Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Securing Certificate Revocation List Infrastructures

Anyone working within a Public Key Infrastructure (PKI) or an environment that uses client side certificates should be concerned that during authentication the Certificate Revocation Lists (CRL) are consistently & properly verified. Microsoft's Internet Information Server (IIS) 5.0 built-in Certificate Revocation List Infrastructure has been openly questioned from several security professionals and been a part of at least one major security vulnerability. This research takes a closer look at the security issues when im...

Copyright SANS Institute

Author Retains Full Rights

AD

Automate more Web application scanning.

watchfire

Eddie Turkaly

Version 1.2e

Securing Certificate Revocation List Infrastructures

Introduction

Anyone working within a Public Key Infrastructure (PKI) or an environment that uses client side certificates should be concerned that during authentication the Certificate Revocation Lists (CRL) are consistently & properly verified. Microsoft's Internet Information Server (IIS) 5.0 built-in Certificate Revocation List Infrastructure has been openly questioned from several security professionals and been a part of at least one major security vulnerability. This research takes a closer look at the security issues when implementing a secure CRL infrastructure as well as looking deeply into how secure Microsoft's IIS 5.0 built in Certificate Revocation List Infrastructure is. Then we will explore alternative CRL solutions from Internet Standards, PKI Toolkits and middle-ware products. Finally, this research should provide you with the security awareness ins and outs for implementing a secure CRL infrastructure.

Importance for Comprehensive CRL Infrastructures

Within PKI, a user generally receives a certificate, sometimes called a client side certificate, from a trusted root Certificate Authority (CA). Certificates help to prove the identity of an individual. Most PKI certificates contains a well know feature or extension called the Certificate Distribution Point (CDP). You can view the CDP by viewing the details of the certificate. The CDP is nothing more than a path or protocol for the location of where the Certificate Revocation Lists (CRL) is available. The path can be in the form of a URL, or a Universal Naming Convention (UNC), or by Lightweight Directory Access Protocol (LDAP). In fact, the CDP can contain more than one type of path to contact the CRL.

A client side certificate, web server and the CRL work together to perform what is called the Certificate Revocation List Infrastructure. Web servers can make use of client side certificates to help manage remote web users. Administrators can assign rights and privileges based on end users certificate, effectively controlling what may or may not be accessed.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

CRL's contain lists of revoked certificates, which the original CA produced. Certificates are created from a Root Certificate Authority. It is the Certificate Authority that issues the originated certificate CRL's periodically. Every client side certificate has a life span, generally of 3 to 5 years. However, if during that lifespan the certificate must be revoked then the certificate serial number is placed on the Certificate Revocation List. The CRL is a digitally signed, time-stamped blacklist of revoked certificates that have not expired. Certificates ensure a chain of trust up to the creator or root certificate authority. Thus, PKI enabled applications or web based applications using certificates must verify this chain of trust and ultimately check against a CRL.

CRLs have some major flaws. For one, they do not operate in real time. Many commercial certificate authorities issue CRLs only once per day at the most. Since each root CA is responsible for updating their CRL, each root CA has different frequencies at which a CRL is updated. For example, the Department of Defense may update their CRL's every eight hours. This means that maintaining the most current CRL becomes critical. Yet placing a certificate on the CRL is not enough. Each application that requires authentication must check the CRL each time the certificate is submitted. Each CA keeps only one CRL for each root certificate, which is a top-level certificate under which many individual certificates are issues. The CRL is cumulative since every revoked certificate is added to the CRL and kept there until it expires. Thus, the CRL file size can become very large. CRLs, for example, issues by VeriSign at http://crl.verisign.com, can be a megabyte in size. This means that transmitting, publishing and processing a CRL is a time consuming process that eats CPU power. This constraint can grow especially if a web site must check certificates against multiple certificate authorities, which possibly could happen after a merger of companies that use different PKI's. Finally, when a certificate authority updates its CRL, it overwrites the previous file, thus keeping no historical data.

Being able to verify the validity of certificates is extremely important to the integrity of a certificate management system. As you can see, it is critical for any application or web server depending on a certificate management system to ensure certificates are not on a CRL list. Events such as staff turnovers and changes in business relationships can create the potential use of non-valid certificates resulting in security breaches. The longstanding method for checking the status of digital certificates has been governed by the use of Certificate Revocation Lists (CRLs) in which applications retrieve CRLs at set intervals. An inherent weakness in CRLs, however, is that there is a potential delay before information regarding a revoked certificate is available to the application.

A Vulnerability Discovered

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

It is interesting that during my research I noticed that Microsoft's CRL Infrastructure was not very well documented. The only documents worth mentioning originate *after* a security vulnerability was discovered. The vulnerability occurred January 2001, when VeriSign issued two Class 3 code-signing certificates to someone falsely claiming to represent Microsoft. About six weeks later, a routine VeriSign audit uncovered the error and VeriSign reportedly did three things: 1. It notified Microsoft. 2. It posted a public notice. 3. It revoked the certificates in its normal Certificate Revocation List (CRL).

Bruce Schneier, the well-known and widely respected security expert, wrote about the episode in the April issue of the monthly newsletter Crypto-Gram, in an article entitled *"Fake Microsoft Certificates"* http://www.counterpane.com/crypto-gram-0104.html#7. Schneier made several statements that, in brief, concluded that Windows had no CRL features installed within it. Of course, Microsoft did not agree with Schneier and published its own article titled: *"Response to Inaccurate Crypto-Gram Article on VeriSign Certificates"*. http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/itsolutions/security/news/VeriSign.asp The article specifically claimed that a way to revoke certificates using a CRL in Windows was available:

> "There is a way to revoke the certificates – via the Certificate Revocation List (CRL) mechanism defined in the relevant industry standard, RFC 2459. And Windows does indeed have CRL features – CRL support has been available for the Windows NT family since 1998, and for the Windows 9x family since early 1999" (Microsoft).

However, VeriSign did not provide the CRL distribution point extension of RFC 2459, and it was within standardized practice to omit it. In other words, RFC 2459 does not require the Certificate Distribution Point (CDP) to be contained in every type of Certificate. Regardless of this, Microsoft objected to this omission. Yet, Microsoft was entirely free to omit VeriSign's Class 3 code-signing root certificates from its product, and prevent all such certificates issued by VeriSign from being accepted. In other words, the default out-of-the box install of Windows NT and Windows 9x already contains the certificates that trust the VeriSign root CA who issued the Class 3 code-signing certificates. No one forced Microsoft to use VeriSign certificates lacking the CRL extension. Thus, Microsoft alone chose to do so.

Microsoft's CRL Infrastructure

The Microsoft CRL vulnerability helped produced more MS CRL Infrastructure documentation. For our purposes the most important MS article is Q289749 entitled *"Certificate Revocation Lists (CRL) and IIS 5.0: Common*

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Questions" located at
http://support.microsoft.com/support/kb/articles/Q289/7/49.ASP which provides the best technical explanation I can find on how Microsoft CRL infrastructure works.

Q289749 describes how the CRL is automatically downloaded by the MS component called CryptoAPI. (CryptoAPI is another subject that is outside the scope of this document) The article states that the download of the CRL would only occur if a CDP is present in the certificate. Of course, we have seen from the Microsoft/VeriSign tragedy that the automatic download is fully dependent on the fact that a CDP in the certificate is available. This means that if a certificate does not contain a CDP then no download of a CRL is possible. If you are depending on Microsoft, be sure that your PKI environment or web server depends on the CDP extension before authentication. Q289749 then states that CRL's are cached in the System profile folder located in:
\Documents and Settings\SYSTEM\Local Settings\Temporary Internet Files.

Microsoft also makes a note that the current CRL is always stored in the profile of the identity under which IIS is running and by default IIS is suppose to be running in the "System" account. After testing the statements made from Q289749 in my own lab, my results proved that in fact Q289749 is wrong and perhaps misleading. The CRL's are in fact installed in the directory:
\SystemRoot\Documents and Settings\Default User\Local Settings\Temporary Internet Files

This directory, or cached directory, appears as a single directory within Windows Explorer. This is because a shell handler is invoked. Yet, if you look at this directory from a command prompt, where shell handlers are not used, you will see that in fact a series of subdirectories are within the Temporary Internet Files folder. Internet Explore uses API's to store cached content into these folders. Either delete the shell handler or use the command prompt to see the downloaded CRL's.

The major problem is that IIS automatically obtains a new CRL only when the cached one's validity period has passed. In other words, the validity period of a CRL is typically longer than the next scheduled release of the new CRL. You can check the validity period of a CRL by looking at its properties. This means that the validity period of the CRL is not running at the same schedule for which the root CA makes updates to the CRL's, those CRL's are not refreshed until they expire! This is a major problem if you do not have central control of your CA. If you do have control over your CA then the only way to make IIS re-obtain a CRL is to have each CA Publishing CRL's validity period be set at the same amount of time it takes for the new updated CRL (for example in most DOD environments this is every 8 hours). According to the Q289749 article, the smallest validity period for a Microsoft Certificate Authority server is 1 hour. This means that if your CA is a Microsoft CA, then you can set you CRL's to be only

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

good for one hour. This approach assumes, of course, that you have sufficient control over the CA and that you can dictate the CRL issuing interval. This is unlikely since most CA's are not running a MS CA, such as ones from VeriSign, Entrust, Baltimore, Thawte, ECT...

In conclusion, the MS Certificate Revocation Infrastructure works at its best only when you are using their Certificate Authority and not when using a CA from a third party. Of course, your web users will likely have certificates from multiple CA's and chances are you will not have any administrative control over these CA's. If this is your case, then you need a more comprehensive solution for ensuring CRL's are obtained from all appropriate CA's and in a timely fashion.

Reverse Proxy "gotcha"

If you're planning to use client side certificates then another important "gotcha" exist if your organization is using "reverse proxy" servers. Reverse proxy is a proxy for the Internet to manage and secure your web or other resource servers. When using SSL as your encryption for Internet data and using MS Proxy 2.0 then your SSL connections are being terminated at the proxy sever and not at the resource server. This may become a problem since you cannot "route" a client side certificate via SSL. SSL is required by IIS 4.0/5.0 when using client side certificates. This may become a potential problem as you may find yourself asking how you are going to get client certificates to your resource server.

One possible way to solve this problem is to use the new IAS proxy server from Microsoft. Although I have not tested it, Microsoft reports that IAS proxy has the capacity to reroute an SSL connection without interfering with that connection. This may allow you to continue the client certificate down the pipeline. The other way is to select form many of the third party solutions.

Better Solutions for CRL Infrastructures

As you can see, depending on Microsoft alone to secure your CRL Infrastructure is not sufficient. However, several options are available to extend your certificate revocation list infrastructure, ranging from standards to third party solutions. Let us look more closely at your options.

Internet Standards

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Online Certificate Status Protocol (OCSP) lets an application quickly verify a certificate's validity in real time. OCSP version 1 was standardized by the Internet Engineering Task Force (IETF) June 1999 in RFC 2560. Version 2 is currently being worked on. In an OCSP based system, when a certificate needs validation, the application passes a request to an OCSP responder. Responders are sold as part of PKI products or as independent packages. Third party vendors such as KyberPASS Validation Trust Platform or ValiCert's Validation Authority contain responders. The responder verifies the certificate, informing the client whether the certificate has been revoked. The responder can be a simple repository for the latest CRLs, but it adds more value when it allows revocation of certificates in real-time from an administrative interface. The responder sits on the network and answers queries form applications that need CRL validation. The OCSP version 2 will add the ability to request information on the status of a certificate from the past, a feature currently not supported. Some of the additions suggested for OCSP version 2 may be put in its own protocol called Simple Certificate Validation Protocol (SCVP). It is argued that instead of making the existing OCSP protocol more complicated why not make SCVP the standard to add functionality. SCVP is still in the IETF draft processes.

Regardless of which protocol IETF drafts, OCSP version 1 works. This means that when you look into providing any third party tool to help validate certificates, be sure the product supports OCSP.

PKI Toolkits

Several CRL checking tools and solutions are available. From an administrative perspective, your job is to ensure web user sessions are authenticated against current revocation information. Large PKI vendors such as Entrust, Baltimore, RSA and VeriSign can help meet this need. They will tell you to "PKI enable" your applications, also know as PKI Toolkits. By doing this all of your applications will have, among other things, built in code to check certificate validity. However, this does not fully solve all your problems. Each vendor handles the validation differently, and some may recommend that you purchase a middle-ware solution in conjunction with their solution.

Keep in mind that PKI-enabling your applications is a very large task and quite expensive. Implementation and ongoing support is labor-intensive making time to market very slow. PKI Toolkits require PKI and security development expertise on staff. Generally, toolkits are not available for mainframe legacy applications. In addition, applications are bound to a particular PKI vendor, their licensening, standards interpretation, interoperability, and support strategies. As If it could not ask for more, PKI Toolkits require access to source code, so commercial applications cannot be supported without the vendor involvement.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Therefore, Toolkits are best used for PKI-enabling a vendor's commercial application, experimentation, and pilot projects. I do not think that toolkits are suited for wide scale enterprise deployment. Be aware that if your organization is purchased or merged with another organization you may end up with more than one PKI solution.

Both Entrust and Baltimore Technologies use a toolkit solution. While evaluating Baltimore, I did not find any CRL functionality. In fact the only information I found is the excerpt that comes from the KeyToolsPro v5.0.5 Developer's Guide, which in Section 9.3 sates: "it is up to the users to ensure that they have the most up-to-date copy of the CRL". Obviously, that solution is not what we are looking for. Entrust recommend to me that I use ValiCert – a middle-ware solution.

Although RSA did not claim to have any built-in certificate revocation checking products, they were positive. After speaking to a representative, he indicated that a future product would provide CRL support. Unfortunately, he did not provide additional details. However, I noticed that on February 1, 2001 RSA Security announced that it acquired Xcert International, Inc., a privately held company that develops and delivers digital certificate-based products for securing e-business transactions. With this acquisition, Xcert Sentry became a member of the RSA Keon family of PKI products, now known as RSA Keon Certificate Authority. From the website at RSA in the paragraph entitled 'Exclusive Real-Time Status Checking' it states:

> With RSA Keon real-time OCSP there is no time lag during which users could gain access to the system after their certificate has been revoked — thereby eliminating the threat of security breaches through the use of non-valid certificates. RSA Keon CA software also fully supports industry standard CRLs (RSA Keon Certificate Authority, Paragraph 7).

If you can afford the costs, time and headache associated with PKI-enabling your applications then from a security perspective this option is well worth it. Otherwise, you might be interested in the middle-ware solutions.

Middle-ware Solutions

In order to mitigate the costs associated with PKI-enabling your applications you could simply use a middle-ware solution. These solutions are called middle-ware solutions because they provide centralized certificate validation on behalf of all applications. The following are some examples.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

ValiCert has a product called Validation Authority http://www.valicert.com/products/validation_authority.html. ValiCert supports all revocation checking types: CRL's, OCSP, SVCP and CRLDP. One very nice feature of CertValidator is that the validation, or VA, can replicate its database to another VA, including cached info if desired. If you were a battleship that came to shore only so often, then this option would be useful. Another feature is that VA can put certificates in "suspend mode", thus not having to wait on a CA to do it for you! This provides some control if you have no control over the root CA. Finally; CertValidator works closely with the PKI vendors Entrust, Baltimore and X-Cert (RSA). This means that if you plan on PKI-enabling your applications at a later time you can plug and play with CertValidator.

KyberPASS http://www.kyberpass.com/ takes a very interesting approach with their Kyberpass Validation TrustPlatform. They provide centralized certificate validation on behalf of all applications and even supports OCSP. Version 4 concurrently supports multiple Certificate Authorities and PKI's for seeking out user certificates.

Their solution does many of the same things as ValiCert but then takes it a few steps beyond. KyberPASS proposes that with their middle-ware solution all you applications become PKI-enabled. By your entire network traffic going through the KyberPASS server it can then translate and even manipulate every connection. It can tunnel all applications through a customer defined single port on the firewall. You can use KyberPASS to re-map the outbound port to a single port number. This means KyberPASS will accept all packets through the single port and transparently fan out the packets to the appropriate application proxy for delivery to the destination server. This capability provides a more secure implementation on the firewall by only opening up one hole rather than one hole per application.

Another example is a product form CertCo called CertValidator http://www.certco.com/certvalidator.shtml. Once again, CertCo is a lot like ValiCert, with features such as certificate suspension, interoperability with other major PKI vendors and real time validation using OCSP. At the time of publication of this paper, Certco's product only ran on Windows NT 4.0 and only supported CRL validation by OCSP responders. While OCSP is likely the future for CRL checking, some networks may not be able to immediately support it. For example, if you are a DOD employee, OCSP will not be available until the release of DOD PKI Class 5. Check with your CA or registration authority for details.

Conclusions

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

This research paper has deeply detailed the issues concerning Certificate Revocation List infrastructures. We started by discussing the vulnerability that occurred to Microsoft after VeriSign removed fake certificates. This demonstrated the importance of having a working CRL infrastructure. We looked at Microsoft's so-called built-in CRL infrastructure. We discussed how the Microsoft IIS 4.0 & 5.0 products contain a major error regarding how IIS automatically obtains a new CRL only when the cached one's validity period has passed. We also discussed that to only improve on their CRL Infrastructure is to have a MS Root CA, a limited option for most of us. Then we looked into the OCSP & SVCP standards, PKI-enabled solutions, and finally the middle-ware solutions. These solutions demonstrate your many options.

Of all the options, I believe the best CRL infrastructure is by using a middle-ware solution. They are a prudent choice since the Internet, software, standards, and market conditions are always changing. Moreover, PKI solutions currently lack the focused functionality middle-ware solutions possess. They appear to have fewer strings attached. If you cannot justify the costs of middle-ware or PKI solutions then your best bet is to wait on standards to take over. Whatever you select, you should now realize the importance of not depending on the current Microsoft built in CRL infrastructure.

References

"Introduction to Public-Key Infrastructure"
URL: http://www.iplanet.com/developer/docs/articles/security/pki.html

Schneier, Bruce. "Fake Microsoft Certificates." Counterpane Internet Security, Inc. Crypto-Gram Newsletter. April 15, 2001. URL: http://www.counterpane.com/crypto-gram-0104.html#7 (5 Sept. 2001)

Microsoft. "Response to Inaccurate Crypto-Gram Article on VeriSign Certificates." Microsoft Corporation. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/itsolutions/security/news/VeriSign.asp (5 Sept. 2001)

R. Housley, W. Ford, W. Polk, D. Solo. "X.509 Public Key Infrastructure Certificate and CRL Profile." Network Working Group Request for Comments: 2459. January 1999. URL: http://www.ietf.org/rfc/rfc2459.txt (5 Sept. 2001)

M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams. "Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP." Network Working

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Group Request for Comments: 2460. June 1999. URL: http://www.ietf.org/rfc/rfc2560.txt (5 Sept. 2001)

Microsoft. “Certificate Revocation Lists (CRL) and IIS 5.0: Common Questions." Microsoft Corporation Product Support Services Article Q289749. March 15, 2001. URL: http://support.microsoft.com/support/kb/articles/Q289/7/49.ASP (5 Sept. 2001)

RSA. “Exclusive Real-Time Status Checking” RSA Keon Certificate Authority. Paragraph 7. URL: http://www.rsa.com/products/keon/datasheets/dskeoncertificateauth.html (5 Sept. 2001)

ValiCert. “Validation Authority” URL: http://www.valicert.com/products/validation_authority.html (5 Sept. 2001)

KyberPASS. “Kyberpass Validation TrustPlatform.” URL: http://www.kyberpass.com/ (5 Sept. 2001)

CertCo. “CertValidator” URL: http://www.certco.com/certvalidator.shtml (5 Sept. 2001)

© SANS Institute 2001, Author retains full rights

Last Updated: September 4th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced