International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 5, May - 2014

Security Challenges of RC4 In TLS

Priya Mishra
M.Tech Scholar
JECRC University

Vijay Prakash Sharma
Assistant Professor
JECRC University

Abstract: ***The Transport Layer Security (TLS) provides confidentiality and integrity of data when data transmits across unsecure or untrusted network. TLS supports several encryption methods but in this paper TLS uses RC4 for encryption. RC4 is a stream cipher. It mainly consists of two algorithms. First one is KSA and another is PRGA. RC4 is extremely fast when implemented in software but at the cost of lower security. This paper mainly consists of basic idea about Security, TLS and RC4.***

***Keywords*: TLS(Transport Layer Security), RC4(Rivest Cipher), KSA(Key Scheduling Algorithm), PRGA(Pseudo Random Generation Algorithm).**

I. INTRODUCTION

In today's world, Internet is playing a very important role in our life. It became a part of human body. A human can't live without breathing, in the same way, today he can't live without Internet.

TLS is debatably the most widely used secure communication protocol on the Internet in the present day [1]. Initial life as SSL, the protocol was adopted by the IETF and specified as an RFC standard under the name of TLS [7]. TLS is currently used for securing a broad variety of application-level traffic: It serves, for example, as the starting point of the HTTPS protocol for encrypted web browsing; it is used in concurrence with IMAP or SMTP to cryptographically protect. Email traffic, and it is a well liked tool to harmless communication with embedded systems, mobile devices, and in payment systems. In Technical words, TLS has two consecutive phases: the implementation of the TLS Handshake Protocol which typically deploys asymmetric techniques to create a secure session key, followed by the implementation of the TLS Record Protocol. In which symmetric key cryptography is used in combination with the well-known session key and sequence numbers to make a secure channel for transporting application-layer data. In the Record Protocol, mainly three encryption methods are used:

- CBC-mode encryption using a block cipher with HMAC.
- An encryption by the RC4 stream cipher with HMAC.
- An authenticated encryption with GCM or CCM mode of operation of a block cipher.

The ICSI Certificate Notary lately done study of 16 billion TLS connections and found that half of the (around 50%) transfer was secured using RC4 cipher suites. By this the security of RC4 in TLS is examined. Whereas the RC4 algorithm is recognized to have a diversity of cryptographic weaknesses, it has not been earlier explored how these weaknesses can be broken in the perspective of TLS. This paper shows that latest and newly exposed biases in the RC4 keystream do generate serious vulnerabilities in TLS when RC4 is used as encryption algorithm in TLS. The attacks on RC4 might also be applicable on other protocols when using RC4 for data confidentiality. Like when RC4 is used in WPA protocol for encrypting wireless network traffic then it allow plaintext recovery by using same attack strategy as in TLS.

.

II. SECURITY

Although the terms Protection and Security are same but there is difference between them.

Protection means controlling the access of programs or users to a set of resources. And Security means measuring the assurance of the policies defined for correct management of an environment [5].

Nowadays, the Internet has already become a crucial part of our lives. It's Internet where we access our banking records, credit card statements, tax returns and other highly susceptible personal information. With all the good things the Internet provide us, it has very serious and potentially overwhelming threats.

Unlike commercial and government computer systems, there are very few personal computers that have any safeguards further than basic virus protection. It means whenever you are online, you are a possible target for online criminals and hackers. And if you are using high-speed Internet, then most of the time your computer is online, making Internet criminals and hackers a 24-hour-a-day, your personal information, and your family. Whenever a person access the Internet, then his/her computer sends a message over the network that distinctively identifies his/her computer and also identifies the location of computer. By this the information, requested by that person is returned to the person. Frequently, the requested information by the person carries with it unnecessary secreted software. This software is created by hackers and online criminals. Then this software installs itself on that person's computer and it can either be

just a nuisance or pretense a more serious threat to that person, his/her identity and sensitive financial information. Generally the nuisances are visible and can easily be identify, whereas the more hazardous threats are typically undetectable, quiet, and hard to discover until it's too late.

When a user requests some data on internet then an attacker can access that data in two ways.

1. By Active attack
2. By passive attack

In Active attack the attacker interacts with the system and tries to control its behavior. In this type of attack the attacker can modify the data or can create same false data [5].

In passive attack the attacker just collects information about the target user. In this, attacker does not make any alteration of data [5].

III. BACKGROUND

A. About RC4

Before discussing about RC4, first we know about cryptography.

Cryptography is a method where security engineering meets mathematics means Cryptography is a science in which mathematics is used to encrypt and decrypt the data [6]. Cryptography enables us to store credential information and transmit it over the internet or insecure network so that no one can read it except the receiver of the information. As we know Cryptography is used to secure the data, there is another word Cryptanalysis that means analyzing and breaking secure communication. And Cryptology adopts both cryptography and cryptanalysis.

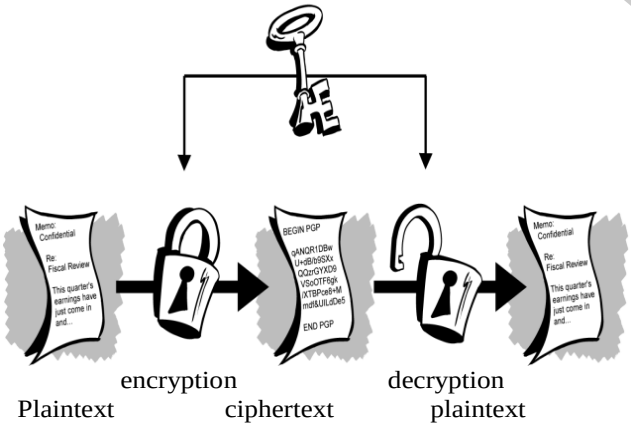

Fig. Encryption and Decryption

At the time when RC4 was developing much of the research in stream ciphers was focused on linear feedback shift registers, or LFSRs [2]. These LFSRs are easy to study from a mathematical point of view, and also making the study of their protection a striking topic. Unfortunately LFSRs use many bit operations, and this makes them slow in software implementations.

RC4 was developed in 1987 by Ron Rivest, who was the co-developer of RSA [2]. And RC stands for "Ron's Code". In compare to LFSRs, RC4 uses byte operations that are more friendly to software implementations, especially when it is used on the 8-bit and 16-bit machines commonly available at the time. The algorithm of RC4 is fairly simple, therefore implementation of RC4 is compact and less error-prone compare to other algorithms such as DES. This makes the use of RC4 in many software packages and also in standards such as Wired Equivalent Privacy (WEP) used in WiFi and the Cellular Digital Packet Data specification. Rivest initially developed RC4 for RSA Security Inc. and this algorithm was kept as a trade secret until 1994. When source code was secretly leaked on the cypherpunks mailing list, since then a lot public research has been done and by doing research many attacks have been found. The RC4 algorithm is quite simple and it leads to a cipher that, regardless of much research and many attacks, is still in use because it is secure enough for many applications.

B. About TLS

Transport layer security (TLS) is probably the most used security protocol, it is widely used for securing web traffic (HTTPS) and also mails, VPNs, and wireless communications. TLS was released because Internet community's demands for a standardized protocol. The IETF provided a location for the new protocol so that it can be discussed openly and encouraged developers. By this they can provide their input to the protocol.

The Transport Layer Security (TLS) protocol was released in January 1999 [4]. TLS protocol creates a standard for private communications. When TLS protocol is used in client/server applications for communication then it prevent eavesdropping, tampering or message forgery. According to the creators of protocol, the goals of the TLS protocol are cryptographic security, interoperability, extensibility, and relative efficiency.

The TLS protocol is composed of two layers: The TLS Record layer and the TLS Handshake layer.

1. TLS Record Layer:

The TLS Record layer is used for encapsulation. It encapsulates various higher level protocols. The TLS record protocol creates a private and reliable connection between the client and the server. However the Record protocol can be used without encryption, it uses symmetric cryptography keys, to ensure a private connection. This connection is protected through the use of hash functions that are generated by using a Message Authentication Code.

2. TLS Handshake Layer:

The TLS Handshake layer consists of the handshake protocol, the alert protocol and the change cipher spec protocol. The TLS Handshake protocol provides authenticated communication to initiate between the server and client. By using this protocol the client and server can communicate using the same language, allowing them to agree upon an encryption algorithm and encryption keys before the selected application protocol begins to send data.

The same handshake protocol can be used in TLS as used in SSL, TLS provides for authentication of the server, and optionally, the client.

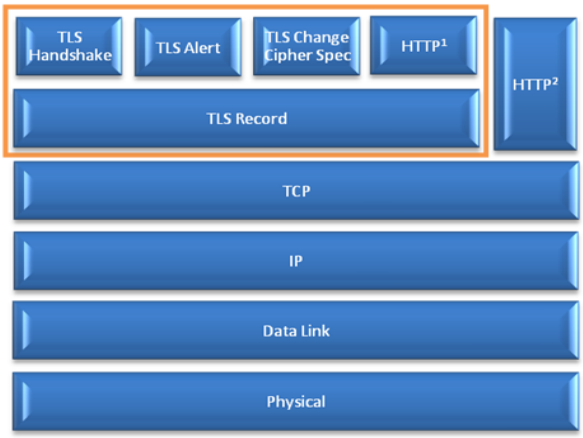

Fig. TLS Protocol Layers

IV. SECURITY OF RC4

RC4 is a stream cipher and is used in a wide variety of cryptosystems like SSL/TLS, WPA, and WEP. RC4 is fairly unique in the world of stream ciphers because of its atypical internal structure, mainly its internal state. We can assume RC4 as a finite state machine that contains some internal state information, and a state change function. And this depends on the current state, and an output function that depends on the internal state. The machine is triggered externally. By doing this the machine first execute the state change function and then return the result of the output function. This general structure can be used to illustrate almost any stream cipher, and in the case of RC4 provides a nice depiction of how the various parts function with each other. RC4 consists of two algorithms: a key scheduling algorithm (KSA) and a pseudo-random generation algorithm (PRGA).

Algo1: RC4 Key Schedule Algorithm
Input: Key k of l words
1. For i = 0 to N − 1
   S[i] = i
2. j = 0
3. For i = 0 to N − 1
   (a) j = j + S[i] + k[i mod l] mod N
   (b) Swap S[i] and S[j].
4. i = j = 0 Output: i, j, S

Algo 2: RC4 Round Algorithm
Input: RC4 state S, i, j
1. i = i + 1 mod N
2. j = j + S[i] mod N
3. Swap S[i] and S[j]
4. Output S[S[i] + S[j] mod N]

In these two algorithms i and j are n-bit words and S[ ] is an array of N = 2^n n-bit words indexed by the values 0 to N − 1. All additions in these two algorithms are carried out modulo N. The initial set-up phase, called the Key Scheduling Algorithm takes a key k[ ] which consisting of l n-bit word. After the set-up phase, the round algorithm is executed once for each word output.

Attacks on RC4: There are two plaintext recovery attacks on RC4 that are vulnerable in specific but realistic circumstances when this cipher is used for encryption in TLS. In both attacks a fixed plaintext is encrypted by using RC4 and transmitted many times in the same, or in multiple independent RC4 keystreams [1]. Interesting candidates for such plaintexts include passwords and, in the setting of secure web browsing, HTTP cookies. The attacks are cipher text only: no complicated timing measurement is needed on the part of the adversary, the attacker does not need to be located close to the server, and no packet injection capability is required.

a) Single-byte bias attack:
In this type of attack the initial 256 bytes of RC4 ciphertext are targeted. Single-byte bias attack is fixed plaintext and multisession also [1]. It means this attack requires a fixed sequence of plaintext bytes to be encrypted independently using a large number of keys. And these keys should be randomly generated. This attack is similar to an attack called as "broadcast-attack". The first 36 bytes of the RC4 keystream are used to encrypt a TLS Handshake Finished message in TLS. This handshake finished message is not fixed across TLS sessions. As a result, this method can be applied only to recover upto 220 bytes of the TLS application plaintext.

b) Double-byte bias attack:
Double-byte bias attack is fixed-plaintext ciphertext-only attack on RC4 [1]. This attack exploits biases that appear in the entire keystream and not just in the first 256 positions. This attack does not assume repeated changes of the encryption key but tolerate them. So this second attack covers those areas where single-byte bias attack does not seem to be applicable. For example, this attack would be able to recover cookies from HTTPS sessions. This attack would also be applicable if the initial keystream bytes from RC4 ciphertext were to be discarded.

In comparison to first single-byte bias attack, second attack exploits certain biases in repeated pairs of bytes in the RC4 keystream. And it was first reported by Fluhrer and McGrew. By evaluating the probability of occurrence for each possible pair of bytes beginning at each position (modulo 256), found a complete view of the distributions of pairs of bytes in positions (i, i+1) (modulo 256). This analysis strongly suggests that there are no further biases in repeated positions of the same strength as the Fluhrer-McGrew biases. And these obtained results are used in a specially designed attack algorithm to recover repeatedly encrypted plaintexts.

V. CONCLUSION

This paper has shown that in today's world, What is the value of internet in a person's life. By using internet a person can send his/her data in any corner of the world, at any time. But internet carries many problems with it. To resolve these problems many cryptographic mechanisms are used. When RC4 is used in TLS for encryption then it is found that plaintext recovery attack for RC4 in TLS is possible for the first 256 bytes of the plaintext stream. So RC4 is not secure but still it is used for encryption due to its fast speed.

REFERENCES

[1] Nadhem AlFardan, Kenneth G. Paterson, Bertram Poettering, and Jacob C.N. Schuldt, Royal Holloway, University of London, Daniel J. Bernstein, University of Illinois at Chicago and Technische Universiteit Eindhoven, On the Security of RC4 in TLS, 2013.

[2] Matthew E. McKague, Design and Analysis of RC4-like Stream Ciphers, University of Waterloo, Canada, 2005.

[3] Santanu Sarkar, Sourav Sen Gupta, Goutam Paul, and Subhamoy Maitra, Chennai Mathematical Institute, Chennai, Indian Statistical Institute, Kolkata, Proving TLS-attack related open biases of RC4.

[4] Karthikeyan Bhargavan, Cedric Fournet, Markulf Kohlweiss, Alfredo Pironti, Pierre-Yves Strub, Implementing TLS with Verified cryptographic security, 2013.

[5] Marco de Vivo, Gabriela O. de Vivo, Germinal Isern, Internet Security Attacks at the Basic Levels.

[6] G. Julius Caesar, John F. Kennedy, Security Engineering: A Guide to Building Dependable Distributed Systems.

[7] ALFARDAN, N. J., BERNSTEIN, D. J., PATERSON, K. G., POETTERING, B., AND SCHULDT, J. C. N. On the security of RC4 in TLS and WPA. Information Security Group at Royal Holloway, University of London, 2013.