Delegated Certificate Validation Model Applicable to the Wireless PKI

JIN KWAK*, SEUNG-WOO LEE*, KYUNG-JIN KIM*, SOO-HYUN OH*, DONG-HO WON*
*Information & Communications Security Laboratory
School of Electrical & Computer Engineering
Sungkyunkwan University
300 Chunchun-dong, Jangan-gu, Suwon, Kyunggi-do
KOREA
{jkwak,swlee,kjkim,shoh,dhwon}@dosan.skku.ac.kr

Abstract: With the rapid growth of the wireless Internet service, the interest in security technology over the wireless Internet has been increased. Wireless Internet security technology provides users with confidentiality, authentication and non-repudiation based on WPKI(Wireless Public Key Infrastructure). To provide these services, the method that enables the wireless Internet using users to validate the other party's certificate efficiently must be provided. But, there is no standard about the certificate validation using the mobile device over the wireless Internet environment. Therefore, we propose the certificate validation model applicable to the wireless Internet environment based on the previous certificate validation model based on the wired Internet environment.

Key-Words : PKI, WPKI, mobile device, delegated certificate validation

1 Introduction

With the activation of wireless Internet service, more users are using the mobile device, and the research on the e-commerce(electronic commerce) using it such as Internet banking service, online-transaction and online shopping is also in rapid progress. To provide the security service such as confidentiality, data integrity and non-repudiation in wireless Internet environment, it is possible one party should validate other party's certificate efficiently through his/her mobile device.

WPKI is not completely standardized like PKI (Public Key Infrastructure), and there are some problem to validate the certificate as PKI environment because of the properties of wireless Internet and the limitation of the mobile device. To provide secure wireless Internet services, research on the certificate validation model considering mobile device's limited processing capability and storage is needed[1].

CRL-based model and OCSP model is the typical certificate validation model. But those two models are not suitable for WPKI environment because of the mobile device's processing capability and the storage. In this paper we propose the WPKI applicable certificate validation model considering the properties of wireless Internet[2][3].

This paper is consisted as follows. In section 2, we explain the related work such as wireless Internet, WPKI and existing certificate validation methods. in section 3, we analyze the different environment of wireless. In section 4, we explain the Delegaed Certificate Validation Model(we called DCV Model) applicable to the Wireless Internet environment on the mobile device. Finally, in section 5, we bring to the conclusion of this paper.

2 Related Work

In this section, we examine the wireless Internet, application protocol, wireless PKI, and existing certifcate validation methods.

2.1 Wireless Internet

Wireless Internet is the process of communicating information in mobile device over a distance through the free-space environment, rather than through traditional wired Internet.

Generally, mobile devices such as mobile phones, PDAs(Personal Digital Assistants), and pagers are less secure than the devices used in wired Internet. This is due to their limited bandwidth, memory, and capabilities of processing or calculation. Also, they send their data into the air where anyone can steal it[1].

2.2 WAP

The WAP(Wireless Application Protocol) is a global specification that empowers mobile users with mobile devices to easily access and interact with information and service instantly. The purpose of WAP is to enable easy and fast delivery of relevant information and services to mobile users. To the definition of WAP, WAP Forum was founded internationally.

The WAP Forum is the industry association comprised of hundreds of members that have developed the world standard for wireless information and mobile service on mobile device[4].

2.3 WPKI

WPKI is the extension of the existing PKI to be applicable in wireless Internet environment. WPKI is also based on the certificate and provides confidentiality, non-repudiation and user authentication of transmitted information over the wireless Internet environment. It is proposed for activating the e-commerce on the wireless Internet environment. IETF enacts PKI as a standard, but there are no WPKI standard and WAP Forum's model is widely used. The organization of WPKI is same as existing PKI;CA (Certification Authority), RA(Registration Authority), Directory, Validation server and the User. The WPKI user should validate the certificate by mobile device[1][4].

2.4 SSL/TLS & WTLS

The TCP/IP(Transmission Control Protocol/Internet Protocol) governs the transport and routing of data over the Internet. Other protocols, such as the HTTP(HyperText Transfer Protocol), or LDAP (Light-weight Directory Access Protocol), run "on top of" TCP/IP in the sense that they all use TCP/IP to support typical application tasks such as displaying wired Internet.

The SSL(Secure Sockets Layer) protocol runs above TCP/IP and below higher-level protocols such as HTTP or IMAP(Internet Message Access Protocol). It uses TCP/IP on behalf of the higher-level protocols, and in the process allows an SSL-enabled server to authenticate itself to an SSL-enabled client, allows the client to authenticate itself to the server, and allows both machines to establish an encrypted connection. The new IETF standard called TLS(Transport Layer Security) is based on SSL. This was recently published as an IETF Internet-Draft. The primary goal of the TLS Protocol is to provide privacy and data integrity between two communicating applications[5][6].

WTLS(Wireless Transport Layer Security) is the WAP Forum's specification for wireless security services that provide privacy, data integrity, and user authentication. WTLS provides similar functionality to TLS, but it is adapted to the wireless Internet[7].

2.5 Certificate Validation Methods

In this subsection, we examine the existing certificate validation methods such as CRL-based, OCSP, and SCVP.

2.5.1 CRL-based

CRL(Certificate Revocation List) is the most widely used method to validate the certificate's status. The CA(Certification Authority) signs the certificate including the serial number and reason of expiration and make it public. Then the client downloads the CRL and searchs for the specific certificate status information.

CRL contains a serial number and reason of all revoked certificates. It is the general method to show the revoked reason.

But it can't give the current cetificate status inforamtion because it is issued periodically and it has a communication overload because of downloading whole CRL[8][9][10].

2.5.2 OCSP

OCSP(Online Certificate Status Protocol) is proposed to provide the current certificate status information. It is composed of client and server, and standardized as an IETF RFC2560. This is a protocol that provides certificate status information to a client without using CRL and it is used online between the server and the client. If a client connects to a server and requests a certificate stauts information that s/he needs, the server searches that information and digitally signs it. Then the server sends it to the client. The client can obtain the certificate status information using the OCSP[11].

The motivation for OCSP is to overcome limitations in CRL-based revocation methods, and provide real-time response to certificate status information. OCSP v2(Internet-Draft) includes DPV(Delegated Path Validation), DPD(Delegated Path Discovery), and ORS(Online Revocation Status) services. DPV and DPD are that the client delegate facility of certificate's path validation and discovery to server, so it makes to reduce cost for client[12].

2.5.3 SCVP

SCVP(Simple Certificate Validation Protocol) is to reduce the overload of certificate path validation from the client. SCVP uses a simple request and response protocol, designed run over HTTP. The SCVP client sends a specific certificate in the inquiry to be validated. The server performs the validation processing and digitally signs it. Then the server sends it to the client.

SCVP has not yet been approved as an IETF RFC document, SCVP is an IETF Internet Draft state[13].

3 Different Environments of Wireless

In this section, we analyze the different environment of wireless and the optimization in WPKI.

3.1 Wireless Environments

The properties of mobile device in wireless Internet environment are different from those of wired Internet environment because of its storage limitation and processing capability. So we have to consider the following things and the mobile device needs gateway to connect with web-based protocol.

Limited Processing Capabilities : We have to consider the CPU and memory of mobile device in wireless Internet environment. Mobile device has limited processing capability because the capacity of CPU and memory is relatively small.

Limited Storage for Data and Programs : Because the storage for datas and programs of mobile device itself is limited, we have to consider the size of certificate and security module that can be stored in the mobile device. Because the size of mobile device is miniaturized, the research on this should be made rapid progress.

Low Bandwidth : wireless bandwidth is constrained, HTTP is not feasible in WAP applications. Therefore, mobile device communicate via a gateway.

Small Device : Mobile device for wireless Internet is smaller than the computer system(generally Desktop PC) for wired Internet environment. Mobile device must contain the function that can use the wireless Internet.

Gateway : it is generally used to translate wireless protocols into wired Internet protocols. It turns user's requests into standard Web-based request using protocols defined in the WAP specifications.

3.2 Optimization WPKI

Protocols : BER(Basic Encoding Rules) and DER (Distinguished Encoding Rules) is used in PKI, but WML is used in WPKI for the service.

Certificate : WTLS certificate format smaller than X.509 certificate or certificate stored URL is used considering the storage of mobile device.

Cryptographic Algorithm and Keys : Cryptographic algorithm and key providing the digital signature efficiently, like ECC(Elliptic Curve Cryptography), are required considering mobile device's limited processing capability.

4 Proposed DCV Model Applicable to a wireless PKI

In this section, we explain the proposed Delegated Certificate Validation Model in this paper.

4.1 Motivation

With the rapid growth of the wireless Internet service, the number of Internet service users using mobile device is also increasing. And research on the e-commerce with mobile device is in rapid progress. Wireless Internet service enables user to use various services anytime, anywhere. Mobile device has some problems to provide security services same as wired Internet environment because of its limited capabilities CPU and memory.

The research for providing security service is in progress, but there is no standardization. WPKI is also based on the certificate like PKI. So user can validate the certificate with his/her mobile device.

Because the certificate validation needs much storage and throughput, there are some problem to apply the PKI's certificate validation process directly into the wireless Internet environment with the mobile device.

Therefore, we propose the Certificate Validation Model applicable to the WPKI environment based on the properties of mobile device.

4.2 Design of DCV Model

Certificate validation process with the mobile device should be simplified than the previous certificate validation process. Therefore, computational cost of the user should be cut down to validate the certificate with mobile device.

The proposed DCV Model is made up CA, directory, gateway, DCV Sever, and user(mobile device-enable for WAP).

Fig.1 shows the operations of DCV Model.

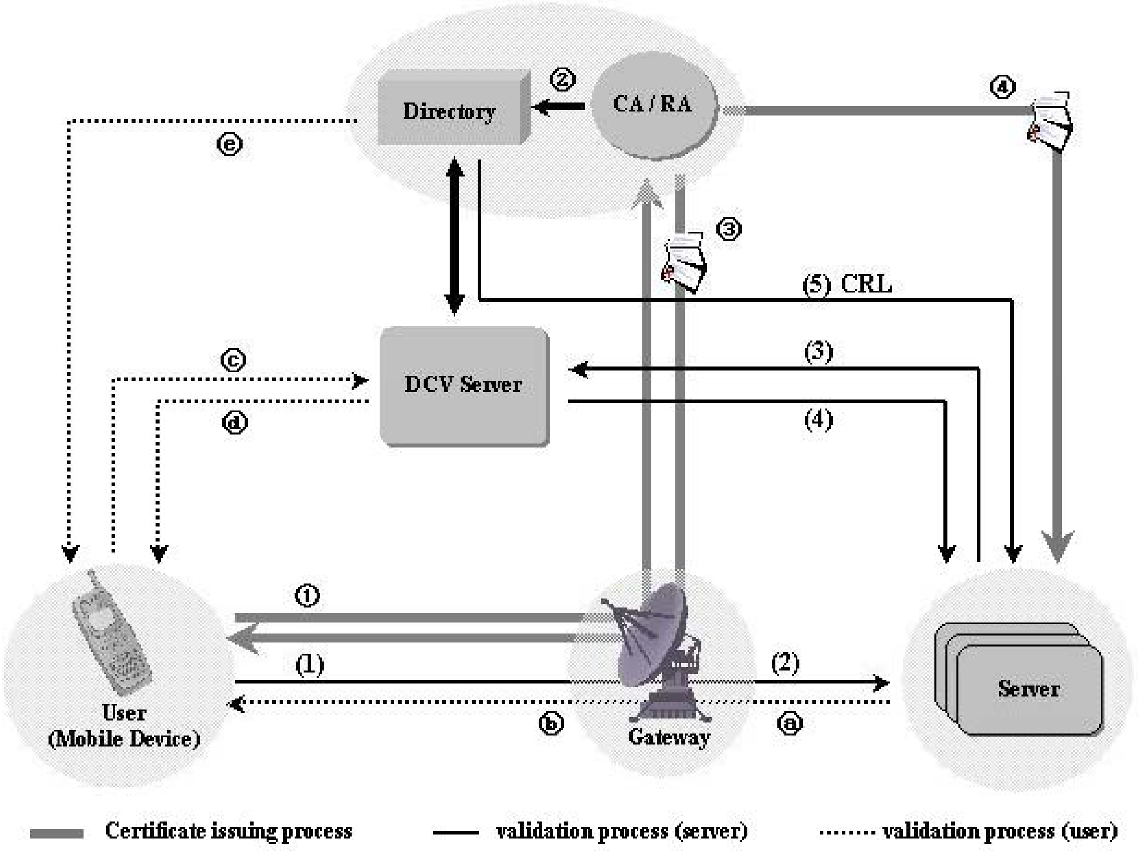

Fig.1 Architecture and Operations of DCV Model

4.2.1 Issuing the Certificate

The process of issuing the certificate through the mobile device is as following. User requests CA to issue the certificate through the gateway, then CA also issues the certificate through the gateway(①~④ in Fig.1). At this time, if CA functions as RA, user should register to CA first. Then user gets the ID and Password used in mobile device from RA. (In case of CA and RA is separated, RA could be financial agency or the security corporation.) User request CA to issue the certificate using his/her ID and Password, then CA checks the ID and Password and stores the information of user and certificate. If needed, certificate also. User receives certificated stored URL instead of the certificate considered his/her storage of mobile device. The certificate is also issued to the server (e.q.Web application, etc) that the user wants to use.

4.2.2 Validation of User Certificate by the Server

The server acquires the URL where the certificate of the mobile device user is stored, and validates the user certificate acquired from the directory designated by the URL. The server(web application) validation process uses the PKI certificate validation ((1)~(5) in Fig.1). First, validation of the certificate is requested to the DCV Sever, and the DCV Sever performs validation and replies with the results. The certificate validation used at this time is based on RFC 2560 OCSP. The DCV Sever that receives the request for validation of certificates uses a protocol predefined with the server, to distinguish the request from validation requests by mobile devices. Then, it sends the validation results to the server. If the DCV Sever fails to operate due to errors, it should be able to validate certificates by downloading CRL from the CA's directory. The methods require for efficient validation of certificates in wired environments[15]

4.3 Certificate Validation using the Mobile Device

In order to validate certificates using mobile devices, considerations need to be made for restrictions of the mobile device, such as calculation capabilities, data storage, and low bandwidth.

In this paper, we proposed the DCV Model for efficient validation of certificates using mobile devices. In the DCV Model, the mobile device user delegates the DCV Sever to validate certificates. The validation process is executed through the request messages, which are used by the mobile device user to request certificate validation to the DCV Sever, and the response messages, which response with the results of the certificate validation by the DCV Sever (ⓐ~ⓔ in Fig.1)

First, the server sends certificate (X.509 certificate) to the gateway, and the gateway relays the certificate (WTLS certificate) of the server to the mobile device. Upon receipt of the certificate of the server, the user delegates the DCV Sever to validate certificates. In turn, the DCV Sever executes the validation process, and sends the results to the mobile device user. The validation of user certificates is delegated by DCV requests, and the certificate validation results are sent to the user through DCV Sever's response. If certificate validation cannot be performed due to temporary error of the DCV Sever, the user manually downloads the CRL from the directory of CA, and validates the certificate. However, this may have problems caused by limited performance of mobile devices.

4.3.1 DCV Request

In this sub-subsection, we proposes the request messages that delegate the DCV Sever to validate certificates by the mobile devices.

First, the user of the mobile device connects to the DCV Sever using the ID and password issued by the CA, and sends the DCV Request message.

The ASN.1 definition of the CITP and the meaning of each fields of the protocol are described as follows[14].

```
DCVRequest  :: =  SEQUENCE {
   tbsRequest            TBS Request
   UserCertURL        User's Cert URL  }

tbsRequest  :: =  SEQUENCE {
   version           Integer DEFAULT 0
   requestCert      Request Cert
         certIssuer        Request Cert Issuer Serial
         certSerial        Request Cert Serial Number
         certURL          Request Cert URL
   requestTime     Generalized Time  }
```

DCVRequest field is composed of *tbsRequest* and *UserCertURL* for the mobile device user's certificate expresses the location to be saved.

tbsRequest field is the information of specifies the certificate in the request. This field contained as follows.

version is specifies the version of the message, initial value is DEFAULT 0.

requestCert is composed of *certIssuer*(-indicates the proper number of issuer), *certSerial*(-contains the serial number of requested certificate), and *certURL* (-indicates the requested certificate expresses the location to be saved).

requestTime field is the time at which the mobile device user transmits the request message.

4.3.2 DCV Response

In this sub-subsection, we proposes the response messages that delegate the DCV Sever to validate certificates, and replies the validation results to the user.

The ASN.1 definition of the DCV Respone message is given in bellow, and the meaning of each field of the message is decribed as follows[14].

```
DCVResponse  :: =  SEQUENCE  {
   version                  Integer DEFAULT 0
   validationResult    Cert Validation Result
   validationTime      Generalized Time
   location                 CRL location OPTIONAL
   responseExtensions    Extensions OPTIONAL
   signature              OPTIONAL Signature  }

validationResult  :: =  ENUMERATED  {
        valid                     (0)
        internalError          (1)
        finished                (2)
        revoked                 (3)
        tryLater                (4)   }
```

version is specifies the version of the message, initial value is DEFAULT 0.
validationTime is the time of the certificate validation, it's indicates generalized time.
location gives supportability to refer to CRL.
responseExtensions indicates that beforehand mutual agreement between DCV Sever and mobile device user.
signature is signature of DCV Sever and OPTIONL.
validationResult field is the result of specifies the certificate for the client's request. This field contained as follows.
valid indicates the validity of certificate. *internalError* indicates the DCV Sever reached inconsistent internal state. *finished* indicates that the certificate is not valid any more. *revoked* indicates that the certificate is revoked before the term of validity because of the revoked reason. *tryLater* indicates that the DCV Sever is running but returns a status for the requested certificate. So it is used to indicate that the service exists, but it is temporarily unable to respond.

5 Conclusions

In this paper, we proposed the Delegated Certificate Validation Model for validating certificates using mobile devices. The validation of certificates under wireless environments is different from that under wired environments, as considerations need to be made for limited performance of the mobile devices.

Since services such as data confidentiality, user authentication, and non-repudiation under wireless environments are performed based on certificates, so the efficient validation of certificates using mobile devices are required. However, research on the process of validating certificates using mobile devices have been limited up to now. Therefore, this paper proposed a model for validating certificates efficiently using mobile devices under wireless Internet environments, also it is based on existing certificate validation methods. The Delegated Certificate Validation model proposed in this paper, delegates the certificate validation process to the DCV Sever, in consideration with the performance of the mobile device, and the DCV Sever that receives the delegation validates the certificate, and provides the results to the user through DCV Response messages. By interworking with wired Internet environments, the DCV Model has been designed for mobile device users to use efficiently and conveniently. It is expected that the DCV Model proposed in this paper should be used efficiently in electronic commerce areas such as Internet banking, stock trading, and on-line shopping using mobile devices.

References:

[1] R. K. Nichols and P. C. Lekkas, *Wireless Security*, McGraw-Hill, 2002

[2] ISO/IEC 9549-8, *Information technology Open System Interconnection The Directory : Authentication Frame Work*, X.509, 1997

[3] R.Housley, W.Ford, W.Polk, and D.Solo, *Internet X.509 Public key Infrastructure Certificate and CRL Profile*, RFC 2459, 1999

[4] *www.wapforum.org*

[5] A. Freier, P. Kalton and P. Kocher, *The SSL Protocol version 3.0*, Internet Draft, 1996

[6] S. Thomas, *SSL and TLS essentials : securing the Web*, Jhon Wiley & Sons, Inc., 2000

[7] WAP Forum Proposed Version 3-Mar-2000. *WAP -217-WPKI : Wireless Application Protocol*, 2000

[8] M.Naor and K,Nissim, Certificate Revocation and Certificate Update, *In Proceeding of the 7th USENIX Security Symposium*, 1998, pp. 217-228.

[9] J.Author, Certificate Revocation Paradigms, *Technical Report, Cybernetica Estonia*, 1999

[10] D.A.Cooper, A Model of Certificate Revocation, *Proceeding of the 15th Annual Computer Security Applications Conference*, 1999

[11] M.Myers, R.Ankney, A.Malpni, S.Galperin, and C.Adams, *Internet X.509 Public Key Infrastructure On-line Certificate Status Protocol-OCSP*, RFC 2560, 1999

[12] D. Pinkas, *Delegated Path Validation and Delegated Path Discovery*, draft-ietf-pkix-dpv-dpd-00.txt, 2001

[13] A. Malpani, R. Hously and T. Freeman, *Simple Certificate Validation Protocol:SCVP*, draft-ietf- pkix-scvp-08.txt, 2002

[14] ISO/IEC 88240-1, *Information technology-Abstract Syntax Notation One (ASN.1) : Specification of Basic Notation*, 1997

[15] J.Kwak, K.J.Kim, S.H.Oh, H.K.Yang and D.H.Won, *Real-time Certificate Validation Model With CSIProvider*, WSEAS Transactions on communications, Volume1, Issue-1, 2002, pp. 203-210