



Private-Key Duplication

The safe use of wildcard and multi-server certificates

Get this
White Paper





Contents

- Background 3
- Multi-Server Certificates 3
- Wildcard Certificates..... 4
- Attack Vectors 5
- Supplemental Safeguards 6
- Conclusion..... 6
- Entrust & You 7



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.

“

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.

”



Wildcard Certificates

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, *.domain.com would match www.domain.com, app.domain.com, test.domain.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.

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.

In addition, a single wildcard certificate and its corresponding private key could be used on multiple servers, exactly as described above.

No benefit, it seems, comes without a cost. For subscribers who place any reliance at all on their certificate approval procedure to control the authorization of new servers and new domains, a wildcard certificate will effectively bypass those controls.

In the Wild

*By deploying a wildcard SSL certificate, organizations could use a wildcard character to stand for all possible branches in a domain name. For example, *.domain.com would match www.domain.com, app.domain.com, test.domain.com, etc.*

Attack Vectors

Two main attacks are facilitated by multi-server certificates. The first one 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.

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.

Wildcard certificates introduce a new style of impersonation attack. In this 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.

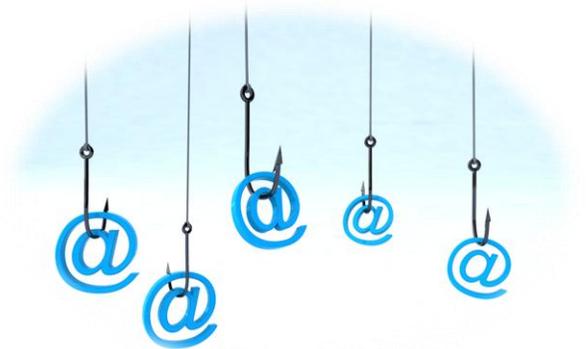
In the case of a conventional certificate, the check would fail and a warning issued. But, in the case of a wildcard certificate, the check would pass.

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 sub-domain.

Now, to complete the fraud, the victim only has to be lured to the misleading sub-domain 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. They also ensure 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 sub-domain name.

Industry experts generally view wildcard certificates with suspicion — a main reason their use is banned in extended validation (EV) certificates.





Supplemental Safeguards

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

Depending on the number and geographical distribution of the servers, this may be an onerous undertaking; much more so than when a single resource with a unique key-pair becomes compromised. For this reason, supplemental safeguards are commonly employed to ensure that this situation does not arise.

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.

Nevertheless, properly managed, multi-server and wildcard certificates can provide increased flexibility. 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.



Entrust & You

More than ever, Entrust understands your organization's security pain points. Whether it's the protection of information, securing online customers, regulatory compliance or large-scale government projects, Entrust provides identity-based security solutions that are not only proven in real-world environments, but cost-effective in today's uncertain economic climate.

A trusted provider of identity-based security solutions, Entrust empowers governments, enterprises and financial institutions in more than 5,000 organizations spanning 85 countries. Entrust's award-winning software authentication platforms manage today's most secure identity credentials, addressing customer pain points for cloud and mobile security, physical and logical access, citizen eID initiatives, certificate management and SSL.

For more information about Entrust products and services, call **888-690-2424**, email entrust@entrust.com or visit entrust.com.

Company Facts

Website: www.entrust.com
Employees: 359
Customers: 5,000
Offices: 10 Globally

Headquarters

Three Lincoln Centre
5430 LBJ Freeway, Suite 1250
Dallas, Texas 75240

Sales

North America: 1-888-690-2424
EMEA: +44 (0) 118 953 3000
Email: entrust@entrust.com

follow us on
 