PUBLIC KEY INFRASTRUCTURE CERTIFICATE REVOCATION LIST VERSUS ONLINE CERTIFICATE STATUS PROTOCOL

CERTIFICATE REVOCATION CHECKING ON CISCO IOS SOFTWARE

Introduction

The support for x.509 digital certificates was first offered in Cisco IOS® Software Release 11.3T. The digital certificate functionality in Cisco IOS Software has evolved over time to offer a greater breadth and depth of capability with a number of significant advances appearing in Cisco IOS Software Releases12.2T and 12.3T. Digital certificates offer a scalable and secure option for managing identity and encryption information by automating the distribution of cryptographic key material and by offering effective identity authenticity mechanisms.

Occasionally a Public Key Infrastructure (PKI) must revoke a certificate issued under certain conditions, such as compromise of a certificate's encryption keys or change in status of an encryption peer, which holds this certificate (e.g. termination of employee or theft of encryption devices). Cisco IOS Software and most of other vendors, who integrate certificate functionality, accommodated this requirement by implementing Certificate Revocation List (CRL) checking functionality in order to ascertain the validity status of digital certificates presented by encryption peers. Establishing of certificate validity by checking CRLs is effective for most circumstances, but some applications may require a more frequent update for certificate revocation information. Cisco IOS Software Release 12.3(2) T introduces support for Online Certificate Status Protocol (OCSP), which offers an online mechanism for determining certificate validity without placing an undue burden on the PKI and associated network. This document qualifies the differences between CRL and OCSP, offering the reader a better understanding of the subject, which helps to make an educated choice between these two mechanisms. A technical discussion of CRL checking and OCSP use is also included in this document.

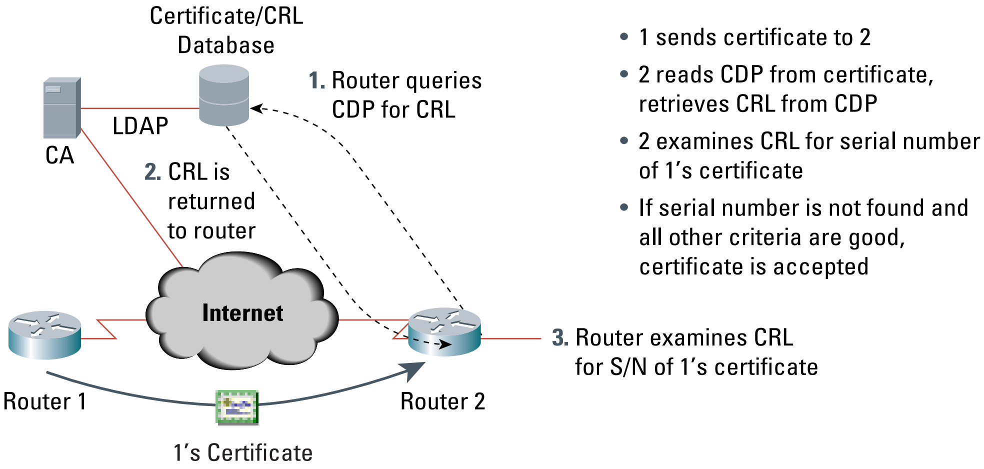
Cisco IOS Software offers another powerful option for certificate status checking in the "PKI+AAA Integration" feature, which adds the additional capability of retrieving authorization information and returning accounting data to a AAA server. As this feature offers functionality and features significantly departing from the revocation checking purpose of CRL and OCSP it will not be covered in this document. For additional information please visit:

http://www/en/US/products/sw/iosswrel/ps5187/products_feature_guide09186a00801b0692.html

CERTIFICATE REVOCATION LISTS

A CRL is a list of revoked certificates that have been issued and subsequently revoked by a given Certification Authority. Certificates may be revoked for a number of reasons including failure or compromise of a device that is using a given cert, compromise of the key pair used by a certificate, or errors within an issued certificate, such as an incorrect identity or the need to accommodate a name change. The mechanism used for certificate revocation depends on the Certification Authority. Most Certification Authorities support cert revocation from the management interface.

Figure 1
Cert Validation with CRL


Certificate/CRL Database
1. Router queries CDP for CRL
LDAP
CA
2. CRL is returned to router
Internet
Router 1
Router 2
1's Certificate
3. Router examines CRL for S/N of 1's certificate
• 1 sends certificate to 2
• 2 reads CDP from certificate, retrieves CRL from CDP
• 2 examines CRL for serial number of 1's certificate
• If serial number is not found and all other criteria are good, certificate is accepted

Revoked certificates are represented in the CRL by their serial numbers. If a network device is attempting to verify the validity of a certificate, it will download and scan the current CRL for the serial number of the presented cert. The CRL is signed by the Certification Authority to ensure the authenticity of the document and may be distributed through a variety of protocols, such as http, ldap, tftp, or other services. CRLs are generally published on a periodic interval, or Certification Authorities may publish a new CRL any time a certificate they are responsible for is revoked. Like most documents created by a PKI, the CRL has an expiration time, date, and all components of a PKI that will verify that certificates should download a new copy of the CRL, when the old CRL expires. Cisco IOS Software based devices cache CRLs until they expire, than the router deletes the CRL from cache. A new, "fresh" CRL is downloaded when certificate is presented for verification again and the cached CRL has been deleted. Unfortunately, the router's cached CRL causes one of the problems for using CRLs. If a newer version of the CRL that lists certificate under examination is present on the server, but the router is still using the CRL in its cache, which does not list the revoked cert, the certificate will pass its revocation check even though it should have been disallowed.

The CRL may eventually grow to a cumbersome size in very large PKIs. Prior to its update PKI software, embedded in Cisco IOS Software, allocated roughly 64K of memory space for processing and caching CRLs, which was adequate under most circumstances for maintaining a local copy of the CRL. After the Cisco IOS PKI Software update, the Cisco IOS Software allocates memory until the local available memory is nearly consumed. If a PKI has revoked so many certificates that the CRL exceeds a cumbersome size, it is worthwhile to look into breaking the CRL into multiple files. This will save bandwidth and time when cryptography peers download a new copy of the CRL and will ensure that a Cisco IOS Software router will have sufficient buffer space to hold and scan the CRL for revoked certificates. The specific of dividing the CRL into a number of more manageable files is outside of this document's scope; however, PKI documentation should offer design guidance for deploying the optimal CRL distribution scheme.

CRLs are practical for most PKI applications, but may not be appropriate for some uses. Some instances where CRLs are not adequate include:

- Large numbers of revoked certificates or multiple CRLs. CRLs in cache on devices can consume a large quantity of memory. Downloading large CRLs over low-speed links may use excessive bandwidth, which causes network congestion.

- Frequent CRL expiration. If CRLs expire frequently, the Certificate Distribution Point (CDP) will be heavily loaded, and frequent CRL download will burden network devices and bandwidth with non-production traffic.
- Immediate notification of cert revocation is required. Some high-security applications require more immediate notification of cert revocation. If CRL has a two day expiration interval, it may be up to 48 hours before a router downloads a new CRL. This leaves a long period of time before a router is notified that a certificate is no longer valid.

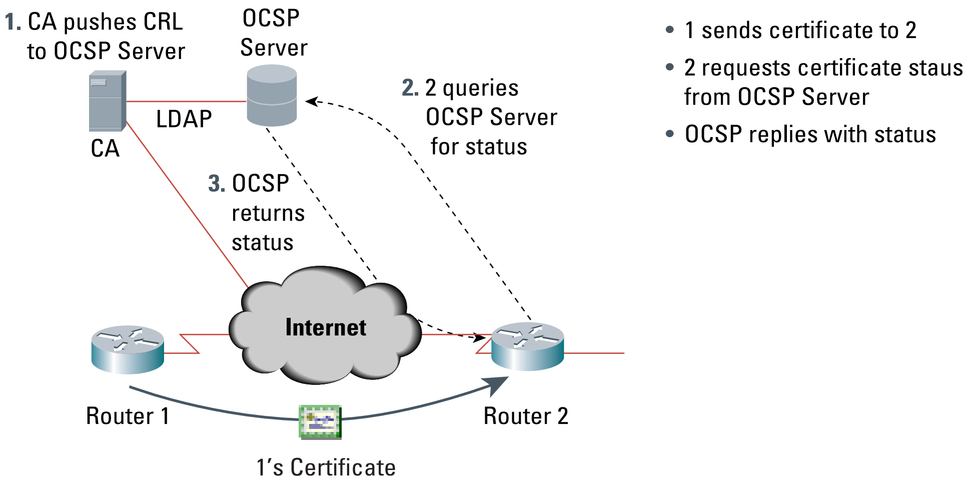
These are circumstances where CRL is an inadequate mechanism for cert revocation notification. In cases where CRLs are inappropriate for checking certificate status OCSP offers a better choice.

ONLINE CERTIFICATE STATUS PROTOCOL

OCSP addresses are some of the shortcomings of CRLs. They offer a real-time mechanism for certificate status checking. An end host can query the OCSP server when a cert is presented to find out if the certificate has been revoked. This resolves many of the issues that arise from the use of CRLs, but some other problems may appear from the use of OCSP.

Some OCSP servers still use the CRL published by a Certification Authority to advise clients on the revocation status of a digital certificate, whereas other OCSP servers integrate tightly enough with the PKI to be able to query the certificate database directly for certificate revocation status. When crypto peers need to check the revocation status of certificates they transmit a query to the OCSP server with the serial number of the certificate in question. The OCSP server examines its copy or copies of the CRL to determine if the Certification Authority has listed the certificate as being revoked and replies with a message to the crypto peer that the certificate's status is "revoked", "good", or "unknown". This dialogue between the crypto peer and the OCSP server will consume less bandwidth than all, but the smallest of CRL downloads. It also consumes no memory on the crypto peer, as it will not have to cache the CRLs. In cases where an OCSP server relies on the CRL, the Certification Authority must only publish the CRL for the OCSP server's use. This will allow CRL to be updated on a more frequent interval and to offer a more "real-time" certificate revocation status, without consuming large quantities of network bandwidth with frequent, large CRL downloads, to all the cryptographic peers in a network. If the OCSP server integrates directly with the PKI to have immediate access to certificate revocation information, cryptographic peers will receive an immediate response to certificate revocation status any time they query the OCSP server.

Figure 2
Cert Validation with OCSP


1. CA pushes CRL to OCSP Server
OCSP Server
2. 2 queries OCSP Server for status
LDAP
CA
3. OCSP returns status
Internet
Router 1
Router 2
1's Certificate
• 1 sends certificate to 2
• 2 requests certificate staus from OCSP Server
• OCSP replies with status

Cisco IOS Software Release 12.3(2) T is the first release offering support for certificate revocation checking using OCSP.

CONFIGURING CISCO IOS CERTIFICATE STATUS CHECKING

Cisco IOS Certificate Revocation checking configuration has been changed with the introduction of additional options and new functionality; therefore, it is understood better if broken down into the major changes of the configuration. This document does not cover concepts related to PKI and AAA features that could be used for basic identity checking and authorization.

Basic support for certificate revocation checking by CRL is available in all Cisco IOS Software releases since digital certificate support was added to Cisco IOS Software. These images can retrieve a CRL from Hypertext Transfer Protocol (HTTP) or Lightweight Directory Access Protocol (LDAP), with mandatory revocation checking being the default behavior. LDAP CRL retrieval requires the "crl query" command to indicate the hostname or IP address of the LDAP server. Then LDAP schema information within the certificate would point to the location of the CRL within the directory. HTTP revocation checks are a little simpler because the HTTP Certificate Distribution Point is located within the certificate pointing directly to the CRL. When mandatory certificate checking is not needed, "crl optional" configures the router to check the CRL only if it has already been downloaded to the cache as a result of manual loading. The router would not download the CRL from the CDP if CRL is not present. The router accepts the certificate in three cases:

- If it came from a trusted issuer
- If it is presented within its validity period
- If any other necessary checks succeeded

After Cisco IOS Software Releases 12.2(13)T and 12.3 the option of configuring "crl best-effort", which will cause the router to download the CRL if it is available, was added to all releases. When the CRL is not available, the router will accept the certificate if the certificate's other relevant parameters pass verification.

Cisco IOS Software Release 12.3(2)T added support for OCSP, so the command-line configuration was changed substantially to offer the capability of configuring multiple revocation checking mechanisms. If a PKI uses OCSP for revocation checking, the OCSP url will be contained in the PKI's certificates. If the AAA revocation-checking location is not included in the certificates, the OCSP server's url must be configured with the "ocsp url" statement.

Cisco IOS Software Release 12.3(2)T also deprecated the "crl optional" and "crl best-effort", replacing them with the "revocation-check" command. A trust point's "revocation-check" configuration defines the order for consulting the various revocation mechanisms. A maximum of three options: "OCSP", "CRL", and "none" can be configured in preferential order. Configuration of "revocation-check ocsp none" or "revocation-check crl none" offers similar functionality to the previous "crl best-effort" command. In case the revocation check via CRL or OCSP times out, the router will accept the certificate if it has been presented during its validity period and it was issued by a trusted Certification Authority. "Revocation-check none" offers the similar functionality to "crl optional", in which the CRL is not checked unless it has been manually loaded on a router.

Cisco IOS Software Release 12.3(7)T added the capability to query multiple Certificate Distribution Points. Previous Cisco IOS Software releases queried only one CDP, regardless of the number of CDPs listed in a certificate. A capability to override the embedded CDPs with a configured CDP url was added in the Cisco IOS Software Release 12.3(7)T as well.

Please consult feature documentation links in the further references section of this document for specific configuration information.

SUMMARY

Significant enhancements have been implemented in Cisco IOS Software to allow greater flexibility in certificate revocation status checking. PKI is employed more frequently in business networks now. As demand grows for greater security, Cisco IOS Software answers customer requirements for a secure, deployable network solution to safeguard valuable data.

FURTHER REFERENCES

- Cisco IOS Software Release12.2T Trustpoint CRL Checking Configuration:

  http://www/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087ca7.html#1043976
- Cisco IOS Software Release 12.3(2)T Trustpoint CRL and OCSP Configuration:

  http://www/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a755b.html
- Cisco IOS Software Release 12.3(7)T Query Multiple Servers During Certificate Revocation Check:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtcertrc.htm
- Cisco IOS Software Release 12.3 PKI Integration with AAA Server:

  http://www/en/US/products/sw/iosswrel/ps5187/products_feature_guide09186a00801b0692.html

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe