Defending Against Compromised Certificates

A digital certificate is a signed, trusted document issued to a company or individual by a trusted certificate authority (CA). Digital certificates are commonly used by web servers to demonstrate their authenticity to web browsers. Trustworthiness in a digital certificate depends on both the confidentiality of the private key for the particular certificate, as well as confidence that the CA who issued the certificate would issue it to only authentic parties. When that trust is broken, it becomes necessary to revoke trust in a certificate or in a certificate authority.

This guidance provides IT personnel with actionable information to defend against compromised CA and web site certificates, which could permit a malicious web server to impersonate the genuine one. Each operating system (OS) and browser may use different mechanisms to check and revoke trust in a certificate. Some use a Certificate Revocation List (CRL), while others use the Online Certificate Status Protocol (OCSP). Still others rely entirely on the issuance of software updates, whose prompt application remains fundamentally important. Variety also exists in how browsers handle certificate validation. Some query the OS certificate store, while others use their own certificate store and thus must be configured separately. Finally, note that some sites may become inaccessible when enforcing strict revocation checking.

Microsoft Windows

Windows Vista and later automatically check Microsoft's Certificate Trust List (CTL) to validate root certificate authorities without any user interaction. However, a compromised certificate could be locally cached for up to 7 days. After Microsoft has updated the CTL, the local certificate cache can be updated immediately with the command:

certutil.exe -urlcache * delete

Windows XP requires software updates in order to revoke trust in compromised certificates. While waiting for updates to be issued, an administrator can manually blacklist a compromised certificate by adding it to the Untrusted Certificates store as follows:

1. Open the **Certificates** management snap-in (certmgr.msc).
2. Find the compromised certificate by name or thumbprint.
3. Right-click on the certificate and select **All Tasks > Export**.
4. Right-click the selected certificate again and select **Delete**.
5. Navigate to the **Untrusted Certificates** store.
6. Right click on the store name and select **Import**.
7. Select the previously exported certificate and complete the process.

The manual blacklisting process and mechanism works for any type of certificate in the store and not just CA certificates. If the certificate to be blacklisted isn't already in the store, then an administrator must install the patch containing it when it becomes available.

The CRL cache should also be cleared by running **certutil.exe** as previously noted, and then rebooting. The **certutil.exe** program for Windows XP/Windows Server 2003 is available in the Administration Tools Pack[1,2].

Group Policy can be used to deploy the untrusted certificate to an enterprise. To do so:

1. Open a Group Policy Object (GPO) and navigate to:

   Computer Configuration/Windows Settings/Security Settings/Public Key Policies
2. Use the same steps previously mentioned to export and import the certificate.

The change will be deployed to the enterprise through the standard Group Policy update mechanism.

Mac OS X

Keychain Access can be used to enable CRL and OCSP checking:

1. In the Finder, select **Go > Utilities > Keychain Access**.
2. In the Keychain Access menu select **Preferences**.
3. Select the **Certificates** tab. Set **OCSP** and **CRL** to **Best attempt** and leave **Priority** set to **OCSP**.
4. To enforce strict revocation checking, set **OCSP** and **CRL** to **Require if certificate indicates**.

Strict revocation checking may create issues with Mac App Store updates, and some programs may not function as expected.

For Mac OS X 10.7.3 and later, Keychain Access can also be used to manually blacklist a CA certificate:

1. Find the certificate and right-click on it to select **Get Info**.
2. Expand the **Trust** section, and set **When using this certificate** to **Never Trust**.

A compromised CA certificate can also be manually deleted from the system keychain as follows:

1. Find the compromised certificate in the following output:

   $ sudo security find-certificate -a -Z /System/Library/Keychains/SystemRootCertificates.keychain
2. Copy the value for the **SHA1 Hash** field.
3. Execute the following command, using this hash value to delete the certificate:

   $ sudo security delete-certificate -Z *hashvalue* /System/Library/Keychains/SystemRootCertificates.keychain

Red Hat Enterprise Linux

Patch the system by running **yum update** to ensure that the latest trusted certificate list is installed. RHEL 5 includes this list as part of the openssl package; in RHEL 6 it is part of the ca-certificates package. After applying the update, view the certificate files located at:

/etc/pki/tls/certs/ca-bundle.crt
/etc/pki/tls/certs/ca-bundle.trust.crt

If the untrusted certificate remains in those files, then it is still trusted and a text editor can be used to delete the certificate.

BlackBerry

BlackBerry devices can be configured as follows:

1. From the home screen, navigate to **Options > Security > Advanced Security > Certificates**.
2. Select the certificate.
3. Press the **Menu** key, and then select **Delete**.

Android

Android 4.0 and later can be configured as follows:

1. Open the Settings application.
2. Select **Security > Trusted Credentials**.
3. Select the certificate.
4. Scroll to the bottom, and select **Disable > OK**.

Apple iOS

Ensure the device is running the latest iOS version.

Microsoft Internet Explorer

Internet Explorer uses the OS certificate store. Consider using registry[3] or GPO[4] settings to enable strict revocation checking.

Mozilla Firefox

Mozilla maintains an internal database of trusted root CAs. If a CA becomes compromised and an appropriate CRL URL can be found, then it can be revoked as follows:

1. Navigate to the **Options** or **Preferences** menu.
2. Select the **Advanced** icon.
3. On the **Encryption** tab select **Revocation Lists > Import** to add the CRL URL.

Alternatively, to manually blacklist a CA certificate:

1. Click the **View Certificates** button.
2. Select the **Authorities** tab.
3. Select the CA certificate and click the **Delete or Distrust** button. The **Edit Trust** button can also be used to unselect all the options.

Firefox's Certificate Manager can be used to manually blacklist other types of certificates but this may not work as expected[5].

The about:config interface can also be used to enable OCSP and strict revocation checking by setting **security.OCSP.enabled** to **1** and **security.OCSP.require** to **true**.

Google Chrome

Chrome uses the OS certificate store. Google also maintains their own certificate revocation database (CRLSet) that is automatically updated. Ensure automatic updates are enabled or update to the newest version when available.

Apple Safari

Safari uses the OS certificate store on both Mac OS X and Windows.

References

[1] Windows Server 2003 Service Pack 2 Administration Tools Pack for x86. http://www.microsoft.com/download/en/details.aspx?id=6315
[2] Windows Server 2003 Service Pack 2 Administration Tools Pack for x64. http://www.microsoft.com/download/en/details.aspx?id=19538
[3] Internet Explorer Feature Controls. Security Certificate Revocation Failure. http://msdn.microsoft.com/en-us/library/ee330735%28v=vs.85%29.aspx#cert_rev_fail
[4] Internet Explorer Feature Control Settings in Group Policy. http://technet.microsoft.com/en-us/library/cc775996%28v=ws.10%29.aspx
[5] Certificate Manager UI latches on trusted state. https://bugzilla.mozilla.org/show_bug.cgi?id=696597

Product of the
Network Components
and Applications Division

NSA Information Assurance
9800 Savage Rd.
Ft. Meade, MD 20755-6704
410-854-6632 DSN: 244-6632