The Analysis and Research of Freak Attack Based on OpenSSL

Hong Xia[1, a], Qianqian Pei[2, b] and Yajuan Xi[3, c]

[1]North China Electric Power University, Beijing, China

[2] North China Electric Power University, Beijing, China

[3] North China Electric Power University, Beijing, China

[a]summerdat@ncepu.edu.cn, [b]peiqianqian1@126.com, [c]juanyaxi@163.com

Keywords: Network Communications; OpenSSL; Encryption; Freak Attack

Abstract. Secure Socket Layer (SSL) technology is widely used to provide a safe and secure environment for network communications. But the Secure sockets layer cryptographic library OpenSSL—which includes cryptographic algorithm, cipher code, certificate encapsulation, SSL protocol implementation—is not absolutely safe. Flowing the breaking of the high-risk Heartbleed vulnerability, OpenSSL has appreared a new RSA encryption problem—Freak Attack Vulnerability. This paper makes a deep analysis on the principle of Freak vulnerability, reproduces its attack scene, studies the detection method, and lays a theoretical foundation for further research on the method of vulnerability defense.

Introduction

Network security problem is increasingly serious; all kinds of attack methods emerge in an endless stream. One of the attack methods is named MITM (Man-In-The-Middle) attack, the attack method have a great threat on online banking, online transactions, and so on. Socket Layer Secure [1] (SSL) technology is widely used in order to prevent the MITM attack. It is responsible for the protection of almost all private information on the Internet. SSL usually uses DES [2] (Encryption Standard Data) as the data encryption algorithm, RSA [2] or DH [2] as the key encryption algorithm.

However, SSL is not absolutely safe. OpenSSL [3] has been released the vulnerability --Freak Attack vulnerability. The loophole is RSA encryption vulnerability. The loophole affects 36% of the global SSL sites. Even more ridiculous is that the US National Security Agency website and the US federal government website had the vulnerability, and has been exploited.

Background of Freak Attack

Back in the early 1990s when SSL was first invented at Netscape Corporation, the United States maintained a rigorous regime of export controls for encryption systems. Therefore, companies were required to deliberately 'weaken' the strength of encryption keys. For RSA encryption, this implied a maximum allowed key length of 512 bits. These ‘weak’ keys are called ‘Export Cipher Code’.

Because of International pressure, the United States finally lifted the ban. However, due to historical problems, a lot of software is still dependent on the old encryption protocol. And also because of compatibility issues, now there are still many servers support the export level encryption protocol. Freak attacker uses the vulnerability, reduces the connection level, and makes clients and servers use export cipher suite, which can be broken easily. By this way, the Freak Attack is achieved.

Principle of Freak Attack

MITM Attcak. The implementation of Freak attack is based on MITM attack. MITM attack is an indirect method of network intrusion. ARP (Resolution Protocol Address) deception is the most commonly used method for the MITM attack. The principle of ARP deception is shown in Figure 1.

Attacker B locates between A and C, deceives them that it is the target of AC. When AC communicates with each other, contents are transmitted by B. B can gain and rewrite the information.

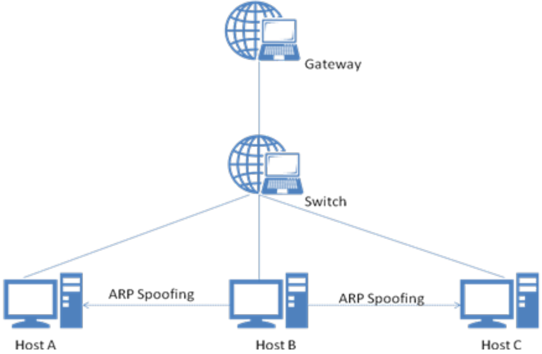


Fig. 1 MITM Attack

Principle of SSL Connection. We usually use SSL to prevent MITM attack. The connection process of SSL is shown in figure 2. Using SSL to establish a secure connection generally requires four steps [4]:

(1) Building security capability

First, client sends 'Hello' to server. The information of client hello includes SSL versions, ciphersuits list, compression algorithms list, random number Rc. Then, server sends 'Hello' to client. The contents of server hello includes SSL version, cipher suit, compression algorithm, and also includes a random number Rs. After this, client and server have established security capability.

(2) server authentication and key exchange

In this process, the digital certification of server is sent to the client, including the server's name, the public key, and the signature of the authority. The client can use the certification to identify sever. And then, server sends its public key to client. Key exchange is related to the algorithm. If the server chooses RSA as key exchange algorithm, the key exchange information is not needed.

(3) client authentication and key exchange

The client decides whether to send certification upon the request of the server. If the server don not request for client certification, the client just needs to echange key. If they use RSA as key exchange algorithm, client does not need to send certification information. The content of key exchange includes the PMS (pre_master_secret), which was encrypted by server's public key.

(4) connection complication

The client and server sent message to tell each other that the session key can be used to encrypt the communication and send "Finish" message to each other.

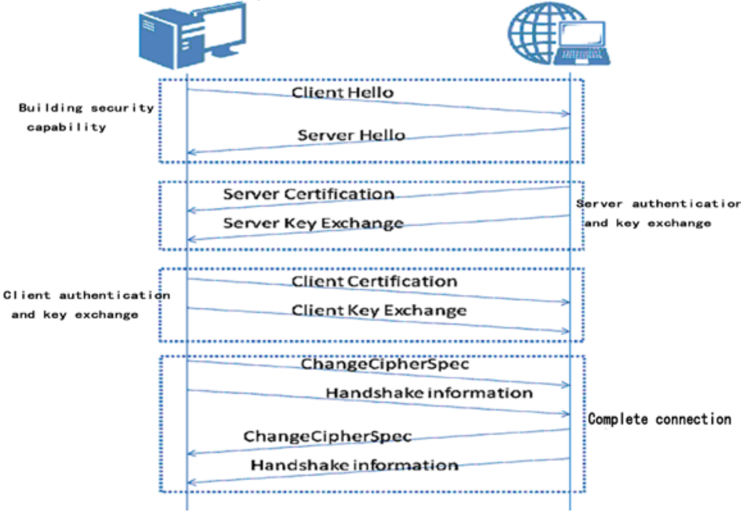


Fig. 2 The process of SSL connection

Principle of Freak Attack. Freak vulnerability is SSL encryption vulnerability. Its whole name is "Factoring Attack on RSA-EXPORT Keys", and CVE number is cve-2015-0204. The vulnerability exists in the OpenSSL communication negotiation method. When the client is connected to the website which supports the export level RSA, attacker can modify the RSA negotiation information, reduce the strength of keys, then get the session key and implement attack through brute force [5].

The vulnerability is located s3_clnt.c [6] file in OpenSSL. S3_clnt.c is used for SSL implementation, including the implementation of SSL, RC4, DES, RSA, lhash and other algorithms. The main functions in this file include: ssl3_connect, ssl3_ client_ hello, ssl3_get_server_hello, ssl3_get_server _certificate, ssl3_get_key_exchange, ssl3_send_client_key_exchange, and so on. These function are used to realize client operation in SSL connection.

Freak attack vulnerability exists in the ssl3_get_key_exchange function in s3_clnt.c. When to establish a connection between server and client, attackers modifies the cipher suites list in client hello to export level to make sure that the server can choose export RSA only. When RSA is used as the encryption algorithm, ServerKeyExchange is not needed. But when use export cipher suite, server needs to send the message. When client receives the message unexpectedly, it should ignore the message or break off the connection. But the existing of the loophole makes the client accept the message, and use the key included in it to encrypt session key. After this, the attack can be received.

Implementation of Freak Attack

Two necessary conditions are needed to achieve SSL Freak attacks: (1) server supports export level cipher suites; (2) the lower encryption suites of client are open.

The implementation process of the attack is shown in figure 3. And detailed process is as follows.

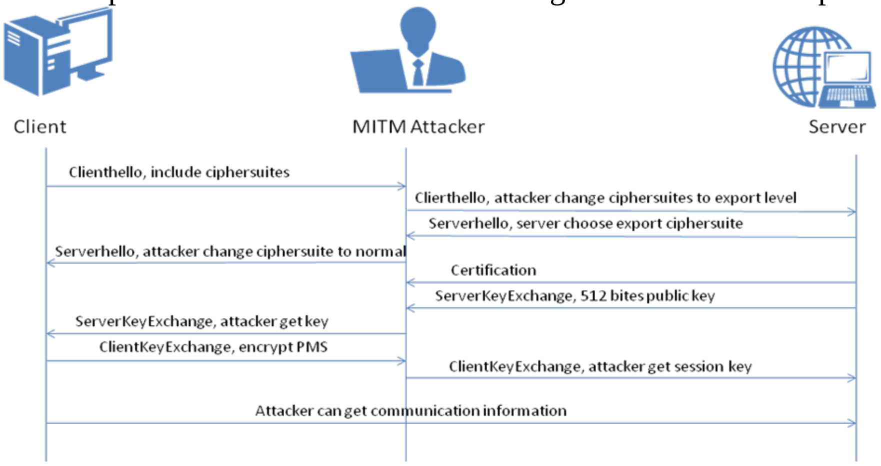

Client
MITM Attacker
Server
Clienthello, include ciphersuites
Clierthello, attacker change ciphersuites to export level
Serverhello, server choose export ciphersuite
Serverhello, attacker change ciphersuite to normal
Certification
ServerKeyExchange, 512 bites public key
ServerKeyExchange, attacker get key
ClientKeyExchange, encrypt PMS
ClientKeyExchange, attacker get session key
Attacker can get communication information

Fig. 3 Freak Attack process

(1) The client sends out Hello message, including the cipher suites list, and a random number Rc used to generate session key. Through this, the client asks the server for RSA password suite.

(2) The attacker gets Client Hello; changes cipher suites in this message to export level.

(3) The server sends Hello message to the client, including the export level suite it chooses, and a random number Rs used to generate session key.

(4) The attacker changes the cipher suite to a normal one included in the client hello message.

(5) The server sends out key exchange message, including a 512 bits EXP_RSA public key.

(6) Due to the existence of the OpenSSL vulnerability, the client accepts the 512 bits public key;

(7) Attacker recovers the corresponding RSA decryption key through the RSA coefficient;

(8) The client uses the 512 bits key to encrypt the Premaster Secret and sends it to the server.

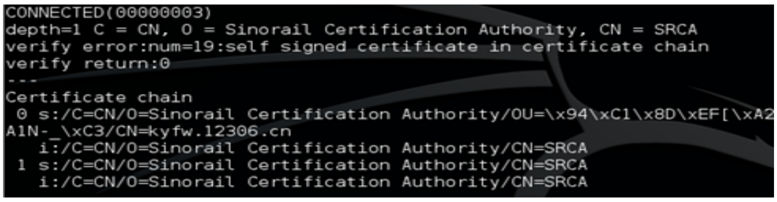
(9) The attacker uses the decryption key to recover PMS to Master Secret, and get the session key.

(10) Since then, the attacker can see the communication plaintext, and can modify it.

Test Methods

The OpenSSL commands can be used to check the Freak vulnerability in a website. This paper detects a number of HTTPS sites, and finds that today, there are still some sites exist the vulnerability. The command, “openssl s_client -connect website: 443 -cipher EXPORT”, can be used to test the target sites.

The figure 4 shows the testing result of a shopping site. It can be found that the website still support export level cipher suites. The site is under the threat of freak attacks.



```
CONNECTED(00000003)
depth=1 C = CN, O = Sinorail Certification Authority, CN = SRCA
verify error:num=19:self signed certificate in certificate chain
verify return:0
---
Certificate chain
 0 s:/C=CN/O=Sinorail Certification Authority/OU=\x94\xC1\x8D\xEF[\xA2
A1N-_\xC3/CN=kyfw.12306.cn
   i:/C=CN/O=Sinorail Certification Authority/CN=SRCA
 1 s:/C=CN/O=Sinorail Certification Authority/CN=SRCA
   i:/C=CN/O=Sinorail Certification Authority/CN=SRCA
```

Fig. 4 Testing result of a shopping site

In addition, RedHat can use the command, "qa|grep - OpenSSL RPM”, and Ubantu or Debian can use the command, "l|grep - OpenSSL dpkg", to detect the OpenSSL version, to detect the loophole.

Preventive Measures

OpenSSL1.01j and all the previous versions are default export-grade RSA key can be used. When it is not convenient to modify the OpenSSL, the purpose of preventing the vulnerability can be achieved by disabling the Export Cipher Suites. Detailed methods are as follows:

(1) Use the command "ciphers MEDIUM OpenSSL" to prohibit the export level RSA cipher suite;

(2) The Apache server can be prohibited from the loophole by modifying the Apache the cipher suites in configuration file to “HIGH:!aNULL:!MD5:!EXP”, and restarting the apache.

(3) The export level cipher suites in Nginx can be forbidden through cinfiguring SSL cipher suite as “ssl_ciphers HIGH:!aNULL:!MD5” and reloading the service.

To completely protect the vulnerability from attack, the existence of the vulnerability should be fixed. Because the broken of EXP_RSA key needs at least 7 hours, new temporary keys can be used to defense attack. As a result, even the key is cracked; the attack can not be putted into effect.The implementation codes are as follows:

```
if (! SSL_C_IS_EXPORT(s->s3->tmp.new_cipher)){
al=SSL_AD_UNEXPECTED_MESSAGE;
    SSLerr(SSL_F_SSL3_GET_KEY_EXCHANGE,SSL_R_UNEXPECTED_MESSAGE);
    goto f_err ;}
```

Conclusion

In this paper, a deep analysis about the principle of Freak attacks based on OpenSSL has been carried out, and the process of the attack has been reappeared. This paper also studies the detection methods, and lays a theoretical foundation for further research on the method of vulnerability defense.

OpenSSL vulnerabilities as middleman attack exploit vulnerabilities; can cause very serious consequences when they break out. As a consequence, people should update fail-safe software in time. In addition, the weak cipher suites should be forbidden promptly. The communication security still haves a lot of work to be done.

References

[1]. Su Cheng, Yin Zhaolin. Analysis and application of the security of SSL protocol. Modern computer, 2002, 29-31 6:

[2].A. O. Freier, P. Karlton, P. C. Kocher. The SSL Protocol Version 3. 0，USA: Network Working Group, 1996: 1-43

[3]. Atul Kahate. Cryptography and network security. tsinghua university press, 2009.

[4]. Xu Jing, Chang Chaowen. Analysis of the security of SSL protocol. Micro computer information, 2006, 22 (3): 3-4

[5]. Shaozhen Chen. Cryptography tutorial. Science Press, 2012

[6]. Xie Fei. A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Engineering. Huazhong University of Science & Technology. 2007