Secure Communication: 
A Proposed Public Key Watermark System

Shadi R. Masadeh, Department of Computer Networks, Al-Isra University, Amman, Jordan,
Shadi Aljawarneh, Faculty of Information Technology, Al-Isra University Postoffice Amman, Jordan
Ashraf Odeh, Faculty of Information Technology, Al-Isra University Postoffice Amman, Jordan
Abdullah Alhaj, Faculty of Information Technology, University of Jordan, Aqaba, Jordan

ABSTRACT

The idea of e-Commerce is 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 security of various organizations. In the article, the authors focus on securing all the contents of e-Commerce by proposing a public key watermarking algorithm for web content integrity verification. The main purpose of this article is to present a new security system that enables e-Commerce to exchange data more securely and by altering the file content structure, detecting illegal access and stopping the illegal operation. Such system combines the watermarking techniques with the cryptography methods in order to provide the highest visible security component that influences on the end user through its daily payment interaction with business.

Keywords: E-Commerce, E-Learning, Encryption and Decryption, Multimedia, Watermarking, WIFI, Wireless Networks

INTRODUCTION

Many organizations have to use wireless networks to provide their employees as well as clients with wireless access to facilitate nomadic access to organization systems and internet. But all that is broadcast 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 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).

An example as a current use of wireless networks in educational institutions is the AL-Isra Private University (IU). AL-Isra Private University has an e-learning network sponsored by the Computer Center, to provide faculties with a new learning approach that could be developed at later stages to provide a portal for professors to access instructional and examinational materials. The Computer Center is utilizing a wireless network that connects to some faculties as a pilot project to fathom the efficiency of the project. This imposes security

DOI: 10.4018/ijisp.2013100101
vulnerability in that the network is using conventional wireless protection schemes (WEP, WPA, and WPA-PSK). The main objective of this 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. This system was implemented and tested in IU.

The IU faculty of Information technology is totally depending on wireless networks. The academic staff has free access to the internet as well as the IU E-Learning system using a unique usernames and passwords to their accounts. The wireless network system facilitate 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 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 ‘crack’ the system.

It should be noted that the problem of web content security is a very sensible area. Currently, if a user is not on the Web, this means he/she does not exist. Also if he/she is online, everything he/she put on the Internet is public and susceptible to being accessed in illegal ways, Aljawarneh A. (2011).

This paper is organized as follows; the next section presents the related works, and the current approaches and their strengths and weaknesses. The proposed solution is described in the section following that. The section after describes the architecture implementation. Finally, the last section presents the conclusion and future work.

RELATED WORKS

In this section, we discuss the cryptography method and approaches, and watermarking techniques that assist to secure the web content.

The history of cryptography dates returns 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, A., van Oorschot, P., and Vanstone, S. (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, the method and the key determine cryptographic security Menezes A., van Oorschot P. and Vanstone S. (2008).

Below are some of the most commonly used schemes that appeared through cryptography history:


2. Public Key cryptography introduced by Hellman, and Diffie 1976. It enables two people to communicate confidentially, or to authenticate each other, without a prearranged exchange of secret cryptographic keys, based on mathematical and discrete logarithm problems. It also provided the first technical mechanism for digital signatures that cannot he repudiated Steve Edmonson, R. (2007).

3. RSA public-key cryptosystem appeared in 1978 by Rivest, Shamir, and Adelman. It is the oldest unbroken public-key system. This provides both confidentiality and authentication. Its security is based upon the difficulty of determining the prime factors of a very large number Steve Edmonson, R. (2007), Tselkov, V., and Stoianov, N. (2003).

4. 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).
Optimizing Privacy-Accuracy Tradeoff for Privacy Preserving Distance-Based Classification
www.igi-global.com/article/optimizing-privacy-accuracy-tradeoff-privacy/68819?camid=4v1a