International Journal of Advance Research and Innovation
Vol. 2(2), Apr-Jun 2014, pp. 14-20
Doi: 10.51976/ijari.221403
www.gla.ac.in/journals/ijari

Article Info
Received: 02 Apr 2014 | Revised Submission: 20 Apr 2014 | Accepted: 20 May 2014 | Available Online: 15 Jun 2014

Enhancement in TLS Authentication with RIPEMD-160

*Mian Ahmad Zeb**

ABSTRACT

This paper describes one of the security feature authentication. The main goal of this research is to achieve authentication to identify legal user and minimize the chance of attacks. Internet is open to every body to access and share information on it. Unfortunately, the intruders are also there, to examine a web application and its infrastructure to develop his own design, find the potential weaknesses, and use these weaknesses to break or exploit the application for information steeling. There are different kinds of protocol and methods used for security but still threats to the information on internet. Through authentication process, we can control up to some extend the illegal usage of application. We proposed algorithm for authentication that is RIPEMD -160. RIPEMD-160 will capture overall secure authentication.

Keywords: *Transport Layer Security; Threats; Authentication; RIPEMD-160.*

1.0 Introduction

In recent time internet is the most popular and cheap source of advertisement for business and every kind of communication in the world. Internet facilitates different communities (ordinary people, organizations, educational departments' and other government offices) to convey their message to the people and communicate them instantly. Today everybody have access to internet, from home, office, and even from their mobiles. Everything that are developed in field of technology have benefits and as well as drawbacks, so same with the internet. Having access of everybody, so the use of it is little bit risky, that's why different methods and techniques are developed to make it secure. As a lot of work is done to achieve security, speed, reliability, feasibility and quality of service but at same time anti of these and steeling of the secret data techniques are also developed. Mostly organizations and academic institutions are using internet for organizational, business matters, video conferences and sharing of information among themselves and other organization.

Communication technology enables the use of the Internet for email, discussion forums, and collaborative software. But using internet for important business transaction, online meetings and discussion and also e-Learning, the security is the most important feature, because if security is not considered than a lot of problems have to be faced by organizations and institutions. Internet is being open to all kind of sample text and multimedia data trafficking, a lot of attacks are accepted by internet. When an organization uses internet to facilitate their clients ,staff working in different places for quality of service in communication and also improve their staff performance capabilities, they faces the following problems.

1.1 General Internet Predicament

While using internet for above mentioned purpose they faces a lot of problems that are given below.

- Loss of confidentiality of business information i.e. financial records, strategic planning data, engineering models and prototypes, marketing plans, medical records, as well as inability to guarantee the integrity of such information;
- Loss of availability of mission-critical services i.e electronic mails;
- Exposure of critical data about your information infrastructure that can be used by your adversaries in planning their attacks;

**Department of Computer Science Engineering, Pukyong National University Daeyon Campus, Busan, Korean (E-mail: mianahmadzeb@hotmail.com)*

- Legal liability, regulatory liability, or public loss of confidence when your adversaries use one of your computers to carry out attacks against other organizations.

There are much kind of attacks is observed:

- A compromised-key attack occurs when the attacker determines the key, which is a secret code or number used to encrypt, decrypt, or validate secret information.
- The denial-of-service attack occurs when the attacker prevents normal network use and function by valid users.
- Eavesdropping can occur when an attacker gains access to the data path in a network and has the ability to monitor and read the traffic. This is also called sniffing or snooping.
- Spoofing occurs when the attacker determines and uses an IP address of a network, computer, or network component when not authorized to do so.
- A man-in-the-middle attack occurs when an attacker reroutes communication between two users through the attacker's computer without the knowledge of the two communicating users.
- A replay attack occurs when a valid media transmission between two parties is intercepted and retransmitted for malicious purposes.
- A virus is a unit of code whose purpose is to reproduce additional, similar code units. To work, a virus needs a host, such as a file, e-mail, or program.
- A worm is a unit of code that is coded to reproduce additional, similar code units, but that unlike a virus does not need a host. This primarily shows up during file transfers between clients or when URLs are sent from other users [1].

1.2 General view about internet

A general concept of people about the communication on internet is having the following components:

- The network on which we are communicating is reliable and secure
- It is more resilient against the attacker.
- There are procedures for security features like authentication and confidentiality
- The users are also trained to use portal and protect their system and data from the intruders.[1]

2.0 Transport Layer Security

To overcome on problems and make the internet communication secure between the client and server, without making degrading it Transport Layer Security is used (TLS). TLS is the successor to SSL (Secure Socket Layer). TLS can reduce the risk of eavesdropping, tampering, and message forgery mail communications.

Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message.

TLS is the standard protocol. By enabling this encryption/authentication technology you not only secure your internal network, but also the end points trying to connect and authenticate with the server [2].

2.1 Transport layer security structure

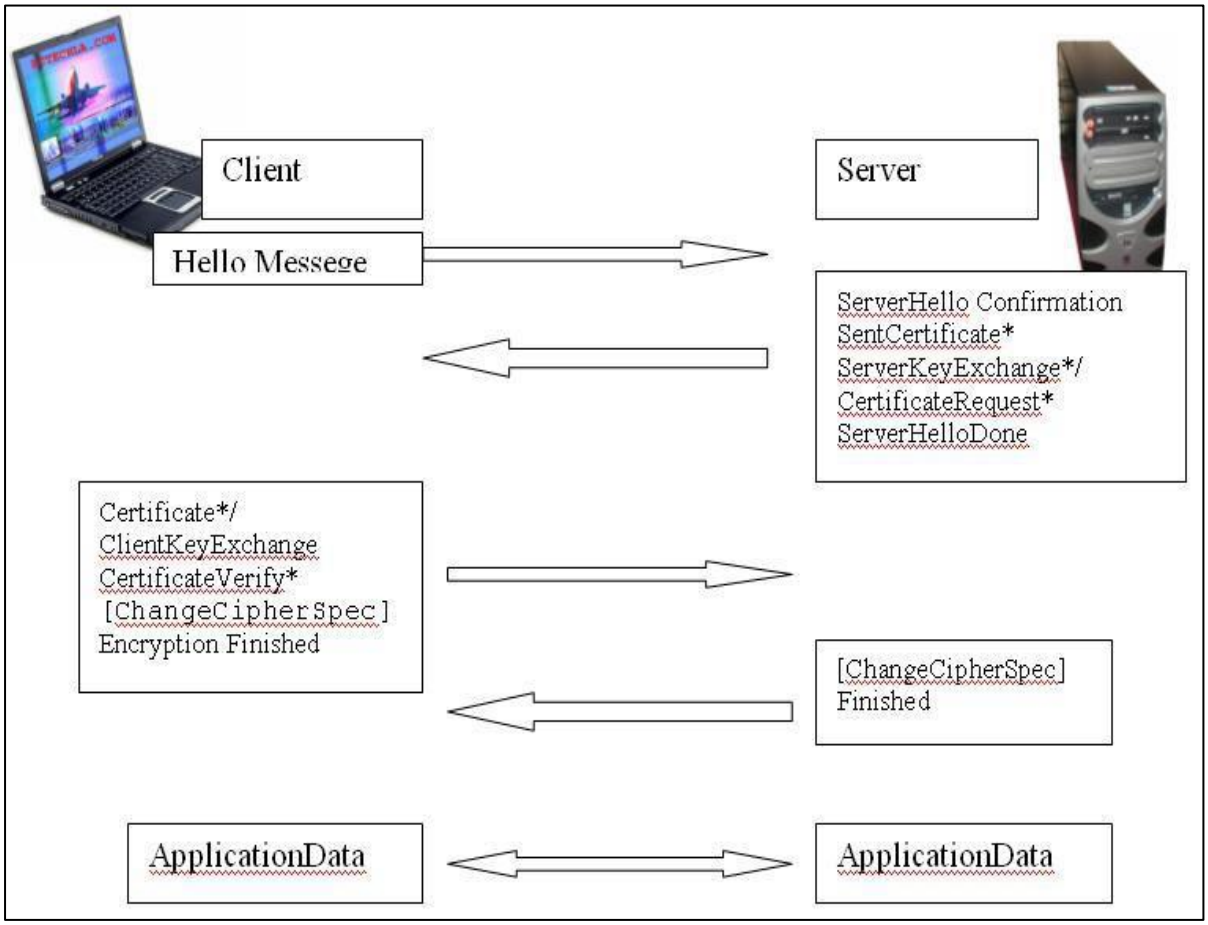
TLS is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol provides connection security with some encryption method such as the Data Encryption Standard (DES).

The TLS Record Protocol can also be used without encryption.

The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged.

The TLS Handshake Protocol first negotiates key exchange using an algorithm.

Fig 1: TLS Handshake Flow Diagram



2.2 Advantages of enabling TLS

1. Greater security
2. Ensured authentic communication between AMT desktop (active management technology) and the server
3. Data integrity
4. Data theft prevention
5. Disallowing un-trusted sources any ability to make use of Pro's powerful functionality
6. Globally accepted
7. Email inspected for Virus
8. Email encryption is transparent
9. Overhead [3].

The TLS (Transport Layer Security) protocol is extensible, means that new algorithms can be added for any of these purposes, as long as both the server and the client are aware of the new algorithms. Many protocols use TLS (Transport Layer Security) to establish secure connections, including HTTP, IMAP, POP3, and SMTP.

2.3 Common security threats

Threats to TLS

There are multiple vulnerabilities in different implementations of Transport Layer Security (TLS) protocols.

- Two certificate message attack: An attacker can send crafted client certificate messages to a server, or attempt to cause a client to connect to a server under the attacker's control. When the client connects, the attacker can deliver a crafted server certificate message.
- Timing Attack: timing attack is a side channel attack in which the attacker attempts to compromise a cryptosystem by analyzing the time taken to execute cryptographic algorithms. Every

- logical operation in a computer takes time to execute, and the time can differ based on the input; with precise measurements of the time for each operation, an attacker can work backwards to the input.
- Convergence threat: When transport layer security mechanism is used, the process of translation makes some problems and opens new attack avenues. TLS channels are established in an end-to-end manner based on the identifiers of the two communicating hosts. These identifiers are the ones employed at the convergence layer. When protocol translation is required, the two end hosts are identified within their respective network realms with different identifiers than the ones used at the convergence layer. Therefore, the TLS channel cannot be established in an end-to-end manner; the host that performs the protocol translation, i.e. the relay node, effectively behaves as a man-in-the-middle. If it is not trusted by both end hosts to perform the translation and participate in the TLS channel then it can eavesdrop on the connection and impersonate any one of them.
- Man in the middle (MITM) attacks: In this type of attack, an intruder intercepts the traffic that is being sent between a client and server, such as by forging DNS replies or by performing ARP redirection. Then, it impersonates the client to the server, and vice-versa. During this attack, the user's web browser does not connect directly to the destination server, but instead to the intruder host, which impersonate the web browser and essentially acts as a proxy.
- Brute-force attack on the session key: This attack can be performed when the intruder knows or can assume part of the clear text that was sent during TLS session, such as the intruder can eavesdrop this session. Then,
- intruder can encrypt the assumed part of the text by using every possible key, trying to find its occurrence in the originally encrypted TLS traffic [4].

2.4 Solution to TLS attack

Several cryptographic techniques and protocols to protect users against MITM attacks:

- Rivest and Shamir proposed the Interlock protocol.
- Jakobsson and Myers proposed a technique called delayed password disclosure (DPD) that can be used to complement a password-based authentication and key exchange protocol to protect against a special form of MITM attack—called the doppelganger window attack.
- Kaliski and Nystr¨om proposed a password protection module (PPM) to protect against MITM.
- Asokan et al. proposed mechanisms to protect tunneled authentication protocols against MITM attacks.
- Parno et al. proposed the use of a trusted device (e.g., a Bluetooth-enabled smartphone) to perform mutual authentication and to thwart MITM attacks [2].
- TLS-SA is the solution to TLS attack.
- Confidentiality using authentication: Authentication is the process of verifying that a message was sent by a given person and this is computed by secret key and the message MAC (Message Authentication Code). This MAC is then appended to the message like a private key encryption because the sender and receiver both share the same secret key [5].

3.0 What is Authentication?

In this study we have observed that most solutions are proposed against the attacks and threats is to make strong authentication. This is more resilient against them.

There are two different words authentication and authorization that some time makes confusion but actually very clear by meaning and functionality.

An authentication system may be as simple as a plain-text password or as complicated as the Kerberos system. In order to verify the identity of a user, the authenticating system typically challenges the user to provide his unique information (his password, fingerprint, etc.) if the authenticating system can verify that the shared secret was presented correctly, the user is considered authenticated.

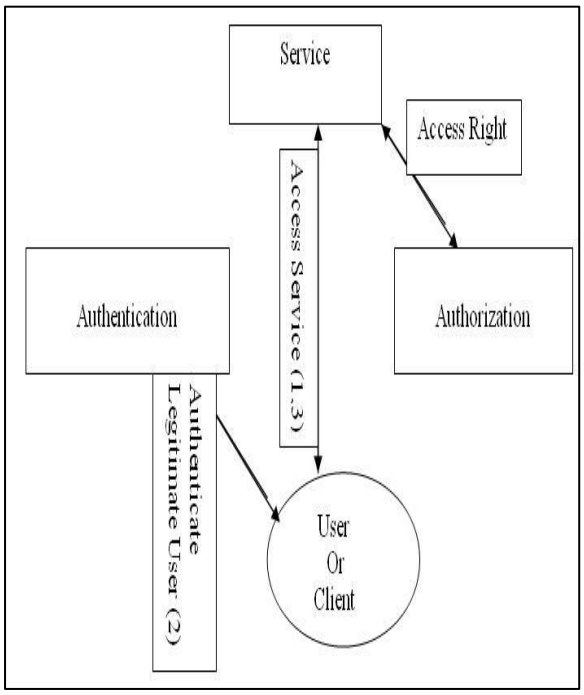
Authorization is the mechanism by which a system determines what level of access a particular authenticated user should have to secure resources

controlled by the system. As database management system provides certain specified individuals with the ability to retrieve information from a database. Authorization systems provide answers to the questions:

- Is user A authorized to access resource R?
- Is user A authorized to perform operation P?
- Is user A authorized to perform operation P on resource R?

MD 5 It is a widely-used well-known 128-bit iterated hash function, used in various applications including SSL/TLS, IPSec, and many other cryptographic protocols [6].

Fig 2: Authentication and Authorization



3.1 Threats to authentication

A kleptographic attack is a forward-engineering attack that is built into a cryptosystem or cryptographic protocol. The attack constitutes an asymmetric backdoor that is built into a smartcard, dynamically linked library, computer program etc [7].

Kleptographic attacks have been designed for RSA key generation, the Diffie-Hellman key exchange, the Digital Signature Algorithm, and other cryptographic algorithms and protocols. Hash functions are among the primitive functions used in cryptography, authentication schemes, message integrity codes, digital signatures and pseudo-random generators. The IHV for the first block is fixed in MD5 and is called the MD5 initial value. Our

presented algorithm together with new conditions we've found allows us to find full MD5 collisions in only minutes on a 3Ghz Pentium4 [8].

3.2 Available solution to authentication

One common tactic to protect older authentication protocols from prying eyes is to encrypt them inside strong tunnels using technologies such as the Transport Layer Security (TLS) and the IP Security protocols (IPSec).

Using a strong tunnel to protect a much weaker legacy method is often called a compound authentication method because a set of protocols is used to accomplish the authentication goal [9].

4.0 Our Proposed Solution & Comparison of Algorithms

Authentication is an important component of security. It is resilience against the access of illegal user to specific data. It is a preliminary process of identification for the legitimate clients. Many algorithms are available for identification, but with development of technology the attacks are also updated. The Transport Layer Security (TLS) protocol which is defined as a proposed Internet standard version for SSL version 3 in uses HMAC algorithm defined as a MAC function. The HMAC function used in the TLS protocol is instantiated either with MD5 or SHA-1 hash functions [12].

Distinguishing, Forgery attack, and computation of output of the compression function are done on HMAC. So as Collision attack is possible on MD5 and SHA-1.

As concern to security that is more important, so we propose an algorithm named RIPEMD-160 (Race Integrity Primitives Evaluation) hash function for authentication for TLS. Because RIPEMD-160 was developed in the response to vulnerabilities it found in MD4 and MD5. The original 128 has same vulnerabilities as of MD4 and MD5. It does twice the processing of SHA-1, performing five paired rounds of 16 steps each for total of 160 operation. With comparison to other algorithm RIPEMD-160 would provide strong security than other hash function although it is little

slow. It can be seen that RIPEMD-160 uses two parallel processes of five rounds, with sixteen operations for each round (5 x 16 operations for the process). This lead us to the logical assumption to use five pipeline stages for each process and a single operation block for each round among with the rest necessary parts. This way not only do we achieve to increase throughput drastically but also keep the hash core small enough.

Moreover, it is the importance of RIPEMD realized and use of RIPEMD-160 combined with HMAC as a keyed authentication mechanism within the context of the Encapsulating Security Payload [ESP] and the Authentication Header [AH]. HMAC with RIPEMD-160 provides data origin authentication and integrity protection [13]. The throughput of RIPEMD can also be enhanced by using different techniques.

The use of RIPEMD-160 is prevention against impersonation and violation of data, this authentication is the assurance that the communicating entity is the one that it claims to be. We used RIPEMD-160 hash function for the authentication. Other hash functions are MD4, MD5 and RIPEMD with different key length. The weaknesses of MD4 are replaced by the MD5, while currently MD5 is becoming insecure one and under attacks.

Table: 1. Comparison of MD5 and RIPEMD-160

	MD5	RIPEMD-160
Digest length	128 bit	160 bits
Basic unit of processing	512 bits	512 bits
Number of steps	64 (4r2ounds of 16)	160 (5paired rounds of 16)
Maximum message size	2^{64}	2^{64}-1 bit
Primitive logical function	5	4
Additive constants used	64	9
Endianness	Little endian	Little endian

The following is comparison of RIPEMD-160 with SHA-1 and MD5

- Brute force attack harder (160 like SHA-1 vs 128 bits for MD5)
- Not vulnerable to known attacks, like SHA-1 though stronger (compared to MD4/5)
- Slower than MD5 (more steps)
- All designed as simple and compact
- SHA-1 optimised for big endian CPU's vs RIPEMD-160 & MD5 optimised for little endian.[11]

The other versions of RIPMD are 128,256,320. But the strengthened version of RIPEMD-160 and expected to be secure for the next ten years.

RIPEMD-160 and SHA-1 are more resistant to Birthday attack but they both showed more resistance in Dos attacks. Although both have bitwise logical operations but it didn't slow the speed than MD5 [10]. RIPEMD-160 provides better security in HASH Algorithms.

5.0 Overall Performance

The objective of TLS (Transport Layer Security) is to provide security over transport layer. So for this different methods were used to get security and quality of service. One of these methods is authentication, different authentication algorithms were used but intruders are always tried to break those algorithms. Providing security to information by secure authentication on TSL. There is proposal, according to which there should authentication for the legal user who can access the data. As MD5 is hash function that provide authentication and resistant to impersonation and intrusion but through some special kind of hardware this hash function could be broken. So it is insecure for strong authentication. I propose RIPEMD-160 to be built with TLS to provide secure transmission of information over the internet. It is more difficult for intruders to get rid of RIPEMD-160.

Comparison of algorithms showed greater difference with each other. We found that RIPEMD-160 has great advantages over the other hash functions.

Table: 2. Result Produced by RIPEMD-160

Algorithm	Word	Cipher text
RIPEMD-160 (For single word)	ahmadzeb	7164785ccbc6f75ae44a81855a0dcd5f42cfdd08
RIPEMD-160 (For complete file)	paper.doc	3067b86de7e3ffaed52d7821d7821e180523414b7e116

6.0 Conclusion

There are many problems with the usage of internet. Different techniques are adopted to override on problem and also made some advancement as precautions. TLS is used to provide security but it is also under attacks, we proposed algorithm RIPEMD-160 for authentication in TLS. With comparison of other algorithm showed good performance. Different version of RIPEMD available like RIPEMD 128,256

References

[1] Common Security Threats http://technet.microsoft.com/en-us/library/bb964031 (loband).aspx

[2] The Bank of New York Mellon "Transport Layer Security" Data Classification August 4, 2008

[3] How to Enable TLS Within Out of Band Management http://www.symantec.com/connect/articles/how-enable-tls-within-out-band-management-70-after-install

[4] Apache 2 with SSL/TLS: Step-by-Step, Part 3 http://www.securityfocus.com/infocus/1823

[5] Confidentiality Using Authentication http://www.acm.org/crossroads/xrds5-2/confide.html

[6] Authentication vs. Authorization http://www.duke.edu/~rob/kerberos/authvauth.html

[7] Kleptography http://en.wikipedia.org/wiki/Kleptography

[8] Marc Stevens "Fast Collision Attack on MD5" Dept of Mathematics and Comp Sc, Eindhoven University of Technology. Netherlands.

[9] Matthew Gast "Security:Which Layer?" Wireless LAN Security Interoperability Lab Page

[10] A. Jalal, Mian Ahmad Zeb "Security Enhancement for E-Learning Portal" CUSIT Peshawar, Pak. IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.3, March 2008

[11] William Stallings Book "Cryptography and Network Security".

[12] Praveen Gauravaram and Adrian McCullagh and Ed Dawson "Attacks on MD5 and SHA-1: Is this the "Sword of Damocles" for Electronic Commerce" March 15, 2006

[13] RFC 2857