A Novel Security Scheme with Message Level Security for Hybrid Applications

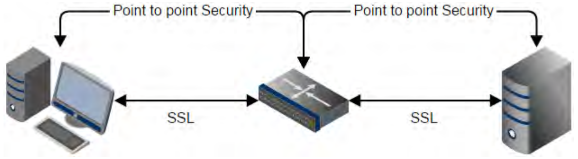
Suoning Ma*, Inwhee Joe*
*Dept. of Computer & Software Engineering, Hanyang University
e-mail : msnlly@hanyang.ac.kr

Abstract

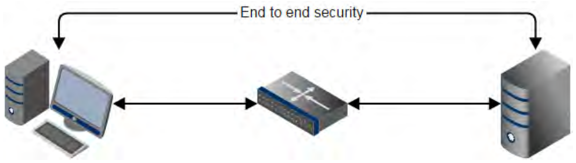
With the popularity of smart device, mobile applications are playing more and more important role in people's daily life, these applications stores various information which greatly facilitate the user’s daily life. However due to the frequent transmission of data in the network also increases the risk of data leakage, more and more developers began to focus on how to protect user data. Current mainstream development models include Native development, Web development and Hybrid development. Hybrid development is based on JavaScript and HTML5, it has a cross platform advantages similar to Web Apps and a good user experience similar to Native Apps. In this paper according to the features of Hybrid applications, we proposed a security scheme in Hybrid development model implements message-level data encryption to protect user information. And through the performance evaluation we found that in some scenario the proposed security scheme has a better performance.

1. Introduction

Smart phone has changed the traditional way of life and the way of communication, the network type also changed from the traditional Internet to the mobile Internet. With the rapid development of mobile Internet the ensuing security problems have gradually aroused people’s attention. Traditional Internet security depends on the transport-level security protocols like SSL, as shown in Figure 1. All the data is encrypted only on the data link layer, during the transmission the encrypted data needs to be decrypted and re-encrypted by each node until it reaches the destination. But in mobile internet, data from the beginning to the end will go through many nodes, the encrypted data will be exposed in plain text on each node, if some node security measures are weak, it will cause the leakage of information, so the security mechanism used in the traditional Internet has been unable to adapt to the current mobile Internet. Therefore mobile Internet environment need to achieve the message-level security as shown in Figure 2, data is encrypted at the sending end and decrypted at the receiving end, data does not appear in plain text at the intermediate node. In this paper, we proposed a security scheme for hybrid development in mobile internet environment including dynamic verification and data encryption.



(Figure 1) Transport Level Security

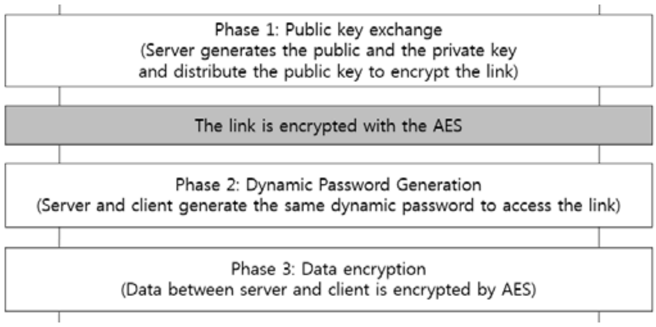


(Figure 2) Message Level Security

2. Design and Implementation of Security Scheme

2.1 Security Scheme for Hybrid Application

In this section , we will introduce the proposed security scheme. Under this security scheme, provided dynamic verification and data encryption to protect authenticated user information. From the user login to use the built-in functions to transfer or request data from the server goes through three stages, as shown in Figure 3. The data encryption using symmetric encryption, during the exchange of symmetric key between server and client the symmetric key is encrypted by asymmetric encryption algorithm.


Phase 1: Public key exchange
(Server generates the public and the private key
and distribute the public key to encrypt the link)
The link is encrypted with the AES
Phase 2: Dynamic Password Generation
(Server and client generate the same dynamic password to access the link)
Phase 3: Data encryption
(Data between server and client is encrypted by AES)

(Figure 3) Security Scheme

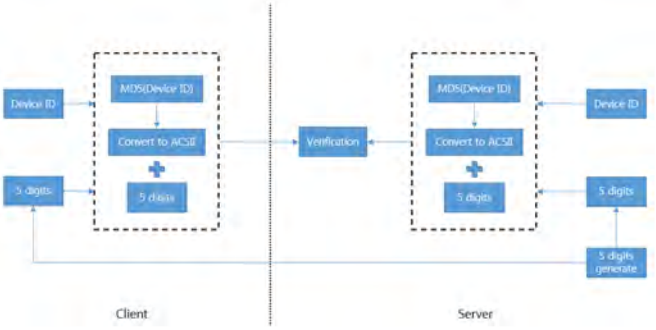
2.2 Phase 1: Public key exchange

This stage is the core stage of the entire security scheme. Firstly, server generates a key length of 1024 bits public key and private key wait for connection request from client. After receiving a public key request from a client, server will return generated public key to client. After the client receives the public key, it will generate 256-bit symmetric key and encrypt it by public key then send it back to the server, server decrypts the symmetric key through its own private key, and now the client and server are complete link encryption.

2.3 Phase 2: Dynamic Password Generation

Dynamic password authentication technology is adding change factor in user login process so that each authentication data transmitted in the network are different. Dynamic password authentication using dual operational factors generating a dynamic password.

In this security scheme, using device id as seed and random parameters as the change factor. Device id was already fetched by calling local API and stored in the database during user registration stage. When user try to login, user's login information will be encrypted and transmitted by the first phase of the establishment of the symmetric encryption link. After verifying the login information server will randomly generate 5 digit number as change factor and transmit it through the encryption link. Now client and server have the same seed and the same change factor. Client calculate the MD5 value of the device id to get a new 32-bit string and calculate the ASCII summation of all the characters in this string and then add the value of change factor to generate a 5 digit dynamic password. Server side using the same way to generate dynamic password as shown in Figure 4.



(Figure 4) Challenge asynchronous dynamic password

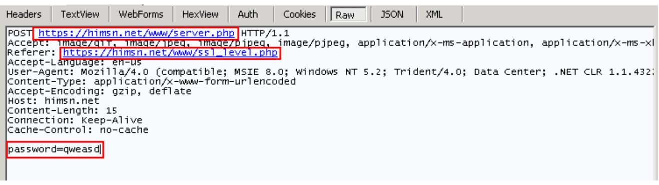
2.4 Phase 3: Data Encryption

When user successfully logged in then goes to the Phase 3. This phase data encryption using symmetric encryption algorithms, but the update of the symmetric key is different from the Phase 1. The symmetric key will be transmitted by custom http header. Before the client send HTTP requests to the server, it will customize a HTTP request header named X-key. Its value is a symmetric key encrypted by public key. Client encrypt the data through the key and send the modified HTTP request which a customize header contain the key. Server side receives the HTTP request and take out the value of customize header decrypt by its own private key. And using the decrypted symmetric key to get the real data from client. The response also encrypted by this key. Thus, implement the message-level encryption of data between the client and the server.

3. Analysis and Performance

3.1 Security analysis

This security scheme implements the message-level data encryption which relative to the traditional SSL data encryption reduces the dependence of the data on the reliability of the intermediate nodes. HTTPS using transport-level security encryption to protect point-to-point data, but between the send side and receive side existing insecure nodes, transmitted data can be read in the intermediate node as shown in Figure 5. We see that although the data using the HTTPS encryption method, but the data can be read in plain text.

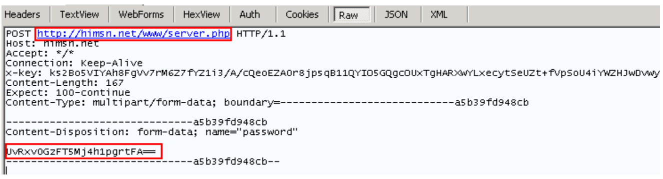


```
POST https://himsn.net/www/server.php HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-ms-application, application/x-ms-xl
Referer: https://himsn.net/www/ssl_level.php
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0; Data Center; .NET CLR 1.1.432
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: himsn.net
Content-Length: 15
Connection: Keep-Alive
Cache-Control: no-cache

password=qweasd
```

(Figure 5) Transport Level Security Issue

But if the message-level encryption method is used it can be guaranteed even if the data is passed through an unreliable intermediate node, since lack of symmetric key the data remains encrypted state as shown in Figure 6. HTTPS was not used but there is a new customize http header named x-key. Its value is encrypted by public key so that only the one has the private key can decrypt it and use the decrypted key to get the real data from user.



```
POST http://himsn.net/www/server.php HTTP/1.1
Host: himsn.net
Accept: */*
Connection: Keep-Alive
x-key: ks2Bo5VIYAh8FgVv7rM6Z7fYZ1i3/A/cQeoEZA0r8jpsqB11QYIO5GQgcOUxTgHARXWYLxecytSeUZt+fVpSoU4iYWZHJwDvwy
Content-Length: 167
Expect: 100-continue
Content-Type: multipart/form-data; boundary=---------------------------a5b39fd948cb

-----------------------------a5b39fd948cb
Content-Disposition: form-data; name="password"

UvRxv0GzFT5Mj4h1pgrtFA==
-----------------------------a5b39fd948cb--
```

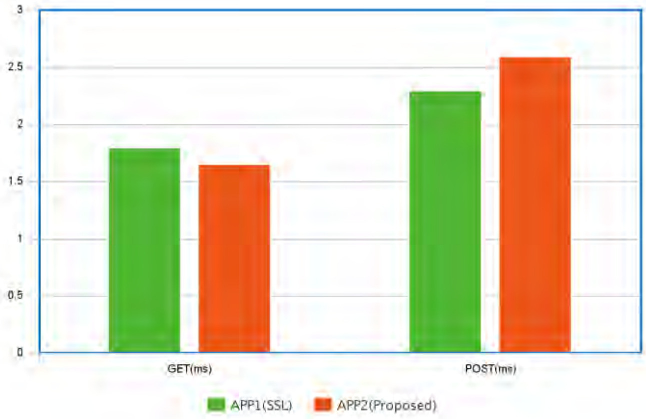
(Figure 6) Message Level Security

This security scheme not only uses the common user authentication but also add dynamic password authentication. It using device id as seed and random parameter as change factor to generate dynamic password. The dynamic password is a random 5 digit number has a very low repeatability, reduced the possibility of replay attacks and improve the system security.

3.2 Performance Evaluation

The security scheme is close to transport-level security. The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating computer applications. Contrast the former, we proposed security scheme is based on message-level security add dynamic password authentication. In order to have a clear result to reproduce performance tests, we measurement the average processing time of two hybrid applications under the different security scheme in two scenarios (GET, POST) on the same environment (Samsung Galaxy S3). Application 1 is using SSL and Application 2 is using we proposed security scheme.

In GET scenarios，two applications request the same size of the data to the server. In POST scenarios, two applications submit the same size of data to server. The results of the average response time as shown in Figure 7.



(Figure 7) Average processing time

4. Conclusion

With the development of computer technology, people pay more and more attention to network security. In order to ensure the user's data security, it is an important way to establish a perfect identity authentication system and adopt more secure data transmission. The traditional password authentication is based on static password that can not meet the high security requirements of system. Traditional transport layer security protocol can not meet the security requirements of the mobile Internet because of its own characteristics. This paper based on the above two points, designs and implements a security scheme for hybrid application. The dynamic password authentication solves the problem of traditional password authentication and the data encryption using message-level security reduces the dependence of the data on the reliability of the intermediate nodes which make the system more secure.

As future works, we intend to improve the dynamic authentication algorithm to generate stronger password. We also like to make this security scheme smarter that select the appropriate encryption algorithm or appropriate symmetric key length based on the size of the transmission data.

References

[1] Paul Kearney. “Message level security for web services”

[2] Craig Isakson. “WEB, HYBRID, NATIVE”

[3] Liu Lei, Liu Qiang. “Research of Hybrid Web/Native Software Architecture”

[4] Tang Wei-dong, Zhou Yong-quan. “Message-level security model for web services and its security evaluation”

[5] Eric Rescorla. “SSL And TLS: Designing And Building Secure Systems”

[6] Daemen Joan, Rijmen, Vincent. “The design of Rijndael : AES - The Advanced Encryption Standard”

[7] Jiezhao Peng, Qi Wu, “Research and Implementation of RSA Algorithm in Java”

[8] Richard Ford, Michael Howard, Franco Callegati. “Man-in-the-Middle Attack to the HTTPS Protocol”

[9] Shuo Chen. “Pretty-Bad-Proxy: An Overlooked Adversary in Browsers' HTTPS Deployments”