CA/Browser Forum

Internal Server Names and IP Address Requirements for SSL:

Guidance on the Deprecation of Internal Server Names and Reserved IP Addresses provided by the CA/Browser Forum

June 2012, Version 1.0

Introduction

On November 22, 2011, the CA/Browser Forum adopted "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Version 1.0" (hereafter referred to as the "BR 1.0") to take effect on July 1, 2012[1]. As part of these requirements, Section 9.2.1 indicates:

> As of the Effective Date of these Requirements, prior to the issuance of a Certificate with a Subject Alternative Name (SAN) extension or Subject Common Name field containing a Reserved IP Address or Internal Server Name, the CA SHALL notify the Applicant that the use of such Certificates has been deprecated by the CA / Browser Forum and that the practice will be eliminated by October 2016.
>
> Also as of the Effective Date, the CA SHALL NOT issue a certificate with an Expiry Date later than 1 November 2015 with a SAN or Subject Common Name field containing a Reserved IP Address or Internal Server Name.
>
> Effective 1 October 2016, CAs SHALL revoke all unexpired Certificates whose SAN or Subject Common Name field contains a Reserved IP Address or Internal Server Name.

This document explains this change and the reasons behind it, and suggests alternatives for affected subscribers.

Definitions

For the purposes of certificate issuance pursuant to the BR 1.0, the following definitions are used:

- **Domain Name**: The label assigned to a node in the Domain Name System.
- **Fully-Qualified Domain Name (FQDN)**: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.
- **Internal Server Name**: A Server Name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.
- **Reserved IP Address**: An IPv4 or IPv6 address that the IANA has marked as reserved: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

  http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

Background

Certification Authorities enable the establishment of trust on the Internet by issuing certificates that bind cryptographic public key material to verified identities. For this document, we are concerned only with certificates that identify computers acting as servers offering one or more of a variety of protocols (most commonly HTTP for Web traffic, but also SMTP, POP, IMAP, FTP, XMPP, RDP and others) over SSL/TLS.

A server might be reachable by a variety of names and addresses. A server connected to the public Internet will typically have a name in the Internet Domain Name System (DNS) that allows its address to be resolved by any other system on the Internet. An example Domain Name would be "server123.cabforum.org". Such a system will have a publicly routable IP address, either or both IPv4 or IPv6.

[1] http://www.cabforum.org

Servers might have additional names and addresses which are only valid in the context of a local network instead of across the entire Internet. These might include names resolvable through NetBIOS, Link-Local Multicast Name Resolution (e.g. on a Windows PC), multicast DNS (e.g. through Apple's Bonjour protocol), or other protocols. Continuing our example above, the same server might also be reachable to other computers on its local network by the names "www" or "www.local".

Local names might resolve to a publicly routable IP address, or they might resolve to addresses that are only valid on a local network. The "192.168.*.*" IP address space used by many home Internet Gateway Devices is perhaps the best known set of private network addresses, but there are many ranges of IPv4 and IPv6 address space reserved for private or other usages.

The key distinction between the two types of names and addresses is uniqueness. A fully qualified domain name like "www.cabforum.org" represents a unique and distinct identity on the Internet (even if multiple servers respond to that name, the control of that name belongs to a single entity). In contrast, at any given time, there may be thousands of systems on public and private networks that could respond to the unqualified name "www". Only one logical host on the Internet has the IP address "97.74.42.11", while there are tens of thousands of home Internet gateways that have the address "192.168.0.1".

The purpose of certificates issued by publicly trusted Certification Authorities is to provide trust in names across the scope of the entire Internet. Non-unique names, by their very nature, cannot be attested to outside their local context, and such certificates can be dangerously misused, so, as of the effective date of the BR 1.0, issuance of certificates for non-unique names and addresses, such as "www", "www.local", or "192.168.0.1" is deprecated.

Current Usage of Deprecated Certificates

As a convenience for users, many servers in corporate networks are reachable by local names such as "mail", "wiki" or "hr". Most publicly trusted certificates for non-unique names are deployed in the context of local networks to enable trust in these local names without the additional cost of provisioning a new trust root to clients. This may be especially desirable for networks lacking centralized policy deployment and management tools, such as "Bring Your Own Device" environments. Unfortunately, even these "legitimate" deployments come with hidden dangers, and such certificates are frequently misused. A survey by the EFF's SSL Observatory in 2011 found over 37,000 certificates with unqualified names on servers facing the public Internet.[2]

Dangers of Publicly Trusted Certificates for Non-Unique Identifiers

Consider a corporation that has deployed an internal mail system at the address "https://mail/". The system is not reachable from the public Internet – only on the local corporate network or over the VPN. Is such a system secure?

If certificates for the name "mail" are available from publicly trusted Certification Authorities, it cannot be. The name mail is not unique, so anyone can potentially obtain a certificate that validates for "https://mail/". If an attacker brings such a certificate into the corporate network, it can be used in combination with local name spoofing to perfectly impersonate the real corporate mail server and steal users' credentials and other confidential information. The attacker might not even need to be on the corporate network to mount a successful attack. If a user connects their corporate laptop to a public WiFi network, the mail client might automatically attempt to connect to "https://mail/" before a VPN connection is established. If an attacker has anticipated this, again, a perfect impersonation can be made and the user's credentials stolen.

[2] https://www.eff.org/deeplinks/2011/04/unqualified-names-ssl-observatory

In thinking about this attack, it is important to note that it does not depend on whether the corporation deploying the mail server purchased the certificate for "https://mail/" from a publicly-trusted CA, or issued it from a private, enterprise-scope CA. If the certificate used by an attacker chains to a CA in the browser or operating system trust store, it will be accepted by all clients -creating a vulnerability even for users of private PKIs.

The dangers these certificates pose extend even to systems that use certificates with fully qualified domain names, because the unqualified names may still be valid in other authentication contexts. In Microsoft Windows Active Directory environments, Integrated Windows Authentication (IWA) over HTTP is a common method of authenticating to web servers in the corporate intranet. IWA uses the host name of a server to look up a target identity in Active Directory and send appropriate credentials – but systems in Active Directory are always registered under both their short, NetBIOS name, and the fully qualified domain name. This means that an attacker presenting a certificate for "mail" can cause Internet Explorer to emit credentials that are valid for "mail.corporate.example.com" – and do so silently and automatically, because unqualified host names are heuristically placed in the Local Intranet Zone.

If cryptographic channel binding technologies such as Extended Protection for Authentication[3] are not configured, this can allow an attacker with an unqualified name certificate to easily gain access to intranet resources with the full privileges of any user on the same network – even if those resources correctly employ only fully-qualified certificates.

Because non-unique names cannot be meaningfully validated in the context of the public Internet, and because of the potential for malicious misuse of such certificates, the CA/Browser Forum has decided to cease issuing them after a grace period to allow affected users to transition away from them.

Recommended Alternatives

Use a fully-qualified domain name certificate and DNS domain suffix search.

Many sites reachable with an unqualified name may still be reachable and properly identified by FQDN because DNS client software uses a process called suffix search, in which it appends configured suffixes to complete unqualified names. This typically happens automatically for the domain a system is part of. So, for example, a system named "client.example.com" will use "example.com" as a search suffix. When attempting to resolve the name "server", it will automatically try "server.example.com" in its DNS search. For more information on configuring the DNS suffix search list on Microsoft Windows, including for disjoint namespaces, see: http://technet.microsoft.com/en-us/library/bb847901.aspx.

Since searches with DNS suffix completion are typically attempted after local resolution fails, it may help to disable legacy NetBIOS name resolution on the client and turn off WINS name servers to force the use of DNS for name resolution. NetBIOS can be disabled using DHCP as detailed in the following KB article: http://support.microsoft.com/kb/313314.

Modern Microsoft Windows networks can run exclusively using DNS name resolution, but you must do careful testing before you turn off NetBIOS over TCP/IP in any production environment. Programs and services that depend on NetBIOS no longer work after you turn off NetBT services, so it is important that you verify that your clients and programs no longer require NetBIOS support before you turn it off. Computers prior to Windows 2000, such as Windows NT and Windows 95 will not be able to function in a network with NetBIOS disabled.

If you are using Outlook 2007 with Autodiscovery, see the FAQ for more information on using FQDNs instead of NetBIOS names to identify your Exchange Servers.

[3] http://support.microsoft.com/kb/968389

Use an enterprise/private CA to issue and trust certificates for non-unique names

The correct way to issue certificates for local names is to use a local Certificate Authority. This can be done manually, using free tools such as OpenSSL[4] (many online tutorials are available), EJBCA[5], CACert[6] or others. On a Microsoft Windows Active Directory Network, a Windows Server can be configured in the Active Directory Certificate Services role to act as an enterprise CA, and the Active Directory Group Policy mechanisms can be used to automatically provision the certificate to domain joined clients and even automatically enroll servers for certificates.[7]

If you do not want to create and manage your own enterprise PKI, your current CA vendor may be able to provide you with a managed private PKI, issuing new certificates for you, managing the issuance infrastructure and assisting you in configuring client systems to trust the new private CA.

Manually provision trust in self-signed certificates

For smaller, unmanaged networks, self-signed certificates can be trusted directly. Many server software packages include tools or the option to generate a self-signed certificate which can be added to the trust store as one would a CA cert, discussed above.

Some applications, most commonly federation products such as Microsoft ADFS and other SAML-based Single Sign On solutions, always use directly provisioned trust, and do not require a certificate that chains to a trusted root to operate correctly.

Many Web Services also have the ability to verify certificates using “peer trust”, where certificates can be explicitly trusted by placing them in a special store or directly in the service configuration (as opposed to “chain trust”, where certificates must chain up to a standard trusted root). More information about using peer trust for web services on Windows can be found on MSDN.[8]

Use IPSec

In some cases, certificates with non-unique names are used to help meet regulatory or audit requirements for network traffic containing sensitive data to always be encrypted. Unfortunately, while encryption without strong authentication (which publicly trusted, unqualified certificates cannot provide) may earn a checkbox from a naïve auditor, it provides no real protection against the threats these requirements are ultimately meant to defend against. In many cases IPSec may be a better option than SSL/TLS for meeting these requirements. IPSec protects all traffic between associated hosts and is application-independent. Network management software such as Microsoft Windows Active Directory may provide tools to automate the provisioning of IPSec Security Associations, or trust can be provisioned manually using self-signed certificates or pre-shared keys. Contact your operating system vendor for more information on using IPSec.

[4] http://www.openssl.org/

[5] http://www.ejbca.org/

[6] http://www.cacert.org/

[7] http://technet.microsoft.com/en-us/library/cc772393(v=ws.10).aspx

[8] http://msdn.microsoft.com/en-us/library/ms731899.aspx

FAQ:

These certificates are only on my internal network / only used for encrypting data in transit. What's the danger?

If there is really no danger on a network, why use SSL/TLS? The reality is that few networks are truly safe, and if it is necessary to deploy SSL/TLS, it is necessary to deploy a certificate that meaningfully identifies the host and is not easily impersonated by an attacker – otherwise the encryption is meaningless. Even if you are willing to accept the risk of these certificates for your configuration, the risk they present to the broader ecosystem means their issuance must be discontinued.

We only use these certificates on test servers to avoid browser warnings.

Even if your usage doesn't depend on the security of these certificates, their existence poses a danger to many other systems, so they are being deprecated. Use a private CA or explicitly trusted certificates, as described above, to enable test scenarios. Contact your CA vendor for information on managed private CA services.

We use the .local domain for our internal network.

DNS suffix completion will not be appropriate for this configuration, but you can still use a private CA to issue certificates for names ending in .local. Contact your CA vendor for information on managed private CA services.

I get certificate errors with Microsoft Exchange and Outlook 2007 Autodiscovery when I use an FQDN certificate.

By default, the registered endpoint URIs for Exchange Autodiscovery use the server's NetBIOS name, not its FQDN. The following KB article describes how to update that configuration to use the server's full DNS name: http://support.microsoft.com/kb/940726

We are using Microsoft Active Directory Federation Services (ADFS) and it requires a certificate from a trusted root CA.

ADFS uses several certificates in its operations. Token Signing and Token Decrypting certificates are used to establish the base trust relationship of a federation. These certificates are always explicitly trusted by the two ADFS servers, and managed with the ADFS snap-in. Because of this, they do not need to be issued by a trusted CA or provisioned to any client machines.

The other type of certificate used is the Service Communication Certificate. This is the same certificate used for IIS to secure SSL communications with a client. Web servers that are ADFS-enabled, such as SharePoint, also need certificates trusted by all clients to enable HTTPS. Because ADFS is used to enable cross-organizational trust, often across the Internet, it is very important that the Service Communication Certificate and HTTPS certificates for ADFS-enabled web servers always use fully-qualified domain names and certificates issued for the same. Use of a publicly-issued, unqualified certificate allows these servers to be easily impersonated by anyone else with a certificate for the same name, possibly resulting in unauthorized access.

For additional information, see: http://technet.microsoft.com/enus/library/dd807040(v=ws.10).aspx