Performance Evaluation of SSL with New Client Authentication

Takuya Yahagi s1090215 Supervised by Hiroshi Toyoizumi

Abstract

The purpose of this paper is to find effective use of Secure Socket Layer(SSL) with Feige-Fiat-Shamir Identification Protocol for client authentication, which prove one's identity without its knowledge. This protocol has 50% chance of finding malicious user per one trial, and it becomes better by increasing the number of trials. In this paper, we find most effective point of number of trials by trade-off between probability of finding malicious user and processing time.

1 Introduction

Many people connect PC to Internet and communicate information. When we communicate information on the Internet, there is a danger of eavesdropping, spoofing, and so on. For example when a client who is mail user receives mail from a server who provides mail service, the client sends user name and password. The eavesdropper is able to know the user name and password easily. When the client sends mail, the server doesn't certify the sender's identity. It means that any person can use others' mail address. In fact, phishing mail, spam, and some kind of virus mail use others' mail address or non-existent mail address. For example, phishing mail is sent by an other host using well-known bank's, credit card company's, and Internet shopping site's mail address. Cryptography protects information from such danger.

Secure Socket Layer(SSL) [2] provides cryptography communication for mail, WWW, and so on. SSL has three steps to begin cryptography communication: authentication, key exchange, and encrypting. First, the client checks the server's identification in the authentication step, Second, the client exchanges key which is used to encipher message. Finally the client and the server begin to communicate using cryptography. In the authentication step, SSL uses Digital Signature to certify. Digital Signature contains personal information, so this method is usually used to certify the server and not good to certify the client. But if there is no client authentication, a malicious person may try to spoof, and use your mail address. So it requires client authentication.

Sender ID [5] is a method for preventing spoofing mail by checking sender's mail address and IP address. Sender ID asks domain part of mail address for Domain Name System(DNS), and then checks returned IP address is same as sender's IP address. If IP address is not same, mail is rejected. This method is based on the integrity of IP address, but if IP address is also forged, this method can't prevent spoofing.

Some methods for client authentication such as Rivest Shamir Adleman (RSA) authentication, Challenge Handshake Authentication Protocol (CHAP), and so on are available, but we use Feige-Fiat-Shamir Identification Protocol [6]. This method can prove identity via demonstration of knowledge of secret without revealing even a single bit of secret. However, when some malicious person tries to be an authenticated user, this Protocol has a 50% chance of finding an malicious user per one trial. Increasing the number of trials, the probability of finding the malicious user becomes larger, while time for confirmation gets longer. So it is necessary to find most effectual number of trials.

The purpose of this research is to evaluate performance of SSL with Feige-Fiat-Shamir Identification Protocol. In this paper, we model SSL with authentication using M/G/1 queue to calculate the waiting time and find effectual method for its use by trade-off between probability of finding malicious user and waiting time.

2 SSL

SSL is used for cipher communication. For example, there are two entities, a server who provides mail service, and a client who wants to send mail using the cryptography. To begin cryptography communication, client and server have to decide specification of cryptography such as cryptography algorithms, and method of key exchange. In SSL, the client and server send some messages to decide specification(See figure 1).

First, the client sends "Client hello"(1) which contains random values and available encryption algorithms list, key exchange algorithms list and so on to server. The server responds "Server hello"(2) which contains random values and selected algorithm, and also sends "Server certificate" and "Server hello done" to the client. Client verifies server's identification by checking the Server certificate. The server certificate contains a public key which is necessary to exchange common key. Messages after Server certificate are encrypted using public key and sent to server. If there is no public key in Server certificate or the server doesn't send Server cer-

tificate, server sends Server key exchange to create public key. Then server sends ”Server hello done” to finish Hello phase. In Hello phase, the server sends certificate to prove his identity, but the client doesn't prove identity. Next, client sends ”Client key exchange”(3) including premaster secret which is to create common key, ”Change cipher spec”(4) and ”Finished”. Change cipher spec is signal transition in ciphering strategies. Server also sends Change cipher spec and Finished and begins to communicate encrypted application data.

In this case, server doesn't check identification of client. There is the possibility that a malicious person tries to spoof. So it requires client authentication.

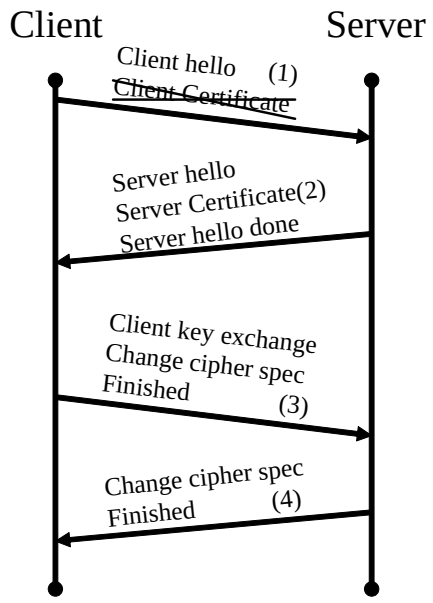


Figure 1: SSL with no client authentication

3 Authentication Method

One of the authentication methods is Arbitrated Protocols. Arbitrated Protocols is suited for identification of owner of a credit card, ID card, or computer account. In the Arbitrated Protocols, Feige-Fiat-Shamir Identification Protocol [6] can prove identity via demonstration of knowledge of secret such as Personal Identification Number(PIN) or password without revealing even a single bit of secret.

3.1 Feige-Fiat-Shamir Identification Protocol

Suppose that there are two persons, Alice and Bob, and Alice wants to prove her identification by proving that she knows a secret to Bob. This method checks that she can calculate some value based on secret number. She has secret number and opens remainder of square of secret number divided by n, where n is large number. Bob checks she can calculate value or not using this open value. He can't find secret number from open value.

Before Alice proves her identification to Bob, they need to register their secrets to trusted a third person, Trent. Registration stage is following:

(1) Trent chooses a modulus $l = pq$, where p and q are large prime and roughly same size numbers to be kept secret and number of trials n.

(2) Alice and Bob respectively randomly select secret natural numbers s_A and $s_B \leq l - 1$ with $gcd(s_A s_B, l) = 1$.

(3) Alice and Bob compute respectively the smallest natural numbers t_A and t_B such that $t_A = s_A^2 \bmod l$ and $t_B = s_B^2 \bmod l$ and resister secrets s_A and s_B with Trent
t_A and t_B don't need to be kept secret

After Registration stage, to prove identification of Alice to Bob, they implement following steps:

(1) Alice selects an m, such that $m \leq l - 1$ and sends $w = m^2 \bmod l$ to Bob

(2) Bob chooses $c = 0$ or 1 and sends it to Alice

(3) Alice computes $r = ms_A^c \bmod l$ and sends it to Bob

(4) Bob computes $r^2 \bmod l$

   (a) If $r^2 = wt_A^c$ then
      i. if $n = 0$ then terminates this protocol and accepts Alice.
      ii. else $n = n - 1$ and go to step (1)
   (b) If $r^2 \neq wt_A^c$ then terminates this protocol and rejects Alice

Figure 2 shows the example of this protocol, when p and q are 17 and 13 and $l = 221$. Preliminarily, Alice and Bob chooses $s_A = 16$ and $s_B = 15$ and calculates $t_A = 16^2 \bmod 221 = 35$ and $t_B = 15^2 \bmod 221 = 4$. Alice chooses $m = 219$ and calculates $w = 219^2 \bmod 221 = 4$, and then sends $w = 4$ to Bob. Bob chooses $c = 1$ and sends it to Alice. Alice calculates $r = 219 \times 16^1 \bmod 221 = 189$ and responds it to Bob. Bob calculates $189^2 \bmod 221 = 140$ and $wt_A^c = 4 \times 35^1 = 140$, and then checks that $r^2 \bmod l$ equals wt_A^c or not. In this case $r^2 \bmod l = wt_A^c$, and Alice passes this trial.

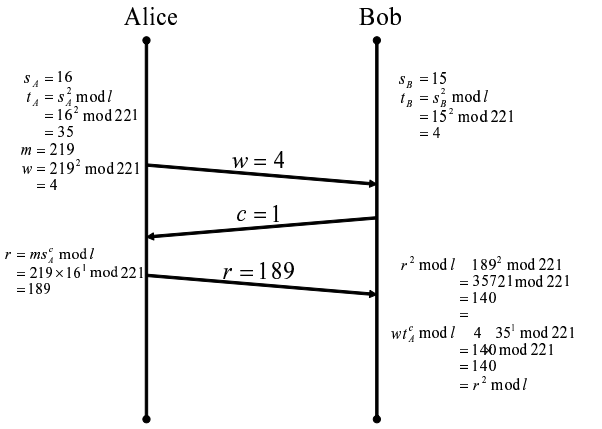


Figure 2: Feige-Fiat-Shamir Identification Protocol example

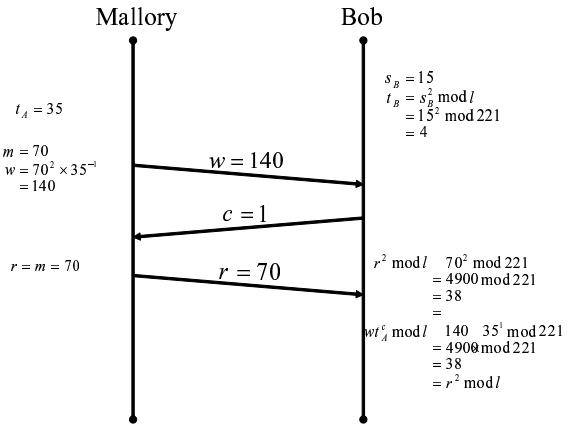


Figure 3: Spoofing example

3.2 Spoofing Method

Suppose a malicious person Mallory tries to spoof Alice, and doesn't know s_A. Though, he has a chance of passing this trial with following steps:

He selects an m such that $0 < m < l - 1$ and sends:

(1) $w = m^2$, if he guesses that Bob will send $c = 0$

- (a) If Bob chooses $c = 0$, then Mallory sends $r = m$
  Bob computes $r^2 = m^2 = wt_A^0 \bmod l$ and accepts Mallory
- (b) If Bob chooses $c = 1$, then Mallory can't send $r = ms_A^c$ and Bob rejects Mallory

(2) $w = m^2 t_A^{-1}$, if he guesses that Bob will send $c = 1$

- (a) If Bob chooses $c = 0$, then Mallory can't send r such that $r^2 = wt_A^c$ and Bob rejects Mallory
- (b) If Bob chooses $c = 1$, then Mallory sends $r = m$
  Bob computes $r^2 = m^2 = wt_A^{-1} t_A^1 = wt_A^1 \bmod l$ and accepts Mallory

This means that Mallory has a 50% chance of passing this Protocol per one trial [6].

Figure 3 shows example spoofing when Mallory guesses that Bob will send $c = 1$ and hits his guess. Mallory selects $m = 70$, calculates $w = 70^2 \times 35^{-1} = 140$ and sends it to Bob. Bob selects $c = 1$ as he expected. Mallory responds $r = m = 70$. Bob calculates $r^2 \bmod l = 38$ and $wt_A^c \bmod l = 38$. Then Mallory can pass this trial without s_A.

4 Modeling

The probability of finding Mallory becomes larger by increasing the number of trials, but it takes a great deal of time. So we have to think the trade-off between the probability of finding and waiting time. In this section, we calculate probability of finding, model SSL and SSL with authentication protocol using M/G/1 queue and then obtain these waiting time to compare and evaluate waiting time of SSL with SSL with authentication.

4.1 Data capture

To calculate waiting time of SSL, we need to know service time of SSL s_{SSL}. We build a simple network which consists of client and mail server applied SSL to obtain service time of SSL. Client reserves mail from server and capture these packets using Sniffer [8]. Then we check time of each packet arrives to client. Figure 4 shows service time of each section of SSL.

4.2 Waiting time of SSL

We consider the mean waiting time of SSL. Figure 5 shows SSL service and its waiting time of each client. First client C1 comes to server and receives SSL service. Before completion C1's SSL communication, C2 comes to server and he has to wait until C1 finishes service. After C1 leaves server, C2 begins to receive service and also C3 comes to server in the middle of C2's service. We define time from client arrives server to leaves as waiting time of SSL. To be served client and server always send same number of messages, so we suppose that service time of SSL is same. Let N_{SSL} be a number of client, λ be a rate of incoming client and $\frac{1}{\mu}$ be a service time of SSL. By Pollaczek-Khinchin formula [9] for M/G/1 queues, expectation value of number of SSL clients is

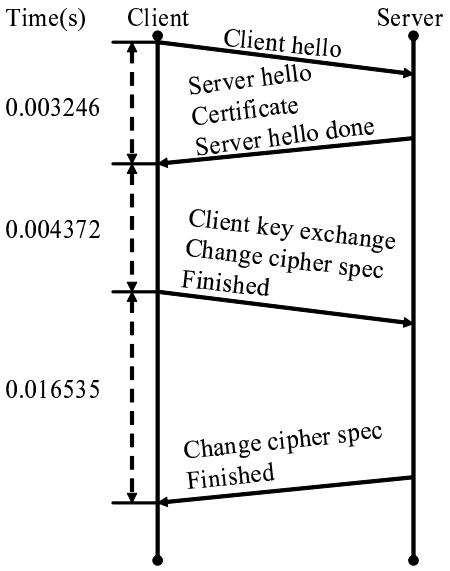


Figure 4: Service time of SSL

$$E[N_{SSL}] = \rho + \frac{\rho^2 + \lambda^2\sigma^2}{2(1-\rho)}, \tag{1}$$

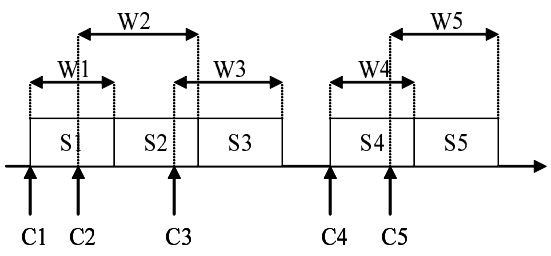
where

$$\rho = \frac{\lambda}{\mu}.$$

Since service time of SSL is always same, variance of service time $\sigma^2 = 0$, then by Little's formula [9], we obtain expectation of waiting time of SSL by

$$E[Y_{SSL}] = \frac{2-\rho}{2\mu(1-\rho)}, \tag{2}$$

where Y_{SSL} represents waiting time of SSL.



C: Client
W: Waiting time of SSL
S: Service time of SSL

Figure 5: State of each client receives SSL service

4.3 Waiting Time of SSL with Authentication

Next, we consider the mean waiting time of SSL with authentication. As section 4.2, service time of SSL is always same, but service time of authentication changes by number of trials up to find Mallory. First we find expectation and variance of number of trials. Let N_M be a Mallory's number of trials, N_A be a Alice's number of trials, x be a probability of finding Mallory per one trial which is 50% in section 3, and n be a number of trials. Expectation value of Mallory's number of trials is

$$\begin{aligned} E[N_M] &= \sum_{k=1}^{n} kx(1-x)^{k-1} + n(1-x)^n \\ &= \frac{1-(1-x)^n}{x}, \end{aligned} \tag{3}$$

and the variance is

$$\begin{aligned} Var[N_M] &= \sum_{k=1}^{n} k^2 x(1-x)^{k-1} + (E[N_M])^2 \\ &= \frac{1-x}{x^2} - \frac{(2n-1)x(1-x)^n}{x^2} \\ &\quad - \frac{(1-x)^{2n}}{x^2}. \end{aligned} \tag{4}$$

Since Alice always passes this trial, Alice's mean number of trials $E[N_A]$ is n, and variance $Var[N_A]$ is 0.

Then expectation value and variance of Mallory's service time of SSL with authentication are

$$E[S_M] = s_{auth}E[N_M] + s_{SSL}, \tag{5}$$

and

$$Var[S_M] = s_{auth}Var[N_M], \tag{6}$$

where s_{auth} and s_{SSL} are service time of trial and SSL, and S_M represents Mallory's service time of SSL with authentication.
Similarly, expectation value and variance of Alice's whole service time are

$$E[S_A] = s_{auth}E[N_A] + s_{SSL}, \tag{7}$$

and

$$Var[S_A] = s_{auth}Var[N_A] = 0, \tag{8}$$

where S_A is Alice's service time of SSL with authentication.
Next, we find whole service time. Let α% are Mallory in all users, $\frac{1}{\mu}$ be a average of service time and σ^2 be a

variance of service time. Whole expectation value and variance of service time are following:

$$\frac{1}{\mu} = (\alpha E[S_M] + (1-\alpha)E[S_A]) + S_{SSL}, \quad (9)$$

$$\begin{aligned}\sigma^2 &= \alpha Var[S_M] + (1-\alpha)Var[S_A] \\ &\quad +\alpha(E[S_M])^2 + (1-\alpha)(E[S_A])^2 \\ &\quad -\alpha E[S_M] + (1-\alpha)E[S_A])^2. \end{aligned} \quad (10)$$

By Pollaczek-Khinchin formula, expectation value of number of clients is

$$E[N_{auth}] = \rho + \frac{\rho^2 + \lambda^2\sigma^2}{2(1-\rho)}, \quad (11)$$

where $\rho = \frac{\lambda}{\mu}$, and N_{auth} is number of client.

By Little's formula, expectation value of waiting time of SSL with authentication is obtained by

$$E[Y_{auth}] = \frac{E[N_{auth}]}{\lambda}, \quad (12)$$

where Y_{auth} is waiting time of SSL with authentication.

4.4 Probability of missing Mallory

Also we consider the probability of missing Mallory. The probability of failing to find Mallory per one trial is represented by $1-x$ then probability of missing Mallory in n trials is

$$p(n) = (1-x)^n. \quad (13)$$

5 Results

Figure 6 shows graphs of the mean waiting time of SSL and SSL with authentication with number of trials $n = 5$, $n = 15$, and $n = 20$, when $x = 0.5, \alpha = 0.01, s_{SSL} = 0.016535$, and $s_{auth} = 0.004$ using equation (2) and (12).

Figure 7 shows graphs of probability of missing Mallory with $x = 0.5$ represented by (13). Probability of missing Mallory when $n = 5$ is 3.125×10^{-2}, $n = 15$ is 3.05176×10^{-5} and $n = 20$ is 9.53674×10^{-7}

Capacity of server applied SSL and authentication with n = 5 is large, on the other hand probability of miss when n = 5 has 3.125 %. When n = 20, probability of miss is enough small, but capacity of server is not sufficient. SSL with authentication when $n = 15$ is effective with waiting time and probability of finding point of view.

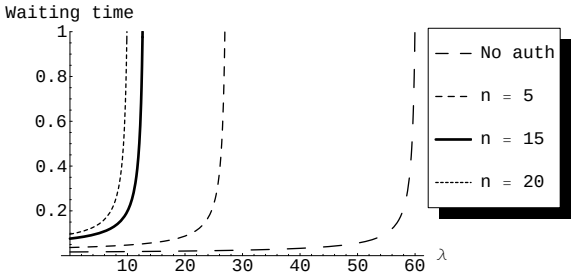


Figure 6: These graphs are waiting time of SSL with no authentication, SSL with authentication $n = 5$, $n = 15$ and $n = 20$ the order from the right.

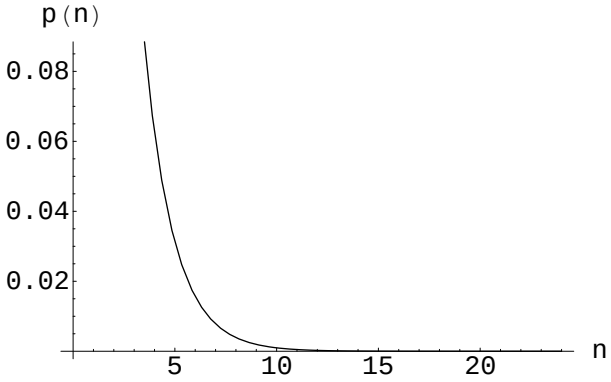


Figure 7: Probability of missing Mallory

6 Conclusion and Future Works

We find effective point of number of trials $n = 15$ by trade of between probability of finding Malloy and waiting time. Riding on the feature of this authentication which can prove identity without sending any personal information to server, client can use client authentication more securely. Further, this method is solution to IP address spoofing which is problem of Sender ID. Using this method, server can apply client authentication to SSL effectively and securely.

However, service time of authentication s_{Auth} and probability of incoming Mallory α is not accurate value. We need to capture these data in the future.

Acknowledgement

I would like to thank Prof. Hiroshi Toyoizumi for his advice on this research, and Prof. Martha Clark Cummings for her help with the writing of this paper. Also I would like to thank member of Performance Evaluation Laboratory for their help.

References

[1] CNET Japan, “http://japan.cnet.com/news/sec/story/0,2000050480,20076884,00.htm,” .

[2] A. O. Freier, P. Karlton, and P. C. Kocher, “The SSL Protocol Version 3.0, http://wp.netscape.com/eng/ssl3/draft302.txt.” .

[3] @IT, “http://www.atmarkit.co.jp/,” .

[4] M. Lentczner and M. Wong, “Sender Policy Framework: Authorizing Use of Dmains in MAIL FROM draft-lentczner-spf-00, Internet-Draft,” .

[5] J. Lyon and M. Wong, “Sender ID: Authenticating E-Mail, Internet-Draft,” .

[6] R. A. Mollin, Rsa and Public-Key Cryptography(Discrete Mathematics and Its Applications), Chapman & Hall, 2002.

[7] S. M. Ross, Applied Probability Models With Optimization Applications, Dover Pubns, 1992.

[8] Sniffer Technologies, “http://www.toyo.co.jp/sniffer/,” .

[9] H. Toyoizumi, “Performance Evaluation, http://www.u-aizu.ac.jp/~toyo/lectures/pe/pe-ex.htm.’’ .