Evaluation of Certificate Revocation in Microsoft Information Rights Management v1.0

Hong Zhou
hzho021@ec.auckland.ac.nz
for CompSci725SC, University of Auckland.
20 October 2006

Abstract

Certificate revocation regards as last process of the Public Key Infrastructure (PKI) life cycle. It is always ignored when people design and implement a secure application based on PKI and few people pay attention to it. Also it is quite controversial topic in PKI and critical to making PKI work. Additionally, it might expose the vulnerability of the consumer PKI applications without fully consideration of certificate revocation. So understanding revocation is very important concern to both PKI service providers and end users. In the paper, we are going to analysis the reason why we need certificate revocation. By given a case study, reader will know how serious could happened if the certificate do not revoked. And then we will generalize the requirement for certificate revocation to examine current PKI application especially Microsoft Information Rights Management (IRM) v1.0 system to see whether IRM meets the security requirements. At last we will provide the general solution for certificate revocation and also will see the whether IRM implement it.

1. Introduction

Symmetrical cryptography might be a way to deploy security within a closed user groups. But it is not properly way when we deploy security in open groups. As a result, the Asymmetrical cryptography represents today the most used technique. However, if the intruder can counterfeit public key, this technology is totally compromised. To solve this problem, public-key certificates (PKC) have been introduced to our application. Nowadays, the PKC has been deployed widely in most computers. In the RFC 2459, it gives a definition to PKC which explained that PKC is a data structure which securely binds a public-key value to a particular entity [1]. The identity information stored in the certificate enable users to be authenticated to each other, and public key in the certificates used to encrypt and decrypt messages traveling to and forward [2].

Moreover, the entity who supply digitally signature for PKC called Certification Authority (CA). CA has to confirm the identity and maybe some other attributes of the holder of the corresponding private key before signing the PKC. If the PKC was signed by CA, can you fully trust the PKC? The end-users still have to check current time is in the validity period which is between issue time and expiration time. Once the PKC expired, it should be not use anymore. End-user requires CA to issue new PKC to replace the expired one in spite of the new PKC might still is same key as previous PKC. However, this process of reissuing actually is not requirement of certificate revocation. We discuss here is that end-user detected or suspended comprise of the private key, change of name, change of the relationship with CA).

There are two parties, owner and issuer both should responsible for revoking a PKC. The revocation will directly influence to reach the users' needs to information security, which listed as Secrecy, Integrity, Availability and Accountability by Lampson [3]. In the Session 2 we will list several case studies to see why the two parties require revocation. After we see many requirements, in the session 3, we will generalize the requirement for certificate revocation. The requirements may be quite different from various user points of view. So we need to find current revocation techniques to solve different user requirement. And then, we will examine current PKI application especially Microsoft Information Rights Management (IRM) v1.0 system to evaluate whether this PKI application meets the security requirements. At the last session of the paper, we will provide the general solution for certificate revocation and also will see the whether IRM implement it.

2. Case studies

No matter how cautiously you prepared for, other reasons for invalidating keys still exist. At some point, some unpredictable problem will lead to a key compromise when it is least expected. End-user should stop relying on PKC after the private key is compromised even it still in validity period. In such case CA will revoke the certificate. Alternatively, the owner of the certificate may leave the company that issued the certificate. As the identity issued to the user linked him to the company, the identity must be invalidated. Once private key has been compromised, CA must notify certificate owner or subscriber.

As we known previously, CA as trusted party plays an important role in signing the PKC, so anyone should trust the CA signed PKC with no doubt. We might have a question whether the CA worth us to trust or whether the CA could abuse their trust. Unfortunately, even the VeriSign, one of the largest SS7 signaling networks in North America has made mistake in signaling PKC to their client.

2.1 Fake Microsoft Certificates

According to Microsoft Security Bulletin MS01-017, VeriSign issued two VeriSign Class 3 code-signing digital certificates to an individual who fraudulently claimed to be a Microsoft employee. The common name assigned to both certificates is "Microsoft Corporation". The ability to sign executable content using keys that purport to belong to Microsoft would clearly be advantageous to an attacker who wished to convince users to allow the content to run. [4]

Obviously the security threat for the case is that the attacker would probably be to convince other users to run an unsafe program, by using the digital signature to convince them that it is actually real Microsoft software and therefore safe to run. There are a variety of scenarios the attacker might use to accomplish this. For example hosting the signed program on a web site or sending an HTML e-mail that would retrieve it from a web site. [4]

VeriSign has revoked the certificates, and they are listed in VeriSign's current Certificate Revocation List (CRL). It is not possible for any browser's CRL-checking mechanism to locate and use the VeriSign CRL. Microsoft has developed an update that rectifies this problem. The update package includes a CRL containing the two certificates, and an installable revocation handler that consults the CRL on the local machine, rather than attempting to use the other mechanism.[4]

3. Circumstances for certificate revocation

From the case studies we know how important the certificate revocation is, in this session, we will discuss what is the circumstances might cause the revocation. Because once the certificate has been revoked, all the application or system relying on the certificate might be exposed to malicious parties and under risk. As a result, we can not ensure secrecy of information when using the public key retrieved from the certificate to encrypt and decrypt secure message. Also the integrity of certification can not ensure if any of this certification was signed by using the key from the invalid certificate. Even the application notices there is a certificate revocation, but it can not be invoked immediately, accessibility will be an issue. So to decide revoke a certificate will be painful for the CA as well as key subscriber whose application based on PKI.

According to VeriSign’s certification practice statement (CPS) [5], we list several circumstances shown on below, which might cause certificate be revoked by CA. CA will flag the certificate as invalid in its database publish the certificate on a CRL.

Reasons:

1. If any one of the CA, certificate subscriber or end-user believes or strongly suspects a subscriber’s private key has been compromised. For example: The owner of the certificate may leave the company that issued the certificate.
2. The certificate subscriber’s name changed. For example: we suspect if the company was been merged or brought by the other company.
3. The affiliation between end-users with subscriber is terminated or has otherwise ended. For example: we suspect if the person who is no longer an employee or their contract with the company was terminated.
4. The information within the certificate, other than non-verified subscriber information, is incorrect or has changed. For example the certificate applied area changed.
5. The subscriber or end-user believes that the certificate was issued in a manner not

materially in accordance with the procedures required. The certificate was issued to without the authorization of the person named as the subject of certificate. For example: in previous case, the certificate was issued without the authorization of the person was real Microsoft employee.

We could not imagine all the cases cause for certificate revocation, but at least we can the list to examine if the case happened to Microsoft Information Rights Management v1.0

3.1 Circumstances for certificate revocation in IRM

The following definitions and objectives of RM and IRM were sourced from the Microsoft website:

> *"Microsoft® Windows® Rights Management – RM is a new Windows platform policy enforcement technology that enables a stronger level of protection of information at the file level. This technology augments existing perimeter based solutions.*
>
> *Windows Rights Management Services – RMS is a Windows Server 2003 premium service that enables RM-capable applications such as Office 2003 to express and enforce rights that are assigned to information.*
>
> *Information Rights Management – IRM is an extension of Windows Rights Management into Microsoft® Office 2003 applications. IRM in Office 2003 requires RMS on Windows Server 2003, either within the organization or via a Microsoft service. IRM is a persistent file-level protection technology that helps protect digital intellectual property from unauthorized use. IRM extends the Windows® Rights Management Services into Microsoft® Office 2003 applications and into Microsoft Internet Explorer."*

Instead of explaining what IRM is and what it can do, we will only discuss here is what circumstance cause IRM server to revoke certificate. The 'trust chain' of public key certificates from the Microsoft RM Root CA down to the end users is illustrated in the following figure. For more information about IRM,

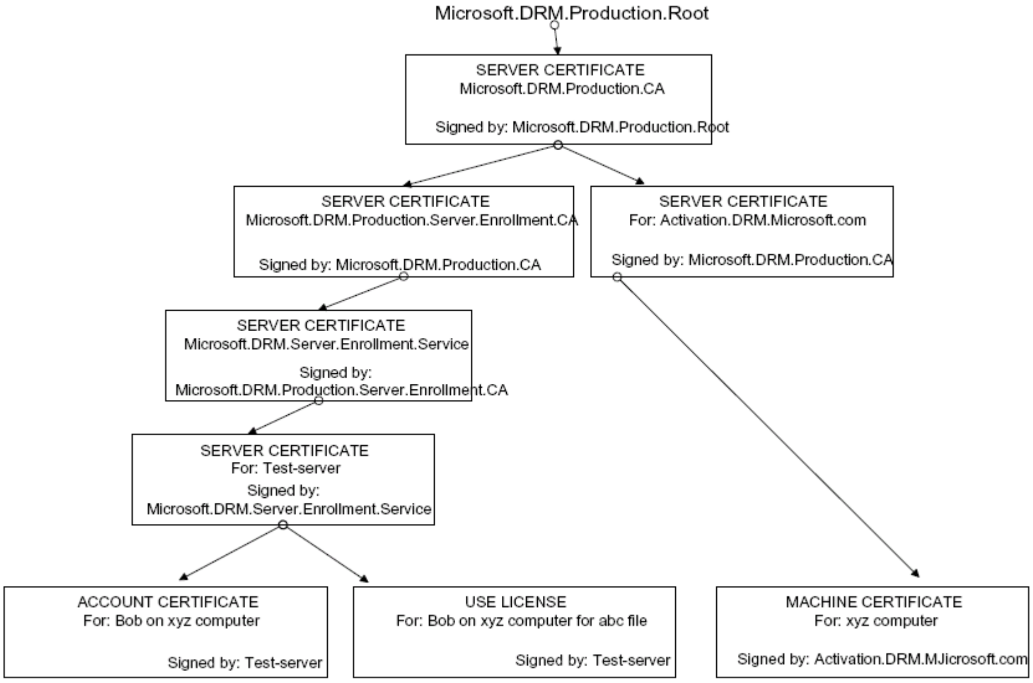
Microsoft.DRM.Production.Root
SERVER CERTIFICATE
Microsoft.DRM.Production.CA
Signed by: Microsoft.DRM.Production.Root
SERVER CERTIFICATE
Microsoft.DRM.Production.Server.Enrollment.CA
Signed by: Microsoft.DRM.Production.CA
SERVER CERTIFICATE
For: Activation.DRM.Microsoft.com
Signed by: Microsoft.DRM.Production.CA
SERVER CERTIFICATE
Microsoft.DRM.Server.Enrollment.Service
Signed by:
Microsoft.DRM.Production.Server.Enrollment.CA
SERVER CERTIFICATE
For: Test-server
Signed by:
Microsoft.DRM.Server.Enrollment.Service
ACCOUNT CERTIFICATE
For: Bob on xyz computer
Signed by: Test-server
USE LICENSE
For: Bob on xyz computer for abc file
Signed by: Test-server
MACHINE CERTIFICATE
For: xyz computer
Signed by: Activation.DRM.MJicrosoft.com

Figure 1: from [6]

To examine whether pervious reason for certificate revocation applied to IRM, we made a table to describe it. In table 1, firstly column will be simplified reasons, second column is the decision we made, and third column will be reason why we made the decision.

Circumstances	Chance for IRM to revoke certificate?	Reason
1. Private key has been compromised	Less	1. People have to figure out how the CryptoAPI work to get private key in Test-Server for signing account certificate. 2. It is hard to get the private key for signing Test-Server which stored DRM server in Microsoft.
2. The certificate subscriber's name changed	Middle	It is possible someone create fake Test-Server which has already been authenticated as the same name in the trust chain.
3. The affiliation between end-users with subscriber is terminated	High	The employee might leave company, it account might be told to the other colleague.
4. Non-verified subscriber	Less	It will depend on system implementation. But I

information, is incorrect or has changed		don’t think that is the case because the certificate issued from the test-server is follows the procedure which people design IRM.
5. The subscriber or end-user believes that the certificate was issued in a manner not materially in accordance with the procedures required	Less	Also It will depend on system implementation. I don’t think that is the case because the test-server is program follows the procedure which people design IRM.

Table 1

4. Current certificate revocation solutions

Current proposed standards for revocation involved with certificate revocation lists (CRL) maintained on key servers. So the key server must be stable, reliable computer system which is accessible over the network that distributes certificates. If subscriber wants to revoke a certificate, it has to send the key server a revocation notice. In this request, it will include the certificate identification such as serial number of the certificate and it has to sign by the third authorized entity. Because this message could be intercepted and modified by attacker due to CA key compromised. Otherwise, it is CA responsibility to make the decision to revoke a certificate, usually as a response to a request also has to come from an authorized entity.

As we known at pervious case studies, VeriSign published their revoked certificate in CRL, Explained by [7] it is one of major mechanism to retrieve the certificate status. CA authenticates the source of the revocation request and after taking the decision to revoke the certificate, the CA has the obligation to inform the subscriber and end-users about the revocation event. To allow retrieving the certificate status, we can classify them into two major methods:

1. CRL-based mechanisms.

The primarily used method for revocation notification in PKI is by means of certificate revocation list (CRL). As we known, there are four popular types for CRL retrieve listed as windowed CRL [8], CRL distribution point (CRLDP) [9], delta CRL [9] and indirect CRL

2. Contrast with CRL-based mechanisms, another providing immediate notification of revocation which is the on-line certificate status protocol (OCSP) [10] represents the solution.

There might be other protocol to design for revocation but they have similar design goals of correctness, scalability, and availability, for example all verifiers must be able to correctly determine the state of a certificate within well-known time bounds and the costs for the determination of current revocation status of certificates should not be expensive.

4.1 Revocation solutions in IRM

Actually we have not seen any above revocation solutions applied to IRM after analyzing the service providing by IRM server. By looking at row data collected by [6], the machine activation only sends the information of OS and CPU. Then it will receive the machine certification signed by Activation.DRM.Microsoft.com. And later the Test-server RM Certification Server will issue the account certificate to individuals. If user want to perform IRM functions on different computer, each computer have to be activated and have user account certificate on it. So if we want to revoke the client certificate in IRM system, we have to revoke all client account certificates in all machines which have been performed IRM function for the client. The workload would be huge for IT security staff to update all machines' CRL once one employee leave from the company. Otherwise, the frequency of checking the CRL from every IRM end-user still might be an issue. I think it might be the feasibility reason why the Microsoft does not implement the revocation service in local RM Certification Server. But I believe that there must be a mechanism to protect key compromise at Enrolment Service CA and Machine Activation Service CA inside of Microsoft. Moreover the identity of the end-user is differentiated by email account, so to activate the correct account certificate is based on trust safety of email account, but at least we know the email account password can be attack easily when user daily use. As a result the account certificate might be issued unsafely.

5. Conclusion

We have seen by looking at the general requirement for certificate revocation that possibly happen in every secure application build on PKI. If we do not give a fully consideration, it will cause entire PKI vulnerability impact. In addition we examined Microsoft Information Rights Management (IRM) v1.0 system to evaluate whether this PKI application meets the security requirements. We have also seen that it is possible solution to revoke the certificate which classified in CRL and immediate notification of revocation. However I could not said that a secure application based on PKI must implement certificate revocation. At least we might suspect the system exist vulnerability if they have no mechanisms to handle certificate revocation or do not handle properly. In conclusion, Microsoft IRM v1.0 will face security threat in issuing account certificate and machine certificate, but now it protected under the window authentication and a number of group policy. Further work will analysis how to designs suitable revocation to achieve availability and accountability for specified system in order to fully address the security needs of users and how a PKI application implements revocation efficiently.

Reference:

[1] R. Housley, W. Ford, W. Polk, and D. Solo. "Internet X.509 Public Key Infrastructure Certificate and Crl Profile." no. RFC 2459 (1999).

[2] Wikipedia. "Public Key Infrastructure." 2006.

[3] Lampson, B.W. "Computer Security in the Real World." Computer Volume 37, no. Issue 6 (2004): 37 - 46.

[4] Diana Berbecaru, Antonio Lioy, Marius Marian. "Security Aspects in Standard Certificate Revocation Mechanisms: A Case Study for Ocsp." Proceedings of the Seventh International Symposium on Computers and Communications (2002): 1346.

[5] Microsoft. "Erroneous Verisign-Issued Digital Certificates Pose Spoofing Hazard." June 23, 2003.

[6] Garden, Jay. "Review of Microsoft Information Rights Management V1.0." 2003.

[7] VeriSign. "Verisign Certification Practice Statement." 30-32, May 01, 2006.

[8] P. McDaniel and S. Jamin. Windowed Key Revocation in Public Key Infrastructures. EECS University of Michigan, Tech. Rep. CSE-TR-376-98, 1998.

[9] ITU T Recommendation X.509-ISO/IEC 9594-8. 1995.

[10] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. IETF, RFC 2560, 1999.