# IMPROVEMENT OF DATA INTEGRITY USING DIFFERENT ENCRYPTION ALGORITHMS

**Serwan Waleed Jirjees**[1]

**Received on: 23 / 2 / 2011**
**Accepted on: 25 / 5 / 2011**

## Abstract

Web services send and receive messages over standard Internet protocols such as HTTP. Plaintext messages can be intercepted by an attacker and potentially viewed or even modified for malicious purposes. By using message protection, we can protect sensitive data against threats such as eavesdropping and data tampering. Sensitive data transmitted over the Internet should always be encrypted to avoid potential intruders from eavesdropping on the communication anywhere along the route the data takes between the two machines.

In this paper, we provide a feasible solution to enhance the integrity of sensitive data. Our approach is to use variant encryption algorithms based on session key which is sent with the client page from the server side where it is used to encrypt and decrypt data so that the data will be unreadable from the attacker. The encryption algorithm will be changed to every connection state. Our approach is very complex as we must cryptanalysis and modify the plaintext from attackers and make it applicable to client-server architecture.

***Keywords***: *web security, authentication, integrity, encryption, session key.*

## الخلاصة

ان من خدمات الويب إرسال واستقبال رسائل غير مشفرة (plaintext) عبر بروتوكولات الإنترنت القياسية مثل بروتوكول نقل النص التشعبي (HTTP). الرسائل الغير مشفرة (plaintext) يمكن أن يتم اعتراضها من قبل مهاجم (attacker) ويحتمل أن ينظر إليها أو حتى تعديلها لأغراض خبيثة. باستخدام حماية الرسالة ، يمكننا حماية البيانات الحساسة من التهديدات مثل التنصت (eavesdropping)والعبث في البيانات. البيانات الحساسة التي ترسل عن طريق الانترنت يجب إن تكون دائما مشفرة لتجنب الدخلاء من التنصت على الاتصالات في أي مكان على طول الطريق ويأخذ البيانات بين الجهازين.

في هذه البحث ، نقدم حلا عمليا لتعزيز أمن البيانات الحساسة. نظريتنا هو استخدام خوارزميات تشفير مختلفة ومتغيرةلكل حالة اتصال مبنية على اساس مفتاح الجلسة (session key) التي ترسل إلى صفحة العميل واستخدامها في تشفير و فك تشفير البيانات وبالتالي تكون النصوص المرسلة غير مفهومة للمتطفل.حيث هذه الخوارزمية المجهزة للعميل تتغير لكل حالة اتصالنظريتنا معقدة جدا كي يتم تحليل الشفرات بوقت قصير ويكتشف البيانات من قبل المهاجمين والتي تنطبق على العميل- المجهز(client-server).

[1] University of Technology/Control & System Engineering, Baghdad, Iraq

## 1. Introduction

In many modern applications, the classical client-server processing architecture has been supplanted by more distributed architectures, characterized by many parties interacting across heterogeneous systems. In the Internet or client server systems, there are several types of security attacks in network and computer security. Those are interception, modification and fabrication. Interception is concerned with an attack on confidentiality [1,2].

Interception is an illegal action that an unauthorized opponent gains much information in a network for information stealing. [3,4,5,6].

To protect our networks and computer systems against security attacks, many security services are needed in a network and server system, such as authentication, access control, confidentiality, and integrity. Among them, authentication service is to make sure whether a client is authentic or not, by using user’s ID, password or internet address, etc. and the Integrity is used to prevent unauthorized modification of resources and maintain the status quo. It includes the integrity of system resources, information, and personnel. The alteration of resources, like information, may be caused by a desire for personal gain or a need for revenge[5,7].

In the Internet, including distributed client server systems, a server system requires a user’s ID and password to prevent unauthorized users from using resources of the server. Authentication focuses on fabrication attack [1, 4].

There are many ways to protect information from eavesdropping as it travels through a network:

- Physically secure the network, so that eavesdropping is impossible.
- Hide the information that you wish to secure within information that appears innocuous.
- Encrypt the information so that it cannot be decoded by any party who is not in possession of the proper key.

We propose an improved integrity of exchanging the sensitive data between client and server by authentication system based on confirming the server from the client then continuing the contact through the encrypted data between them. The server will provide the client with the encryption code after the completion of the authentication stage used to encrypt the sent data. The encryption code and key will be changed from one client to another or to the same client after another connection.

This paper is organized as following. In section 2, a brief introduction is given about Client Server Security Requirements, and in section 3, integrity is defined. In section 4, we explain the characteristic encryption used to protect information from modification. While in section 5we present our proposed systems.

## 2. Client Server Security Requirements

Most Internet services are based on the *client/server* model. Under this model, one program requests service from another program. Both programs can be running on the same computer or, as is more often the case, on different computers. The program making the request is called the *client*; the program that responds to the request is called the *server*. Often, the words "client" and "server" are used to describe the computers as well, although this terminology is technically incorrect.

The data sent over computer networks are sensitive to attacks by adversaries. Private/sensitive information must be protected from others since the malicious adversaries can read and/or alter the message content or masquerade himself/herself as someone else. In order to make sure that the information is secure, four main requirements are considered. These are authentication, integrity, non-repudiation and confidentiality. They are also the least secure environments in client-server models. Clients connect to servers and these connections, if left open or not secured; provide entry points for hackers and other intruders that may use data for nefarious purposes. Aside from physical client security in the form of disk drive locks or diskless workstations that prohibit the loading of unauthorized software or viruses, accessibility to all files stored on a workstation operating system is the other gaping security hole in clients.

## 3. Integrity

Data integrity is an assurance that unauthorized parties are prevented from modifying data. Participants in distributed data exchange include primary data sources, intermediate sources, and end users. [10,11]

Data integrity services therefore are `safeguards against the threat that the value or existence of data might be changed in a way inconsistent with the recognized security policy' [2]. Modification or changing the value of a data item includes writing, changing, changing the status, deleting, substituting, inserting, reordering, and delaying or replaying of transmitted messages [7,8].

There are many ways to protect information from modification when it travels through a network; encryption is one of these methods. Encrypt the information it cannot be decoded by any party who is not in possession of the proper key.

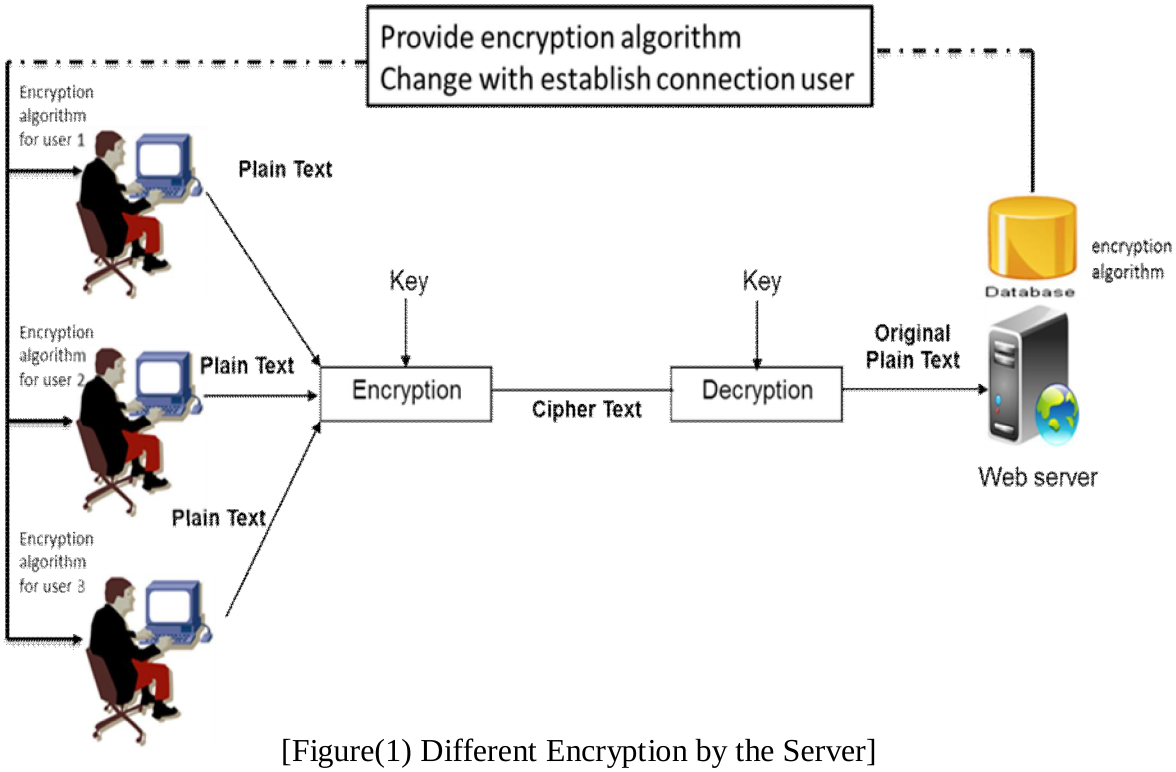
## 4. Encryption

Encryption has primarily been used to prevent the disclosure of confidential information, but can also be used to provide authenticity of the source of the message, verify the integrity of received data, provide the digital equivalent of a hand written signature, and non-repudiation. Non repudiation assures that a transacting party cannot deny that the transaction took place.

Symmetric encryption schemes use the same secret key, or two keys easily computed from each other, for both the sender and the receiver of a protected message. The secret key is typically shared between two or more communicating parties prior to its use to secure a communication channel. One major issue for the use of symmetric encryption show to securely exchange the secret key[4,5].

In this paper, we propose a method for the data encryption by different encryption algorithms and keys provided from the server and uploaded with the web. At this stage of the design we used data encryption system by different encryptions and keys provided from the server and uploaded with web browser after making sure of authorizing it for the user when he/she enters to the system prepared for a temporary database connection including the type of encryption algorithm from the database server.

This data base contains various types of encryption algorithms including the method of encryption and decryption. When the connection is established, it will select one of the algorithms to the user that holds the encryption method with the data to the user, after the receipt of encrypted data where it is disassembled by the server with the same algorithm is fitted to the user by referring to the temporary data base that change to same user when change the time entered.


Provide encryption algorithm
Change with establish connection user
Encryption algorithm for user 1
Plain Text
Encryption algorithm for user 2
Plain Text
Plain Text
Encryption algorithm for user 3
Key
Encryption
Cipher Text
Key
Decryption
Original Plain Text
Database
encryption algorithm
Web server

[Figure(1) Different Encryption by the Server]

## 4.1 Encryption Algorithms

Different encryption algorithms use proprietary methods of generating these keys and are therefore useful for the proposed system. Blowfish is a symmetric block cipher just like DES or IDEA. It takes a variable-length key, from 32 to 448 bits, making it ideal for both domestic and exportable use. Another encryption algorithm is DES which is a block cipher with 64-bit block size that uses 56-bit keys. RC4 is a cipher with a key size of up to 2048 bits.

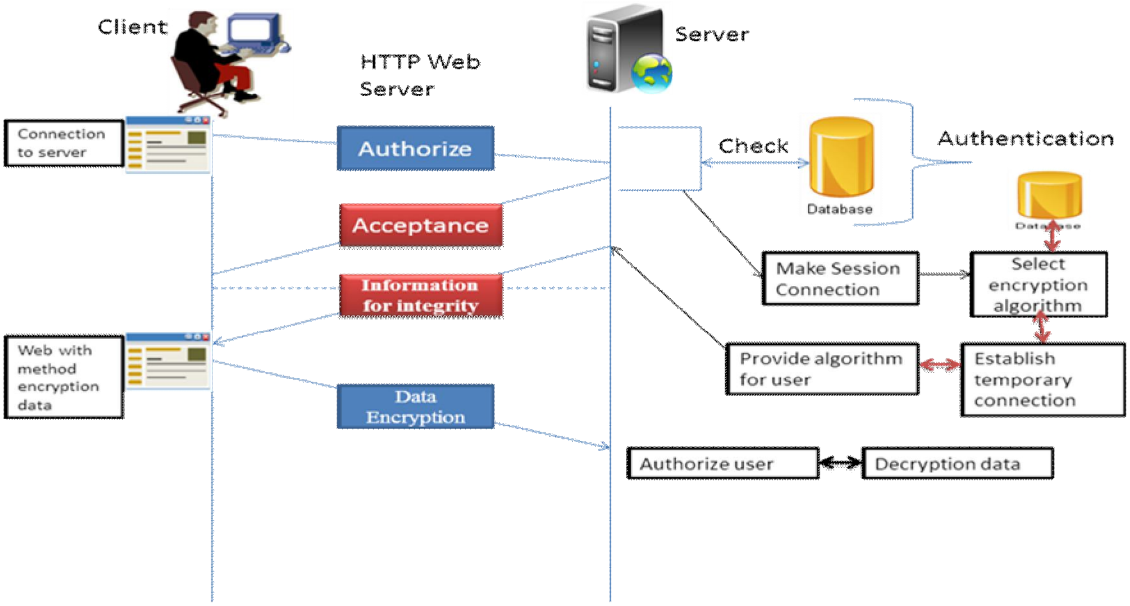
## 5. The Proposed System

In this paper, we propose a new approach to improve data integrity using encryption based on variant encryption algorithms and keys provided by the Server for each session connection. Our system contains authentication phase, and encryption and decryption phase, as shown in figure 2.The proposed system is based on the protection and safety of the transfer of information to web pages between the server and client.

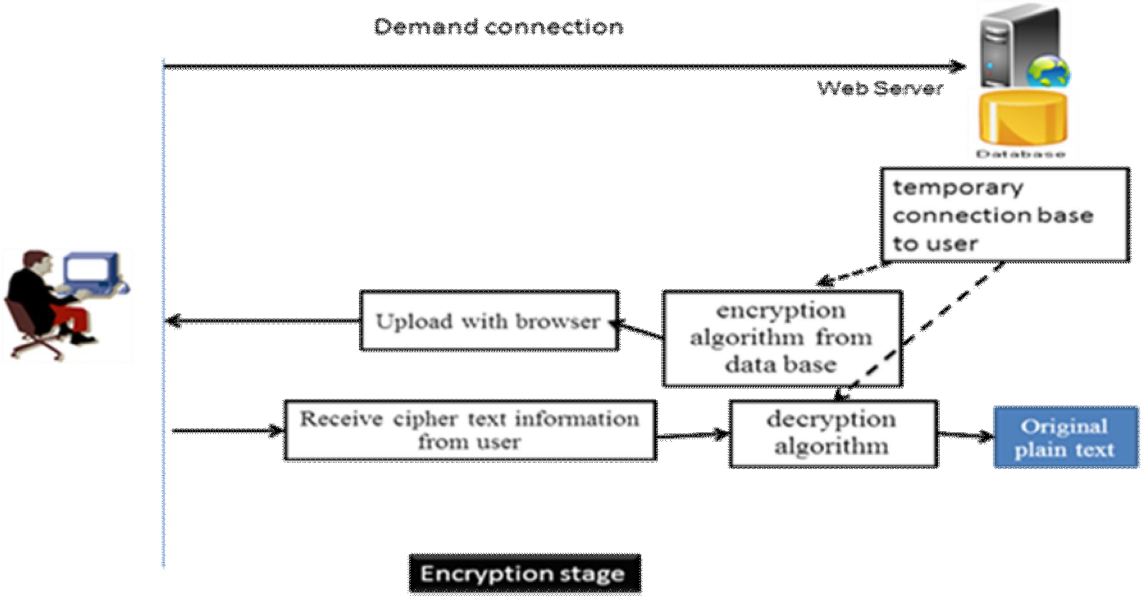
The system consists of two stages. The first stage is to build an authentication system based on assuring a user's access to the system by checking data that have been processed previously by the server. The second stage is insuring the integrity of the information by encrypting it through the algorithms provided by the server and uploaded with the web page fitted to the user. After receiving the page where the data is sent, we encrypt it by an algorithm send with the same page. These algorithms are based on the form of a database prepared by the server to the clients. Data base is composed of a number of encryption algorithms and the way her jaw, after the client requests the connection is provided contact one of these algorithms randomly, where change this algorithm to the same client after a period of time.

After the server verifies the identity of the client and the connection established in authentication phase, the server creates a temporary data base, private to the client, which contains encryption algorithm and session key selected randomly from variant algorithm in server connection

In encryption and decryption phase, the server sends the encryption algorithm and session key to the client to encrypt his secret data and send it to the server, and when received it decrypts using the same algorithm and key, as shown in figure3.



[Figure (2) The General Structure of the Proposed system]


Demand connection
Web Server
Database
temporary connection base to user
Upload with browser
encryption algorithm from data base
Receive cipher text information from user
decryption algorithm
Original plain text
Encryption stage

[Figure (3) Temporary Connection Database]

## 6.Conclusion

We conclude from our paper that sending sensitive data is very important and must be encrypted to ensure the non-arrival of the attackers to the data to modify it , in order to ensure integrity, just not enough data to verify the identity of the user where they are eavesdropping or modification during transmission. To ensure that this happens we have strengthened the confidentiality and integrity of data through data encryption. But encryption methods are easy to break (Cryptanalysis) and possible to infer the key used in the encryption after a few attempts, especially when this key is used several times in the encryption.

In this research, we have multiple encryption algorithms used in the client server equipped with a different algorithm each session a new connection, but for the encryption key used to also be different each session so that it is a different connection from the communication session only, where it will be difficult for the attacker to conclude the key because it will change for each new connection. Thus, it would be difficult for the attacker to detect data sent and thus we have enhanced confidentiality and data integrity.

## References

[1] William Stallings, Network Security Essentials: Application and Standards,Prentice Hall, 2002

[2] S. M. Bellovin and M. Merritt, "An Attack on the Interlock Protocol WhenUsed for Authentication," IEEE Transactions on Information Theory, 40(1):273-275, Jan., 1994.

[3] Andrew S. Tanenbaum “Computer Networks” Prentice Hall, ISBN: 0-13-066102-3, Fourth Edition 2003.

[4] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Transactionson Information Theory, IT-22(6):644-654, 1976

[5] Michael Cross,” Security+ Study Guide and DVD Training System”, SyngressPublishing, Inc., 2010.

[6] Jae Seung Lee, Sang Choon Kim, and Seung Won Sohn, "A Design of theSecurity Evaluation System for Decision Support in the Enterprise NetworkSecurity Management," Lecture Notes in Computer Science, Vol. 2015:246-260, Springer-Verlag, 2000

[7] SimsonGarfinkel& Eugene H. Spafford,” Web Security & Commerce”, ISBN: 1-56592-269-7, First Edition, June 1997.

[8] SoichiFuruya, "Slide Attacks with a Known-Plaintext Cryptanalysis," LectureNotes in Computer Science, Vol. 2288:214-225, Springer-Verlag, 2001

[9] James Giles, Reiner Sailer, Dinesh Verma, and Suresh Chari, "Authenticationfor Distributed Web Caches," Lecture Notes in Computer Science, Vol.2502:126-145, Springer-Verlag, 2002

[10] Charlie Kaufman, Radia Perlman, Mike Speciner, Network Security: PrivateCommunication in a Public World, Prentice Hall, 1995.