

E-Guide

SSL Certificate Management: Common Mistakes and How to Avoid Them

Contents

SSL Certificate Management: Common Mistakes and How to Avoid Them

Errors are bound to occur when SSL certificate management is handled manually. Learn how to avoid these common mistakes.

SSL Certificate Management: Common Mistakes and How to Avoid Them

By: Rob Shapland

It can be difficult to manage all your SSL certificates if you have a large estate of Web applications. There are many critical tasks that come with enterprise SSL certificate management, and ignoring or mishandling any one of them can set the stage for a Web application exploit. In this tip, we'll look at the most common mistakes in implementing and managing SSL certificates, and how to avoid them.

For those new to SSL certificate management, the many tasks involved can be surprising. For instance, certificates need to be purchased, deployed and renewed when they've expired. This all takes time, especially when multiplied over the dozens or even hundreds of applications and domains that exist in many enterprises.

Then there is the matter of ensuring that each certificate is correct for the Web application with which it is being paired. Is it necessary to have Extended Validation certificates, which are more expensive because they are provided by and vetted through a trusted certificate authority (CA)? Or are low-assurance (but cheap) certificates appropriate, such as for nonpublic-facing Web applications?

The suite of offerings from certificate vendors is confusing. There are several different levels of validation offered, different hash types, lengths and warranties (which actually protects the end user, not the certificate owner). It can be difficult to know what type of certificate is required for a particular application.

Contents

SSL Certificate Management: Common Mistakes and How to Avoid Them

Worse still, researchers have found that more than half of companies have at one point lost a digital certificate, or there were certificates on their network whose origins could not be accounted for. This may be because a developer or other employee created a certificate without telling anyone, but the problem is that often no one knows.

Most companies manage a variety of digital certificates manually with spread sheets. This can lead to mistakes, such as lost, mismatched or mislabelled certificates. Certificates can inadvertently expire, meaning CAs no longer consider a website or Web application secure and trusted. This can be a very expensive mistake if an affected Web application is public-facing. It may lead to reputational damage for the organization, or visitors' browsers may block access to the site entirely. It's been the cause of many high-profile system outages and is often one of the last causes administrators investigate, contributing to significantly more downtime.

Another problem occurs if the CA that issued the organization's certificate is compromised, as happened to DigiNotar and Comodo in 2011, and TurkTrust at the start of this year. The certificates are then revoked by other CAs, so when a client connects to the affected server, the certificate is no longer valid. Without proper SSL certificate management on an enterprise-wide level, it's impossible to tell how many (if any) of your certificates are no longer valid.

Fortunately there are solutions to the enterprise certificate management dilemma, one of the most effective being automation. Automated tools can search a network and record all discovered certificates. Such tools can usually assign certificates to business owners and can manage automated renewal of certificates (though most do not support renewing with a different CA). The software can also check that the certificate was deployed correctly to avoid mistakenly using an old certificate. Automated tools aren't perfect, however, and do require some manual intervention, as the scanner may miss certificates stored in places it does not have access to, such as the registry in the case of keys that support Microsoft's Encrypting File System.

Contents

SSL Certificate Management: Common Mistakes and How to Avoid Them

When purchasing one of these automated tools, ensure that the software can manage certificates from all CAs. Some will only manage certificates issued from a particular CA, and it's easy to miss some of the certificates on your domain, even if you believe you only use one provider.

It is essential for sound enterprise certificate handling that certain events are planned for and managed. Procedures should be written and communicated that detail what should happen if a certificate authority is hacked, and how certificates in the organization's network should be replaced. Tracking down certificates from the compromised CA is time-consuming if it's not planned for ahead of time.

This article has demonstrated the issues associated with manual digital certificate management. If your organization is doing SSL certificate management manually, it may be time to investigate an automated alternative, even if you think you know about all your certificates. You may be in for a surprise.

About the author:

Rob Shapland is a penetration tester at First Base Technologies, where he specialises in Web application security. He has used his skills to test the websites of companies that range from large corporations to small businesses using a wide variety of Web technologies. He is a firm believer that all penetration testing should have manual techniques at their core, using automated tools to support these skills. He is also involved in network testing and social engineering.



Contents

SSL Certificate Management: Common Mistakes and How to Avoid Them

Free resources for technology professionals

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more—drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

What makes TechTarget unique?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.

Related TechTarget Websites

-  SearchMidmarketSecurity
-  SearchFinancialSecurity
-  SearchSecurityChannel
-  SearchCloudSecurity