X.509 Certificate Revisited

Tohari Ahmad
Informatics Department,
Faculty of Information Technology - FTIF,
ITS Surabaya
Email: tohari@its-sby.edu

Abstract

A digital certificate is used for identifying resources' identity over networks such as the internet which is formally standardized in X.509. In general, X.509 consists of certificate issuance, renewal and revocation. Those three processes are elements which must be secure, real-time update and easy to access. However, they may also suffer from attacks which lead to losing the resources' authenticity and integrity. This paper does not provide a new scheme for X.509 security but it discusses the security's structure, potential attacks and its countermeasures.

Keywords: security, public key infrastructure, authenticity and integrity

1 INTRODUCTION

Information security properties such as: authenticity and integrity have become very important in the internet communication. This is because the internet is an open environment which anyone can connect to our systems and we can also connect to any other systems. In this case, we need to make sure who we are communicating with because it is possible that any unauthorized party pretends to be another in order to get our secret information. Authentication can be a problem if it is not managed well.

Digital certificates or public key certificates, as one of authentication protocols, can be used to do such authentication. It has been widely used to authenticate the identity of machines or users in many environments such as banking and government website. However, different environments may use different certificate's formats. It can cause difficulties for performing authentication and also developing the certificate itself.

To overcome this problem, International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) and ISO/International Electro technical Commission Directory introduced a certificate format standard, known as X.509. Since its first development, X.509 has experienced some modifications to improve its capability. The term X.509 certificate refers to RFC 3280 which contains Internet Engineering Task Force Public Key Infrastructure (IETF PKI) Certificate and Certificate Revocation List (CRL) Profile. Yet, in facts, RFC 3280 itself has been updated by RFC 4325.

2 CONCEPT OF CA

A digital certificate is developed based on *trust.* It means that the clients will trust such certificate if it is issued by trusted issuers, namely trusted certificate authorities (CA). A CA provides three services: certificate issuance, certificate renewal and certificate revocation. As the number of CA increases, it needs to develop the relationship between them in a hierarchy.

2.1 Structure of CA

A CA may be in the CA chain which its highest level is the Internet PCA registration Authority (IPRA). IPRA is responsible for certifying and issuing certificates to policy certification authorities (PCA). In turn, PCA is certifying and issuing certificates to CAs.

There are some structures of CAs that are used at the present: hierarchy, mesh, bridge and hybrid models. The hierarchy model is more implemental than others. It needs the subscribers (clients) to trust the top level CA (root) before they trust other subscribers. Yet, it is not practical. By using 'additional' cross certification, this problem is mitigated. According to [1], a cross certification will propagate trust between CAs and shorter the CA hierarchy as in figure 1.

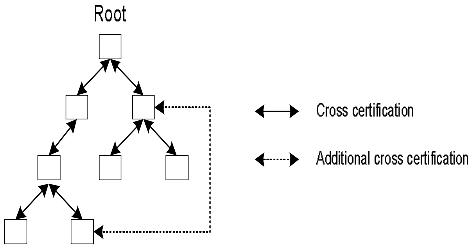


Figure 1. Cross Certification Hierarchy

However, [2] believe that those structures are not applicable to a global environment because many countries implement different versions of PKI and technologies. As a solution, they propose a new CA structure as in figure 2. In this model, a cross certification is not needed because those in the ring behave like a single root but in different parts.

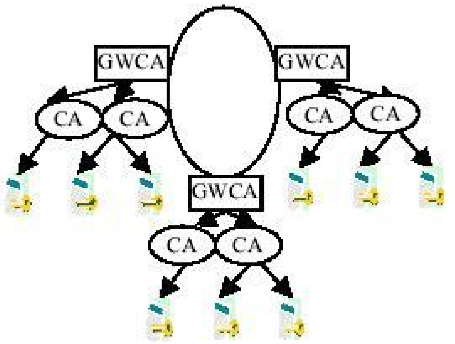


Figure 2. Gateway CA model [2]

Yet, this model still has limitation in authenticate CAs in different GWCA (Gate Way Certificate Authority). A subscriber of a CA has to verify the GWCA (root CA) in order to trust subscribers of other CA in other GWCA.

2.2 Certification Services

The certification is intended for organizations to get the trust from others. So, the certification is not only about authenticity but also confidentiality, integrity, authority and non-repudiation.

CAs have responsibility to manage certificate-related services in order to maintain subscribers' trust. Certificate issuing is an important process in maintaining such trust. This is because false certificate issuing has a big impact on the system security. Moreover, when issuing certificates, a CA should also be considering laws and policies.

3 X.509 DIGITAL CERTIFICATES

3.1 Digital Certificate and Trust

Trusting the CA means that the users will also trust the certificates issued by the CA. So, a CA will keep such certificates to be as secure as possible. This is done by giving digital signature to the certificate after verifying its subject.

An attacker will not be able to forge the certificate because they do not know the CA private key that is used to sign the certificate. Therefore, the CA private key is very important in X.509 environment.

3.2 Authentication Process

Certificates can be owned by clients, servers or both. In an *e*-commerce application, it is common that only servers need the certificate. However, in a system with high security, both should have the certificate. The authentication process of such system begins when the client sends its certificate to the server and vice versa as in figure 3 [3]. After the authentication process has finished, the client and server have the session key which is used for the entire communication.

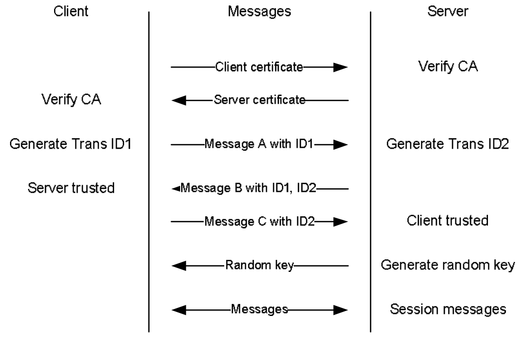
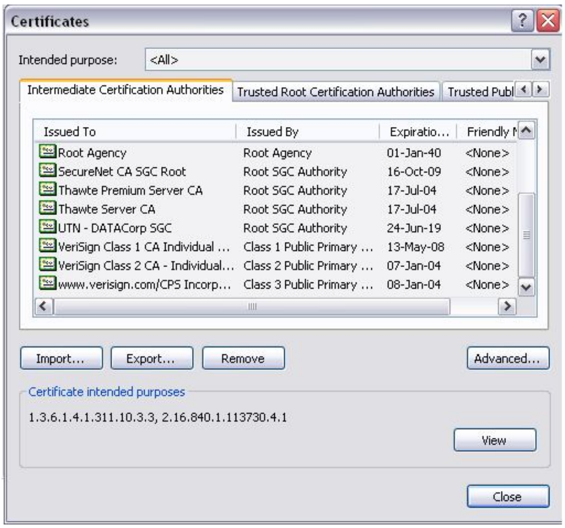


Figure 3. X.509 Authentication Process

3.3 Digital certificate in browsers

A browser recognizes major CAs that have been installed in it. In case a browser does not know the CA-signed certificate, it will give a security alert to the users. In the Microsoft Internet Explorer, for example, some major CAs have already been installed automatically as in figure 4.


Certificates
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Import...
Export...
Remove
Advanced...
View
Close

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly N
Root Agency	Root Agency	01-Jan-40	<None>
SecureNet CA SGC Root	Root SGC Authority	16-Oct-09	<None>
Thawte Premium Server CA	Root SGC Authority	17-Jul-04	<None>
Thawte Server CA	Root SGC Authority	17-Jul-04	<None>
UTN - DATACorp SGC	Root SGC Authority	24-Jun-19	<None>
VeriSign Class 1 CA Individual ...	Class 1 Public Primary ...	13-May-08	<None>
VeriSign Class 2 CA - Individual...	Class 2 Public Primary ...	07-Jan-04	<None>
www.verisign.com/CPS Incorp...	Class 3 Public Primary ...	08-Jan-04	<None>

Certificate intended purposes

1.3.6.1.4.1.311.10.3.3, 2.16.840.1.113730.4.1

Figure 4. List of CA in the Microsoft Internet Explorer

4 X.509 CERTIFICATE REVOCATION LIST (CRL)

A certificate is only valid in a certain period. There are some reasons why certificates have become invalid, such as: expiration and compromised by disclosures or attacks. The list of those invalid certificates needs to be distributed in order to avoid misuse of them.

X.509 CRLs has become a standard for publication and distribution of the identity of revoked, unexpired certificates [4]. Therefore, CRL should be issued periodically to inform them to the public.

4.1 CRL Propagation

Frequent updates of CRLs increase the awareness of detecting and rejecting revoked certificates. The frequency of CRLs may depend on how important the transaction is. For example, VeriSign generates CRLs daily or hourly for all enterprise customers. Yet, issuing CRL too often will increase the bandwith requirement, while issuing it rarely will increase the risk.

According to [5], there are some mechanisms to distribute CRLs such as:

- Polling for CRLs
  The subscribers (applications) have to know the schedule of CRL update when they should download the latest CRL from the CA. The period between the latest and the next download is very critical since there may be many transactions occurred in that time without assuring the certificates' status.
- Pushing CRLs
  CAs distributes CRL to subscribers (applications) once they revoke a certificate. The advantage is that the update is faster than polling mechanism. However, the problem is the bandiwth because this revocation should be informed to all subscribers which may be in a large number. Moreover, the revocation may intercepted and deleted by attackers before reaching subscribers.
- On-line Status Checking
  Using on-line status checking, subscribers (applications) may check only a specific certificate's status. This checking can be performed before the transaction begins, for example. So, there is no delay between the revocation status and the transaction.

Those mechanisms may be implemented in Delta CRLs and On-line Certificate Status Protocol (OCSP). Delta CRL contain only the latest revocation updates since previous CRL was issued. While in OCSP mechanism, the users can just check the status of specific certificates. According to [6], over-issuing delta CRL with distribution points method has the lowest bandwith usage.

However, even a CRL is an important property in the X.509 environment, it is rarely checked in practice because users just believe that checking only the authenticity of public key certificate have been sufficient [7]. Users may think that certificate revocation happens rarely.

A CRL is as important as the signed certificate itself. It should be checked before doing any transaction even in the small value one. This is because the transaction does not only relate to the value involved but also the non-repudiation principle and user's trust.

4.2 Profile

CRL profiles which is used to identify unique settings for CRLs consist of some fields as in figure 5 [8]. As for the certificate, a CRL is signed by a CA for the authenticity. All those CRL fields are specified in respective RFC. For example, a CRL extension field, which provides a means of retrieving CRL issuer certificates, is specified in RFC3280 which is updated by RFC4325 [9]. Both RFCs determine that this field must not be marked as critical.

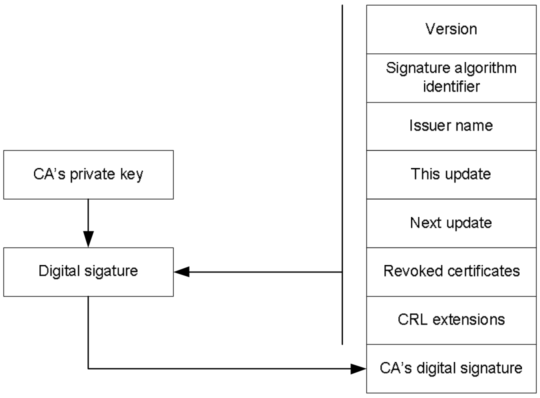


Figure 5. X.509 CRL Profile

5 X.509 ISSUES, SYSTEM ATTACK AND COUNTERMEASURES

Digital certificates are a good way for securing the internet users from attacks [10] especially in securing data confidentiality, integrity and a client/server authenticity. It means that the data should be transferred in an encrypted form to the right web site.

However, such mechanism is still vulnerable to attack. The attack may occur to the web client (browser), web server and even to the CA itself.

5.1 Attacking to CA

Attacking to CAs is likely to get the CA's root cryptographic signing key [11]. The key is very important because it is used to sign public keys of certificate holders and CA's public key itself. If the key is compromised, there may be lots of invalid certificates signed.

The CA attacker may be from either externals or internals. External attacks are hard to do because the CA system must be protected tightly. For example, it is protected by using firewall and intrusion detection system. According to [12], internal system is the common source of risk. Some mechanisms that can be performed to avoid internal attacks are:

- Limiting internals access
- Nobody knows a complete key (eg. by dividing key into some parts)

National Institute of Standard and Technology (NIST), National Security Agency (NSA) and Canadian Communications Security Establishment (CSE) have developed security standard as in Federal Information Processing Standard (FIPS) 140-1 (http://www.itl.nist.gov). This standard requires protection of root key by using a hardware from the beginning of deployment. Placing cryptographic key management and encryption in a hardware is more secure than in software because sensitive cryptographic processing can be offloaded from CA server [11].

5.2 Attacking to Web Client

5.2.1 Eavesdropping Attack

Digital certificates implementation which is usually using SSL protocol is still vulnerable to the eavesdropping attack. There is a tool, `webmitm`, which can be used to capture sensitive packets (eg. client credential) even the communication is SSL secured [13]. Even this attack is hard to do, subscribers (users) need to be aware of it and try to minimize the attack possibility. This can be done by installing intrusion detection system or using the on-line transaction as needed, for example.

5.2.2 Man-in-the-middle Attack

According to [14], it is easy for attackers to intercept SSL communication if they get the private key of server's SSL certificate. The key itself is protected so it is very difficult to steal.

Moreover, web client give a security alert to the users if they try to connect to servers whose an invalid certificate. The security alert gives some choices whether the users cancel or proceed the access. It is possible that the users just proceed it without checking whether they are communicating with the right server or not.

This security alert may be caused by:

- The certificate is signed by unrecognized CA
- The certificate date is invalid
- The certificate's common name field does not match the server's domain name

The first and third causes above can happen if, for example, the attackers may just use a self-signed certificate with a fake identity or real certificate stolen from other servers. So, if the users ignore the alert, it is possible that they are just communicating with the wrong servers and any information they sent is captured easily by the attackers.

5.3 Other Issue - Hash Collision

A CA has used hashing algorithm such as MD5 for signing certificates. However, this algorithm does not always provide unique result. Sometimes, two files have the same hash function value. Therefore, it is possible to construct two X.509 certificates whose signature is identical and only differ in public keys [15]. This has become a vulnerability of X.509 certificates.

That vulnerability can be exploited by attackers by changing the public key which may lead to attacks that affect on the integrity and repudiation. For instance, a user sends an encrypted message to a bank using bank's public key. However, since the bank has a pair public key collision, the bank is able to deny the message from the user, by saying that their public key is not that which is used by the user.

It needs for CA to find and use a better hashing algorithm to secure the certificates to avoid the collision. Moreover, finding two values whose hash function value are the same can be done only in hours [16].

6 CONCLUSION

X.509 digital certificate has been widely used in many applications. It provides some security features: authenticity, confidentiality, integrity, authority and non-repudiation. However, digital certificates are still vulnerable to the attacks. One of major vulnerability is the hashing collision which may impact on those security features. A certificate is only one of security tools that is better if combined with other security applications.

There should not be a gap between CRLs distribution and the transaction. The transaction should only be performed once the certificate used is valid that it is checked in CRLs. Therefore, CAs need to proceed such CRLs as soon as they receive the revocation request. On the other hands, subscribers should also report to the CA once their certificate is compromised. So, it is better to implement a reliable communication mechanism between subscribers and CAs in order to have a real time CRLs update and request.

In the common system, such as an e-commerce environment, only servers that need to have a certificate while in a system which need high level security, both client and server need to have a digital certificate. This is because, in implementing a certificate, it should verify the system environment before deciding what an effective architecture should be used.

Overall, X.509 digital certificate is applicable in the internet environment. It helps the organizations to secure their system and maintain the users' trust despite of its vulnerabilities.

7 REFERENCES:

[1] D. P. Barton, A. S. MoranL, and O'Connor, PKI design issues. Boca Raton, FL: Auerbach, 2004.

[2] Guo, Okuyama, and Finley, "A new trust model of PKI interoperability," presented at Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services 2005.

[3] R. Hollar and R. Murphy, Enterprise web services security. Massachusetts, USA: Charles River Media, Inc., 2006.

[4] M. Merkow, "Growing a tree of trust," in Public Key Infrastructure Building Trusted Applications and Web Services, J. R. Vacca, Ed. Boca Raton, FL: Auerbach, 2004.

[5] J. Feghhi, J. Feghhi, and P. Williams, Digital certificates – applied internet security. Reading, Massachusetts: Addison-Wesley Longman Inc.

[6] A. Rojanapasakorn and C. Sathitwiriyawong, "A performance study of over-issuing delta-CRLs with distribution points," presented at the 18th International Conference on Advanced Information Networking and Application (AINA'04), 2004.

[7] K. Bicakci, B. Crispo, and A. S. Tanenbaum, "Trust, recommendations, evidence, and other collaboration know-how (TRECK): How to incorporate revocation status information into the trust metrics for public-key certification," presented at the 2005 ACM symposium on Applied computing SAC '05, Santa Fe, New Mexico, 2005.

[8] Federal, Identity, Credentialing, and Committee, "X.509 certificate and certificate revocation list (CRL) extensions profile for the shared service providers (SSP) program," [On line] available at: http://www.cio.gov/ficc/documents/CertCRLprofileForCP.pdf [accessed: 28 April 2006]

[9] S. Santesson and R. Housley, "Internet X.509 public key infrastructure authority information access certificate revocation list (CRL) extension," [On line] available at:

http://www.ietf.org/rfc/rfc4325.txt [accessed: 26 April 2006]

[10] N. Issa, "Internet security," presented at 2004 International Conference on Information and Communication Technologies: From Theory to Applications, 2004.

[11] Deloitte, Touche, and Tohmatsu, CA system attack. Boca Raton, FL: Auerbach., 2004.

[12] S. Pramanik, V. Sankaranarayanan, and S. Upadhyaya, "Security policies to mitigate insider threat in the document control domain," presented at the 20th Annual Computer Security Applications Conference (ACSAC'04), 2004.

[13] H. Xia and J. C. Brustoloni, "Security through the eyes of users: Hardening Web browsers against man-in-the-middle and eavesdropping attacks," presented at the 14th international conference on World Wide Web (WWW '05), Chiba, Japan, 2005.

[14] S. Rahman, T. A. Nguyen, and T. A. Yang, "Developing certificate-based projects for web security classes," Journal of Computing Sciences in Colleges, vol. 21, 2006.

[15] A. Lenstra and B. Weger, "On the possibility of constructing meaningful hash collisions for public keys," [On line] available at: http://www.win.tue.nl/~bdeweger/CollidingCertificates/CollidingCertificates.pdf [accessed: 22 April 2006].

[16] V.Klimaptography.hyperlink.cz/md5/ MD5_collisions.pdf, "Finding MD5 collisions – a toy for a notebook," [On line], available at: http://cryptography.hyperlink.cz/md5/MD5_collisions.pdf [accessed: 25 April 2006].