Research Journal of Applied Sciences, Engineering and Technology 5(6): 1978-1985, 2013
DOI:10.19026/rjaset.5.4738
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: July 12, 2012 Accepted: August 15, 2012 Published: February 21, 2013

Research Article

Secure Access to Private Services in Intranet for Mobile Clients

Li Kuang, Yingjie Xia, Caijun Sun, Jiaming Wu and Liangdi Bao
Hangzhou Institute of Services Engineering, Hangzhou Normal University,
No. 222 Wenyi Road, Hangzhou, 310012, China

Abstract: With wide adoption of Service Computing and Mobile Computing, people tend to invoke services with mobile devices, requiring accurate and real-time feedback from services at any time and any place. Among these services, some are private to limited users and require identity authorization before use; hence secure access control in wireless network should be provided. To address the challenge, in this study, we propose the architecture and protocols of a system of access to private services for mobile clients, which combines the technologies of trusted computing, Diffie-Hellman key agreement protocol, digital certificate, DES data encryption algorithm and twice verification. We further show the implementation of the proposed system, in which we have realized the authentication and authorization of mobile clients and then secure data transfer between mobile clients in the unsafe Internet and private services in the Intranet.

Keywords: Access control, mobile computing, service computing, trusted computing, wireless networking

INTRODUCTION

In recent years, Service Oriented Computing (Papazoglou and Georgakopoulos, 2003) has emerged as a highly promising paradigm for distributed computing and software engineering, changing the way that software applications are designed, delivered and consumed. More and more companies and organizations encapsulate their software as services. This way alleviates users the burden of traditional software maintenance, while providing users a more simple, flexible and personalized way to accessing software. On the other hand, with the popularity of mobile computing (Forman and Zahorjan, 1994; Imielinski and Korth, 1996), the smart-phones and tablet devices become more and more intelligent and have advantages in high portability, so people tend to invoke services with mobile devices, requiring accurate and real-time feedback from services at any time and any place nowadays.

Among these services and applications, some are private to limited users and require identity authorization before use. For example, the service for policemen inquiring data of criminals when they are on duty outside, the service for traffic policemen inquiring illegal driving records of vehicles and so on. To prevent private services from being accessed by unauthorized users, secure access control technology in wireless network should be provided. However, generally speaking, the wireless network is low-bandwidth and open, while mobile devices usually have limited display, processing, storage, power and communication resources, hence it is not possible to simply apply tradition PKI/PMI (Solo *et al*., 1999; Chadwick and Otenko, 2003) based secure infrastructure in wired network to wireless network. Therefore, we aim to investigate a secure and reliable access technology for wireless network, so that various mobile clients can access private resources of corresponding organizations in a secure and real-time way after authentication and authorization.

Presently, there are mainly 2, 2.5 and 3G network in wireless mobile communication, such as GSM (ETSI, 1997), GPRS, CDMA, WCDMA and TD-SCDMA (3GPP, 1999). Authentication and authorization have been realized in the public mobile network to an extent, but it is mainly for mobile network operators to distinguish users' identities so as to manage users and realize personalized charges (3GPP, 2004). Therefore, general authentication and authorization mechanisms for mobile communication network cannot be applied to secure access to services in private Intranet, since authentication for different organizations needs to be customized.

As the development and mature of WPKI (Wireless Public Key Infrastructure), a suite of standards for certificates and keys management have been formed (WAP, 2000, 2001a, 2001b). The security mechanism of PKI (Public Key Infrastructure) has been introduced into WPKI, but has been extended and optimized according to the characteristics of wireless network. The aim of WPKI is to realize authentication and

Corresponding Author: Li Kuang, Hangzhou Institute of Services Engineering, Hangzhou Normal University, No. 222 Wenyi Road, Hangzhou, 310012, China, Tel.:86-571-28866717

authorization of mobile users and data encryption transmission in wireless network, so that a secure, stable and reliable wireless network can be established. Main adaptive changes in WPKI include: using WTLS (Badra *et al*., 2004) instead of TLS, using WTLS certificates which is simpler than X509 certificates used in PKI, using ECC (Elliptic Curve Cryptography) instead of RSA, the most widely adopted public key encryption algorithm in PKI, for authentication.

Although WPKI is designed especially for wireless network and mobile devices, in which many components have been designed under the considerations that the computation and memory of mobile devices are weak as well as that the bandwidth and reliability of wireless network is low, there are still some potential safety hazards in existing protocol:

- Although the memory occupation of WTLS certificates is less than that of X509 certificates, since it is stored in the mobile devices, the memory of which would be tense further and the certificates may be copied and embezzle by others.
- A TTP (Trusted Third Party) service has been employed in WTLS protocol, but the service itself is lack of trusted measurement and supervision. Once the TTP service is attacked to be unreliable, the whole system may be unsafe.

Therefore, in this study, we aim to propose a system supporting secure access to services in private Intranet for mobile clients based on trust computing. We employ trust computing (Berger, 2008; Choi *et al*., 2008; Yan *et al*., 2006; Zheng *et al*., 2005) technologies, such as trusted border gateway, construction and verification of trusted software, to improve the algorithms and architecture of WPKI, so as to realize that mobile clients with limited memory and processing ability can be verified via wireless network and then access services in private internet in safety.

METHODOLOGY

We propose a system that can support secure access to private services in Intranet for mobile clients. The architecture is shown as Fig. 1.

The Board access component (*B*) is located in the intranet while the wireless trusted Gateway (*G*) is located in the Internet. *B* together with *G* isolates the internet and the intranet of some organization. A secure channel between *B* and *G* is guaranteed and monitored by Monitor server (*M*). *B* and *G* are in charge of message forward from the internet to intranet and the reverse.

Certificate Server (*CS*), application Server (*S*) and Monitor server (*M*) are located in the Intranet. *CS* is in charge of issuing certificates to mobile clients and validating the clients who possess certificates. *S* provides various private services that can only be accessed by privileged users. *M* monitors *B* and *G* to ensure that they are not invaded. Mobile clients are usually located in the Internet and connected to *G* through wireless route and firewall via the wireless network. Once the certificate of the mobile client is validated by *CS* through *G*, secure communication links can then be established between the client and various private services, hence the mobile client located in the Internet can operate various private resources by invoking private services safely.

Implementation: We implemented a system of secure access to Intranet private services for mobile clients under wireless network. The system is composed of two components: certificates based authentication and

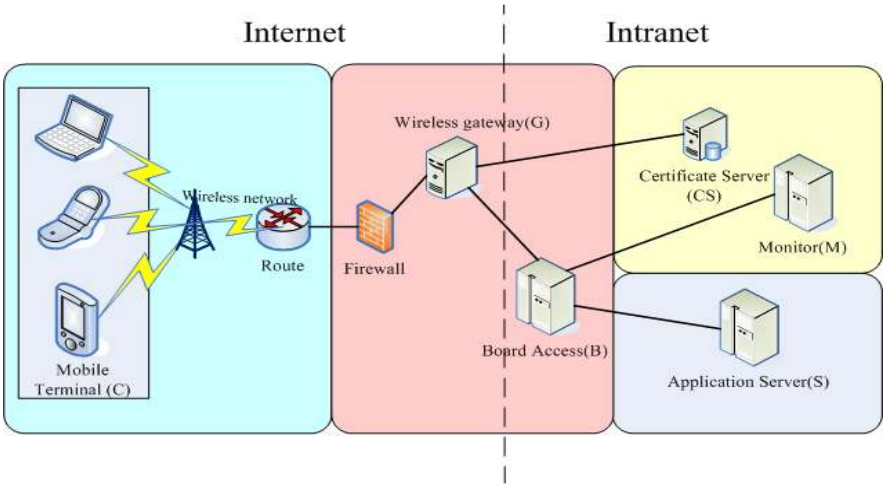

Fig. 1: The architecture of the system of secure access to private services for mobile clients

Fig. 2: GUI of requesting a certificate

authorization, as well as access to private services based on the established private link. We will illustrate the implementation of the two components in the following.

Authentication and authorization based on certificates:

Registration for privileged users: Registration for privileged users is accomplished in the Intranet. The related information for users who have registered successfully will be recorded in the certificate server *CS* which is located in the Intranet and the users will get their own certificate and place it in their own mobile device, so that users can use the mobile device with the certificate for authentication.

As Fig. 2 shows, users are required by *CS* their personal profile, including province, city, organization, department, name, Email and password, wherein Email will be served as a primary key. All of the submitted information except password will be used in the generation of identification certificate, while the password is used to encrypt the certificate, in case that the certificate is embezzled by others, if they cannot input the correct password, the certificate cannot be used as an identification of mobile clients.

After *CS* has received the registration request of users, it will first generate a RSA key pair including a public key and a private key and then generate its signature by encrypting the user's personal information which is pre-processed by Hash function with the RSA private key of *CS* and finally generate the identification certificate of the user which is composed of three parts: user's personal information, user's RSA public key and the signature of *CS*. A sample generated certificate is shown as Fig. 3.

In order to make the subsequent authentication safe, *CS* will generate a DES key for the client by Diffie-Hellman key agreement protocol after the generation of client's certificate. The detailed process is as follows: *CS* generates its DH key pair (including public key *CS_pub* and private key *CS_pri*) for the current client *C* and correspondingly in the client terminal, *C* generates its DH key pair (including public key *C_pub* and private key *C_pri*) for *CS* and then *CS* generates the DES key according to both *CS_pri* and *C_pub* and stores it.

And next *CS* sends user's certificate, user's RSA private key and *CS*'s DH private key *CS_pri* to the user and notifies the user of the successful registration. The user then generates his DES key according to *CS*'s DH public key *CS_pub* and his own DH private key *C_pri*.

Login of privileged users: Users can login into the system in the public network environment and their login requests will be forwarded by trusted wireless gateway. As Fig. 4 shows, users are requested to input their account and password, wherein the account is read automatically after the certificate is verified successfully in the mobile terminal and cannot be modified by the user and the password is used to decrypt the user's certificate which was encrypted and stored at the mobile terminal, so that the original certificate can be obtained for its local validation.

The login of privileged users through mobile devices consists of two steps: local validation of user's certificate and the mobile device's login on *CS* in the intranet.

The certificate stored in the mobile terminal needs to be validated before the mobile device logins on *CS*. The detailed validation process is as follows:

Fig. 3: A sample generated certificate

Fig. 4: GUI of user login

- The password is input in the mobile device and the user's certificate and RSA private key is decrypted and obtained.
- Generate digest 1 by hashing the personal profile in the certificate using SHA1 algorithm.
- Obtain digest 2 by decrypting the signature in the certificate using user's RSA private key.
- Compare digest 1 and 2, if they are the same, the certificate is valid, or else the certificate is invalid.

After successful local validation of user's certificate, the mobile device can then login to *CS*. The detailed process is as follows:

- Mobile device sends its login request to *CS* through wireless gateway.
- *CS* queries the user's DES key in the server's database according to the account, if the key is found, it notifies the user of successful login, or else failed login.
- If the DES key for the client is found in *CS*, *CS* generates the current timestamp and encrypts it with the DES key and then sends it to the client to request the 2nd login verification.
- The client decrypts the received message with its local DES key and sends the plaintext to *CS*.
- *CS* compares the plaintext sent by the client and the timestamp recorded in the server, if they are

the same, the client is treated as an authenticated user.

Traditional pattern of user login is once verification, i.e., the user provides his account and corresponding password and the server verifies the legality of the user identification by comparing the provided information with that stored in the server. Although the login pattern is simple and intuitive, the provided information may be intercepted maliciously during the transmission.

Twice verification may also suffer the risk of replay attack, i.e., if the message used for 2nd verification is fixed or repeatable, the third party can intercept the account information as well as the plaintext of legal users and resend it to *CS*, so there exists the possibility that the third party achieves replay attack by the intercepted message to login as a legal user. To deal with replay attack, timestamp is used as the message for the 2nd time verification of users in our proposed system, since the timestamp is unrepeatable, once *CS* receives a timestamp that has been used before, the request can be deemed as a replay attack and hence be rejected.

Access to private services based on the established private link:

Establishing a private link between the client and application server: When a client sends an invoking request to a private service located in the Intranet for the first time, a secure communication link must be established to ensure the safety of all the transmitted messages during the subsequent service invocation process. The private communication link can be reused when the client invokes the service again as long as the deadline is not reached. The detailed process of establishing a private link between a client and a service is as follows:

- When a client *C* requests to invoke a specific service from a list of privileged services, the selected service ID as well as the user's account and his RSA public key are sent to the wireless gateway *G*
- *G* forwards all the received messages to the application server *S*
- Once *S* gets the request from *C* forwarded by *G*, it generates a key pair (public key *Ss_pub* and private key *Ss_pri*) according to the public key of *C* i.e., *C_pub*, then generates the DES key between *C* and the selected service *Ss* according to *C_pub* and *Ss_pri* and stores the DES key for *C* and *Ss* in *S*. Finally *S* sends *Ss_pub* to *G*

Fig. 5: A sample of private services listed for the client after he has login with his certificate

- *G* forwards *Ss_pub* to *C*
- *C* generates the DES key between *C* and the selected service *Ss* according to *C_pri* and the received *Ss_pub* and stores it

So far, a secure communication link between the client *C* and the selected service *Ss* is established. A sample of private services listed for the client after he has login into the system with his certificate is shown as Fig. 5.

The client and the service exchange their public keys to each other after the service is selected by the client. A sample of *Ss_pub* held by the client and *C_pub* held by *S* is shown as Fig. 6.

Once the link between the client and the selected service is established, the client is forwarded to the interface of service invocation. Figure 7 shows a sample of a privileged service.

Access to private services: Once the communication link between the client and the service is established, the client can then access the private service safely.

When the client accesses the service, the request parameters will be encrypted with the DES key generated in the link establish step and sent to the wireless gateway *G*. *G* forwards the encrypted request to the responding service *S*. *S* decrypts the

```
From G:The uid is baofangdi@126.com
From G:The sid is 1
From G:The base64_cPubKey is
MIHfMIGXBgkqhkiG9w0BAwEwgYkCQQD8poLOjhLKuibvzPcRDIJtsHiwXt7LzR60ogjzrhYXrgHz
W5Gkfm32NBPF4S7QiZvNEyrNUNmRUb3EPuc3WS4XAkBnhHGyepzOTukaScUUfbGpqvJE8FpDTWSG
kxOtFCcbnjUDC3H9c9oXkGmzLik1Yw4clGI1TQ2iCmxBbIC+eUykAgIBgANDAAJAIozR6uJOCiyG
IAKYkY7clszwg6MbnINO6sUCgBQrWzvMTwK6tpMQBoyAX9+gl25Ixs6IICFSe7KABLXwa2udCw==

From G: The link path is http://localhost:8080/S/slink
From G: The response of link from CS is <?xml version="1.0" encoding="UTF-8"?
><response><code>0</code><title>From
S:success</title><s_dh_pub_key>MIHgMIGXBgkqhkiG9w0BAwEwgYkCQQD8poLOjhLKuibvzPcRDIJtsHiwXt7
LzR60ogjzrhYXrgHz%0D
%0AW5Gkfm32NBPF4S7QiZvNEyrNUNmRUb3EPuc3WS4XAkBnhHGyepzOTukaScUUfbGpqvJE8FpDTWSG%0D
%0Akx0tFCcbnjUDC3H9c9oXkGmzLik1Yw4clGI1TQ2iCmxBbIC%2BeUykAgIBgANEAAJBAOyjqgQ2guLq%0D
%0AtvblOt9soD2ihrvpGK%2BBTND4Hj93pzUd1SsrcrMOBqQYQ6LOfEG6jGk2FaSJcw%2Fo%2BeAUlrBR5OA%3D
%0D%0A</s_dh_pub_key></response>
The log.properties path is C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps
```

Fig. 6: A sample of *Ss pub* held by the client and *C_pub* held by *S*

Fig. 7: GUI of a sample private service

Fig. 8: Service request of inquiring illegal driving records of vehicles

```
Before dec the param is : uD+x/Oue3hO=
2012-04-07 16:06:16 [sun.caijun.SService]-[INFO] Before dec the param is : uD+x7Oue3hO=
After dec the param is : ac2589
2012-04-07 16:06:16 [sun.caijun.SService]-[INFO] After dec the param is : ac2589
After urlencoder, the param in service is ac2589
2012-04-07 16:06:16 [sun.caijun.SService]-[INFO] After urlencoder, the param in service is
ac2589
Before urldecoder, the param in service1 is     ac2589
2012-04-07 16:06:16 [sun.caijun.service.service1.Service1]-[INFO] Before urldecoder, the
param in service1 is    ac2589
After urldecoder, the param in service1 is ac2589
2012-04-07 16:06:16 [sun.caijun.service.service1.Service1]-[INFO] After urldecoder, the
param in service1 is ac2589
The param for the service1 is ac2589
```

Fig. 9: The encrypted and decrypted service request

Fig. 10: The result of service invocation

received request with its DES key and gets the result corresponding to the request. The result is then encrypted with the DES key and forwarded to the client through *G*. And finally the client decrypts the result with his DES key. Therefore, the client can communicate with the private service safely based on the established link.

Take the service for traffic policemen inquiring illegal driving records of vehicles as an example. The user inputs the license plate number to query, as Fig. 8 shows.

In the console of the system, the encrypted service request of the mobile terminal as well as the decrypted service request in the service server is shown as Fig. 9.

The private service answers the request from the client and the illegal driving records of the specific vehicle are transferred and listed in the mobile terminal, as Fig. 10 shows.

In the console of the system, the answer of the service as well as it encrypted transfer from *S* to *C* and decrypted display in *C* are shown as Fig. 11.

CONCLUSION

In this study, we propose a mechanism of secure access to services in private Intranet for mobile clients based on trust computing. A set of technologies such as Diffie-Hellman key agreement protocol, digital certificate, DES data encryption algorithm and twice verification, are applied in the proposed access protocol. Based on the proposed approach, a secure access system for mobile clients is implemented. It has realized the authentication and authorization of users, as well as secure data transfer between Internet and Intranet for mobile clients.

In the future, we aim to design possible attack scenarios to prove the robustness of the proposed system and apply more technologies of trusted computing in the architecture design.

ACKNOWLEDGMENT

The study is supported in part by the following funds: National Natural Science Foundation of China under grant number 61202095, Zhejiang Provincial Natural Science Foundation of China under grant number Y1110591 and Hangzhou Normal University under grant number 2010HSKQ0006.

<?xml version="1.0" encoding="gbk"?><cars><count>1</count><car><car_id>浙
AC2589</car_id><count>1</count><record><id>5</id><inf_time>2012-02-16
18:04:07.0</inf_time><inf_loc>宁波</inf_loc><inf_detail>闯红灯
</inf_detail></record></car></cars>
<?xml version="1.0" encoding="gbk"?><cars><count>1</count><car><car_id>浙
AC2589</car_id><count>1</count><record><id>5</id><inf_time>2012-02-16
18:04:07.0</inf_time><inf_loc>宁波</inf_loc><inf_detail>闯红灯
</inf_detail></record></car></cars>
<?xml version="1.0" encoding="UTF-8"?><response><code>0</code><title>From
S:success</title><enc_content>i1YOVHYgI8PGPhuYMtyFqU5ChRPbojsFvofkO2VkOhSUcUyg2BzZN6hgIEGF
EGZ6xszs33xukO5K
5xe82E59yB/1DUia8b98FFIRVIx6yxSOwxuLgGHuzYM82WGM1zda+7oiMMFKtIXXY1ewL433aSr3
OQQOFk5tvN5TvzjxzhP2N+xFD9JGEH+3kALuyKwRv5dwEcAARFuWnjVaXJ/0032o2BocyrYWPB81
5PzJGMwXhI8NXmqY2+dcDJUGFQDMraFgvI3mwyJx5ALb1h+zj2uDiZsnqjDNgaqI2HFcx2XOsyIy
7wuc2wwWLSf57/Mj+rsMkO3H3d4=
</enc_content></response>

Fig. 11: The encrypted and decrypted answer of the service

REFERENCES

3GPP, 1999. 31.102 V3.12.0 (2003-03) Technical Specification 3rd Generation Partnership Project. Technical Specification Group; Characteristics of the USIM Application.

3GPP, 2004. 3G TR 33.900 V1.2.0 (2000-01) Technical Specification 3rd Generation Partnership Project. Technical Specification Group SA WG3; A Guide to 3rd Generation Security (3G TR 33.900 version 1.2.0).

Badra, M., A. Serhrouchni and P. Urien, 2004. A lightweight identity authentication protocol for wireless networks. Comput. Commun., 27: 1738-1745.

Berger, B., 2008. Guide to Trusted Computing. Computer Technology Review.

Chadwick, D.W. and A. Otenko, 2003. The PERMIS X. 509 role based privilege management infrastructure. Future Gener. Comp. Sy., 19(2): 277-289.

Choi, S.G., J.H. Han, J.W. Lee, J.P. Kim and S.I. Jun, 2008. Implementation of a TCG-based trusted computing in mobile device. Lect. Note. Comput. Sci., 5185: 18-27.

ETSI, 1997. Digital Cellular Telecommunications System (Phase 21): Specification of the Subscriber Identity Module—Mobile Equipment (SIM-ME) interface. GSM 11.11 Version 6.2.0 Release 1997.

Forman, G.H. and J. Zahorjan, 1994. The challenges of mobile computing. J. Comput., 27(4): 38-47.

Imielinski, T. and H. Korth, 1996. Introduction to Mobile Computing. Kluwew Publishers, pp: 1-43.

Papazoglou, M.P. and D. Georgakopoulos, 2003. Introduction to a special issue on service-oriented computing. Commun. ACM, 46(10): 24-28.

Solo, D., R. Housley and W. Ford, 1999. Internet X. 509 Public Key Infrastructure Certificate and CRL Profile. Retrieved from: http:// www.hjp. at/doc/ rfc/rfc2560.html.

WAP, F., 2000. Wireless Transport Layer Security Specification. Retrieved from: http:// www1. wapforum. org/ tech/documents/WAP- 199-WTLS-20000218-a.pdf.

WAP, F., 2001a. WAP Public Key Infrastructure Definition. Retrieved from: http:// www1. wapforum. org/tech/documents/WAP-217-WPKI-20010424-a.pdf.

WAP, F., 2001b. WAP Certificate and CRL Profiles. Retrieved from: http:// www1. wapforum. org/ tech/ documents/ WAP-211-WAPCert-20010522-a.pdf.

Yan, F., H. Zhang and Z. Shen, 2006. an improved wireless grid security infrastructure based on trusted computing technology. International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM, 2006.

Zheng, Y., D. He and W. Yu, 2005. Trusted computing-based security architecture for 4G mobile networks. 6th International Conference on Parallel and Distributed Computing, Applications and Technologies, Washington, DC, pp: 251-255.