White Paper

Private-Key Duplication

The safe use of wildcard and multi-server certificates

ENTRUST

SECURING A WORLD IN MOTION

Table of Contents

Background

Historically, an authentication key-pair was created by its authentication subject; the public key was exported to be certified by an authority, and the private key never existed outside the subject's crypto-module in unprotected form. In this way, each authentication subject had a unique name and a (statistically) unique key-pair. What this approach lacked in flexibility it made up for in assurance.

Multi-server certificates

As deployments of public-key technology grew in sophistication, the need for a subject to assert its identity on more than one machine emerged. This need was accommodated by exporting the key-pair from one machine and importing it into one or more other machines.

The procedure necessarily entailed a reduction in assurance, because the private key corresponding to a certified public key now existed in more than one location and it (potentially) passed through several people's hands in the course of its lifetime. At the same time, because of the broader range of resources that it protected, the value of that one private key became considerably greater.

The possible existence of a certificate corresponding to a misplaced private key elevated the risk of an impersonation attack; greater vulnerability, greater impact – much greater risk. So, additional procedural safeguards were commonly put in place to reestablish the original level of assurance. These procedures were designed to mitigate the risk of a private key falling into the hands of a disgruntled employee or criminal, or of copies existing that were impossible to trace.

Wildcard certificates

The latest developments in TLS/SSL certificate technology have mitigated one of the major risks associated with wildcard certificates in that it is now possible to obtain a unique private key for each server utilizing the wildcard certificate while consuming only one certificate license.

In a system, such as the web, with a hierarchical namespace, a practice called “wildcard” certificates emerged. Instead of assigning a unique name to an authentication subject at a leaf node in the namespace, a key was certified for a higher-level domain containing an unconstrained number of sub-domains and leaf nodes, and a wildcard character (the asterisk) was used to stand for all possible descending branches in the namespace. For instance, *.example.com would match www.example.com, app.example.com, test.example.com, etc.

A wildcard certificate could be obtained before decisions about the structure of the namespace were finalized, and the chosen structure could then be modified after certificates were issued, with no management impact on those certificates.

Wildcard certificates are attractive from the point of view of the flexibility they offer, but historically, there have been some known vulnerabilities related to what makes them so flexible: the fact that wildcard certificates can be installed on multiple servers for multiple subdomains of a common root domain.

Thus, in the wrong hands, a wildcard certificate could be used with either a fictitious or fraudulent sub-domain name.

« At the time, wildcard certificates were attractive from the point of view of the flexibility they offered. But, in the wrong hands, they can be used with either a fictitious or a fraudulent sub-domain name. »

Unlimited certificate duplication

While wildcard certificates present certain security vulnerabilities, the flexibility offered by this certificate type can make wildcard certificates an attractive security solution. The advent of unlimited certificate duplication, where users of wildcard certificates can duplicate a wildcard certificate with its own unique key using a single certificate license, adds some resilience to this certificate type.

Specifically, here are two scenarios where wildcard certificate features make this certificate type seem like the best solution.

Load balancing

In an environment where there are multiple servers being utilized to optimize resource use, it means having to either buy a unique certificate for each unique server so that each server maintains its own private key or copy a wildcard certificate (and its corresponding private key) from one identical-purpose server to another (a practice that introduces security risks, as copying the private key will render the security of the entire environment as strong as the least protected key).

Thus, unlimited certificate duplication allows for certificate keys to be deployed based on purpose, and not by load.

Dual key support

An environment that supports both RSA and ECC keys would normally require one certificate for each key type. For a web server that supports ECC-RSA dual key implementation, wildcard certificates offer the ability to duplicate a single wildcard license, each with unique keys, allowing for multiple certificates of the same purpose to be deployed without having to purchase unique certificates for both key types.

Attack vectors

Wildcard certificates are attractive from the point of view of the flexibility they offered. But, in the wrong hands, they can be used with either a fictitious or a fraudulent subdomain name.

Two main attacks are facilitated by multi-server certificates.

Eavesdrop attack

The first is an eavesdrop attack, in which an insider who has the ability to intercept user traffic and has access to the private key corresponding to the multi-server certificate can decrypt sensitive traffic, thereby compromising sensitive personal or corporate information.

Impersonation attack

In the second attack, the attacker can use the private key to impersonate a genuine resource in the domain. The attacker must redirect user traffic to its server using methods such as redirecting IP traffic, poisoning the user's DNS cache or hosts.txt file, or through a social-engineering attack such as a phishing email.

In this type of attack, the victim is lured to a fraudulent resource in the certified domain through phishing. Conventional certificates detect this attack, because the user's browser checks that the private key is hosted on a server whose name matches the one displayed in the browser's address window. In the case of a conventional certificate, the check would fail and a warning would be issued. But, in the case of a wildcard certificate, the check would pass.

A related attack that doesn't depend on DNS poisoning involves an unscrupulous subscriber who obtains a wildcard certificate for a domain that he genuinely owns and then creates a misleading subdomain.

Now, to complete the fraud, the victim only has to be lured to the misleading subdomain by means of a phishing email. In order to eliminate this attack, diligent certification authorities take steps to ensure that wildcard certificates are only issued to subscribers that can be properly identified and held accountable, and that (in the unlikely event that a fraud should occur) the technical and contractual infrastructure exists to effectively revoke an affected certificate.

In the case of a conventional certificate, the diligent certification authority gets an opportunity to ensure that nothing misleading appears in any subject subdomain name.

The benefits of unlimited certificate duplication

Industry experts generally view wildcard certificates with suspicion. However, the advent of unlimited certificate duplication helps manage the risk associated to attacks by allowing for any compromised certificate to be revoked and replaced quickly with a new private key. While this feature recognizes the use of wildcard or multi-server certificates as an efficiency and cost-saving measure, it does not completely eliminate the threat of attack.

Supplemental safeguards

If a subscriber discovers or suspects that the private key corresponding to a multi-server or wildcard certificate has been misused or may be in the future, then it will be necessary to replace the private key and certificate on the affected resources and revoke the affected certificate.

Unlimited certificate duplication makes certificate replacement much easier. Because any network compromise is a serious concern, supplemental safeguards are commonly employed.

Conclusion

The use of multi-server certificates increases the probability of eavesdrop and impersonation attacks – whether perpetrated through redirection of IP traffic, DNS cache poisoning, or phishing. Wildcards also enable a new type of impersonation attack, because they reduce the specificity of the browser's domain-name matching check. Unlimited certificate duplication helps manage the consequences of these attacks by multiplying the number of private keys associated to a single wildcard certificate, thus making it easier to replace a compromised certificate and key.

It is important that all TLS/SSL certificates be properly managed – especially multi-server and wildcard certificates. Many services are provided by certification authorities that help to ensure certificates are properly monitored for security, as well as provide expertise for safeguarding data.

Since the consequences of a compromise can be more severe than they would be for a conventional certificate, supplemental safeguards should be employed. In the absence of these safeguards, we do not recommend the use of either multi-server or wildcard certificates, due to both the security risks involved and the expanded scope of management issues in the wake of a compromise.

For more information

888.690.2424
+1 952 933 1223
sales@entrust.com
entrust.com

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223