A Survey on Web Security: A Study

Ms.Rati Bajpai[1], Mr. Ankit Srivastava[2,]
[1]*Department of Electrical Engineering, Faculty of Engineering and Technology, Rama University, Kanpur, UP, India 209217*
[2]*RKDF College of engg. Bhopal*

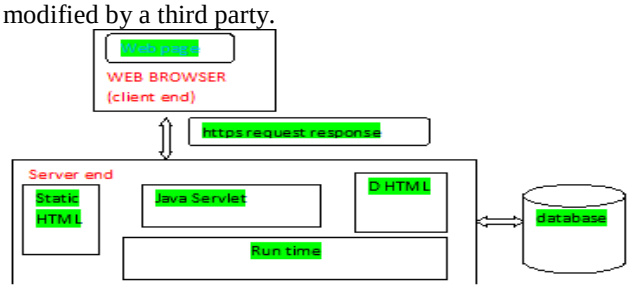
Abstract: This is a review paper that describes the various algorithm of web security. Web security is a large area about computer system security, network security, authentication services, message validation, personal privacy issues and cryptography.
Web is one of the most used communication medium for information sharing over internet today. Cryptography is one the method for applying the web security. In this paper some of the cryptographic techniques, algorithms and applications in computer networks are reviewed.
Keywords: Cryptographic Algorithms, Security Attacks, Security Aspects, Web Security.

I. INTRODUCTION

A general definition of web security is provided by Garfinkel and Spafford 1997 [1]. Web security is a set of procedures, technologies for protecting web servers, web users, and their organizations. Security protects the user against sudden behavior. Users and web service providers have a set of predefined target for expected behavior of the web with respect security.

Users have their prospect is the service being provided is genuine, safe, and private; genuine in the sense the services or information being supplied by the web server is the web server the user expects to provide those services or information; safe in the sense that the services or information being provide will not altered, not contain computer viruses or content that will harmful for users system.

From the server's view their expectation is the user of the information or a service is genuine and responsible; genuine in the sense the has been accurately identified; responsible in that the user will not attempt to access restricted documents, server, or use the server computing system as means of illegal access to another computer system. From the perspective of both the server and the user, they have an prospect that their communications will be free from eavesdropping and reliable in terms that their transmissions will not be modified by a third party.



Where **p** is dipole moment and **E** is the external applied field. Conventional Rabi oscillations are studied using the rotatingwave approximation (RWA) [5]. This is an approximation, where rapidly oscillating terms of the effective Hamiltonianare removed. This approximation is valid near the resonance i.e. when the incident frequency of the light field nearlyequal to transition frequency of the two level systems. In the off-resonance case, a new kind of Rabi oscillation is seen,in topological insulator. To study this, we employ an approximation known as asymptotic rotating wave approximation (ARWA) [6–11] (otherwise known as Fouquet approximation [12, 13]). The dephasing of anomalous Rabi oscillations in monolayer graphene can also be seen by including the electron-phonon interaction [14]. In this article, the effect of Zeeman term on anomalous Rabi oscillation is shown and how this is sensitive to qualitative changes in the low-energy band structure rather than the conventional Rabi oscillation.

II. RELATED WORK

The web security problem consists of three major parts:
• Securing the web server and the data that is on it. The server can continue its operation, the information on the server is not modified without authorization, and the information is only distributed to those user to whom you want it to be distributed.
• Securing information that travels between the web server and the user. The user and organization like to assure that information supplies to the web server (usernames, passwords, financial information, etc.) cannot be read, modified, or destroyed by others. Many network technologies are especially susceptible to eavesdropping,
• Securing the user's own computer. The users have to be ensuring that information, data, or programs downloaded to their systems will not cause damage in some cases, we have the challenges of:
• Verifying the identity of the user to the server
• Verifying the identity of the server to the user
• Ensuring that messages get passed between client and server in a timely, reliably, and without replay
• Logging and auditing information about the transaction for purposes of billing, conflict resolution, "nonrepudiation," and investigation of misuse

III. CRYPTOGRAPHY

Cryptography is the science of writing in secret code and is an earliest art, the first documented use of cryptography in writing dates back to1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in a message. Some experts dispute that cryptography appeared spontaneously sometime after writing was invented. It is no surprise, then, that new forms of cryptography came soon after the development of computer communications. Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication.

The best way to achieve web security is through Cryptography. Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. Cryptographic algorithms can be broadly categorized as follows:

Private (single, shared) key algorithms are used for bulk data encryption, as they are comparatively fast. They do require a secret key to be known by both parties.

Examples include: DES, Blowfish, IDEA, LOKI, and RC4.

Public (two) key algorithms are used for key validation & distribution, good because a public key is used, but limited by their computational cost compared to private key schemes.

Example include: Diffie-Hellman, ElGamal, and RSA

Signature algorithms are used to sign & authenticate data, and are also usually public key based.

Examples include: ElGamal, RSA, and DSA

Hash algorithms are used to compress data down to a fixed size for signing.

Examples include: MD5, Havilland SHA

A. Block cipher algorithms

Block ciphers, the most common form of private key algorithms operate on a fixed size data block (eg 64 bits), use a single secret, shared key (eg 56,64, or128 bits), and

Generally involve multiple rounds (8-32) of some simple, non-linear function which uses half the value as input and whose output is XOR'd with the other half. This is known

As a feistel structure, invented by Horst Feistel. Some common algorithms include:

DES/3DES

The Data Encryption Standard (DES) was developed and endorsed by the U.S. government in 1977. DES is a block cipher with 64-bit block size that uses 56-bit keys [2]. Triple-DES (3DES) has emerged as a stronger method. Using standard DES encryption, Triple-DES encrypts data three times and uses a different key for at

Least one of the three passes giving it a cumulative key size of 112-168 bits.

FEAL

In cryptography, FEAL (the Fast data Encipherment Algorithm) is a block cipher and designed to be much faster in software. The Feistel based algorithm was first published in 1987 by Akihiro Shimizu and Shoji Miyaguchi from NTT. The cipher is susceptible to various forms of cryptanalysis, and has acted as a catalyst in the discovery of differential and linear cryptanalysis [3].

IDEA

A 64-bit, 8 round iterated block cipher with a 128-bit key [4], designed by X. Lai and J. Massey in 1990. The concept used is the "mixing operations from different algebraic groups".

BLOWFISH

It is a Feistel network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is a complex initialization phase required before any

Encryption can take place; the actual encryption of data is very efficient on large microprocessors [5].

RC2, RC5

Two private key block ciphers developed by RSA Data Security Inc [6][7] . They are parameter sable, with various sized data and keys, and number of rounds, possible. These ciphers have been widely licensed and Used in products such as Netscape.

B. Stream Cipher Algorithms

Stream cipher is a symmetric key cipher where plaintext bits are combined with a pseudorandom cipher bit stream typically by an exclusive-or (xor) operation. In a stream cipher the plaintext digits are encrypted one at a time.

RC4

The RC4 algorithm is a stream cipher from RSA Data Security, Inc. The published algorithm performs identically to RC4 implementations in official RSA products. RC4 is widely used in many applications and is generally regarded to be secure. This cipher is widely used in commercial applications including Oracle SQL, Microsoft Windows and the SSL.

SEAL

SEAL (Software-Optimized Encryption Algorithm), designed by Don Coppersmith of IBM Corp, is probably the fastest secure encryption algorithm available. The key

Setup process of SEAL requires several kilobytes of space and rather intensive computation involving SHA1, but only five operations per byte are required to generate the key stream

C. Hash Algorithms

A cryptographic hash function takes an arbitrary block of data and returns a fixed-size bit string, hash value, such that an accidental or intentional change to the data will change the hash value. The data to be encoded is often called the "message", and the hash values are sometimes called the message digest or simply digest.

MD2

It was designed to work on 8-bit processors and, in today's 32-bit world, is rarely used. It produces a 128-bit digest. MD2 is different in design from MD4 and MD5, in that it first pads the message so that its length in bits is

Divisible by 256. It then adds a 256-bit checksum. If this checksum is not added, the MD2 function has been found to have collisions.

MD4

Although MD4 is now considered insecure, its design is the basis for the design of most other cryptographic hashes. The algorithm, introduced by Ronald Rivest, takes as input an input message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. The MD4 algorithm is suitable for digital

signature applications, where a large file must be "compressed" in a secure manner before being signed with the RSA public-key cryptosystem.

MD5

While MD4 was designed for speed, a more

Conservative approach was taken in the design of an enhanced version, the MD5, by Rivest himself .MD5 is widely used in several public key cryptographic algorithms and Internet communication in general.

SHA-1

SHA-1 was developed by the NSA for NIST as part of the Secure Hash Standard (SHS). The SHA-1 is required for use with the Digital Signature Algorithm (DSA) as specified in the Digital Signature Standard (DSS).The SHA-1 is for computing and verifying a digital signature at the transmitter and intended receiver. SHA-1 used to protect against "birthday" attacks, where two different messages are selected to produce the same signature.

IV. SECURITY ATTACKS

Some of the most important and easiest to perform network attacks include [8]

• Eavesdropping. The attacker sense data as they traverse a network. Such attacks are possible even when strong cryptography is used

• Tampering. The attacker maliciously modifies data that are in travel on a network. This is type of active attack.

• Spoofing. The attacker generates fake network data to present the illusion that valid data are arriving, when in reality the data are fake.

• Hijacking. The attacker replaces a stream of data on a network with his or her own stream of data.

• Capture/replay. An attacker records a stream of data, and later sends the exact same traffic in an attempt to repeat the effects, with undesirable consequences.

•Man-in-the-middle attack. It is an attack in which an attacker is able to read, insert and modify at will, message between two parties without either party knowing that the link between them has been compromised.

V. SECURITY ASPECTS

The goals of web security include [9]:

• Authentication: In security systems, authentication is the process of giving individuals access to system objects based on their identity. Authentication ensures that the individual is who he or she claims to be.

• Authorization: It is the process of giving someone permission to do something. In multi-user computer system, a system administrator defines for the system which users are allowed access to the system and

Privileges of use.

• Confidentiality: Information possesses confidentiality when it is accessible only to those who are authorized to access it. Confidentiality ensures that computer related assets are accessed only by authorized parties.

• Message Integrity: It deals with methods that ensure that the contents of a message have not been tampered with and altered. Integrity means that assets can be modified only by authorized parties or only in authorized ways.

• Accountability: One of the keys to recovering from an attack is to know who did what, and when they did it.

Knowing that there is a system for accountability dissuades potential attackers.

• Availability: Availability means that assets are accessible to authorized parties at appropriate times. Availability is the proportion of time a system is in a functioning condition.

• Non-Repudiation: Non-repudiation is the concept of ensuring that a party in a dispute cannot repudiate, or refute the validity of a statement or contract. The most common application of this concept is in the verification and trust of signatures..

VI. CONCLUSION

This paper has described briefly about how cryptography works. The reader must beware, however because there are number of ways to attack every one of

these systems; cryptanalysis and attacks on cryptosystems, however, are well beyond the scope of this paper.

Cryptography is a particularly interesting field because of the amount of work that is, by necessity, done in secret. The irony is that secrecy is not the key to the goodness of a cryptographic algorithm. Regardless of the mathematical theory behind an algorithm, the best algorithms are those that are well-known and well-documented because they are also well-tested and well-studied! In fact, time is the only true test of good cryptography; any cryptographic scheme that stays in use year after year is most likely a good one. The strength of cryptography lies in the choice (and management) of the Keys.

REFERENCES

[1] Web Security and Commerce ; "Simson Garfinkel, Gene Spafford" O'Reilly Nutshell Inc

[2] Federal Information Processing Standards Publication 46-3 "SPECIFICATIONS FOR THE DATA ENCRYPTION STANDARD (DES)"

[3] A. Shimizu and S. Miyaguchi, "Fast Data Encipherment Algorithm FEAL" (Advances in Cryptology EUROCRYPT '87 Proceedings, Springer-Verlag, 1988, pp.267 {278).

[4] " Lai, X., Massey, J., and Murphy, S., Markov" Ciphers and Differential Cryptanalysis, Advances in Cryptology –
EUROCRYPT '91, Lecture Notes in Computer Science,Springer-Verlag, 1991

[5] Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) "B. Schneier " Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204.

[6] Lars R. Knudsen, Vincent Rijmen, Ronald L. Rivest, Matthew J. B. Robshaw: On the Design and Security of RC2. Fast Software Encryption 1998: 206–221

[7] Rivest, R. L. (1994). "The RC5 Encryption Algorithm" (pdf). Proceedings of the Second International Workshop on Fast Software Encryption (FSE) 1994e. pp. 86–96.http://theory.lcs.mit.edu/~rivest/Rivest-rc5rev.pdf.

[8] http://www.informit.com/articles/article.aspx?p=23950

[9] Cryptography and network security- Principles and practices ;"William Stallings" Pearson Education Third Edition