

[4] A. Menezes, P. van Oorschot and S. Vanstone ," Handbook of Applied Cryptography", / ajmeneze at uwaterloo.ca / last updated **(2008).**

[5] B. Schneier, "Cryptography, Security, and the Future," Communications of the ACM, v. 40, n. 1, 1997 p. 138. http://en.wekipedia.org/wiki/automation.

[6] R. Steve Edmonson, "Data Encryption and Cryptography, Investment and Governance Division Ohio Office of Information Technology", **(2007).**

[7] V. Tselkov, N. Stoianov, "A Model of Software Cryptography System for Data Protection in Distribution Information Systems", (**2003**), www.dataprotection2003.info/speakers/Veselin_Tselkov/presentation.pdf.

[8] B. Schneier, "Key Length And Security." Crypto-Gram , **(2001).**

http://www.counterpane.com/crypto-gram-910.html#KeyLengthandSecurity

[9] Wi-Fi Alliance. "Wi-Fi Protected Access (WPA)", Version 2.0**,(2003).**

[10] Wi-Fi Alliance. "Securing Wi-Fi Wireless Networks with today technologies", **(2003).**.

[11] A. Schneier and J. Kelsey, "Unbalanced Feistel Networks and Block Cipher Design," Fast Software Encryption, Third International Workshop Proceedings, 1996. ,Springer-Verlag, pp. 121-144**, (1996).**

[12] M. Wiener. ``Efficient DES Key Search", presented at the Rump session of Crypto '93. Reprinted in Practical Cryptography for Data Internetworks", W. Stallings, editor, IEEE Computer Society Press, pp. 31-79 **(1996).**

[13] S. Landau," Data Encryption Standard (DES)" .Notices of the AMS, March **(2000).**

.

Authors

Dr. Shadi R. Masadehreceived a BSc degree in Computer Science and Computer Information System in 2000 and MSc degree in Information Technology in 2003. with a Thesis titled "A Mathematical Approach for Ciphering and Deciphering Techniques" After that, I received PhD from department of Computer Information System in 2009 with a Thesis titled "A New Embedded Method for Encryption/Decryption Technique Using Self Approach" My research interests including E-learning Management and Security Issues, Encryption and Decryption Systems. Networking and Wireless security. Currently, I'm working at ISRA University in Computer Networks Department as assistant Prof. I have submitted a number of conference papers and journals.

Prof. Bilal Abul-huda received a BSc degree in Mathematicsand computer science SUNY at Plattsburgh, Plattsburgh, New York, U.S. and M.SC Systems Engineering UPM, Dhahran, Saudi Arabia. Ph.D. Universityof Ulster at Jordanstown, Northern Ireland, UK His research interests include WLAN security, learning systems.. He is a full professor at Yarmouk University, Irbid, Jordan

Dr. Nidal Turab received a BSc degree incommunication engineering from theUniversity of Garounis, Benghazi, libya 1992 and an MSc in telecommunicationengineering from the University of Jordan,Amman in 1996. His PhD in computerscience is from the Polytechnic Universityof Bucharest, 2008. His research interests include WLAN security, computer network security and cloud computing security.. He is an assistant professor at Isra University, amman, Jordan