

X.509 Certificate Management: Avoiding Downtime and Brand Damage

Published: 4 November 2011

Analyst(s): Eric Ouellet, Vic Wheatman

Organizations are often not aware of the scope or the validity status of their X.509 certificate deployments until it is too late. Organizations need to establish formalized plans and, if necessary, leverage available tools to minimize impacts.

Key Findings

- Many high-profile, externally facing and internally facing system outages are traced to unplanned X.509 certificate expiry.
- While several offerings exist to discover X.509 certificates, most organizations rely on spreadsheet-based tracking methods and manual processes to keep track of certificates, resulting in many undocumented installations and increased exposure to risks.
- Organizations with roughly 200 or more X.509 certificates in use that are using manual processes typically need one full-time equivalent (FTE) per year to discover and manage certificates within their organizations.¹
- Service outages due to unplanned certificate expiration impact service availability, SLAs, brand confidence and trust by customers, partners and other relying parties, and can lead to noncompliance with regulatory or other requirements.

Recommendations

- Organizations with roughly 200 or more documented X.509 certificates in use are high-risk candidates for unplanned expiry and having certificates that have been purchased but not deployed. They must begin a formalized discovery process immediately.
- Automated certificate discovery and renewal/management works to minimize the risk of unplanned expiry. Manual or automatic certificate management should be leveraged to attribute accountability and ownership of X.509 certificates within organizations.
- Organizations need to create an inventory of X.509 certificates and certificate issuers to minimize the impact and downtime in the event of a certificate issuer compromise, suspected

compromise or attack as seen over the past 18 months involving several certificate authorities. Furthermore, organizations need to plan for and practice what they will do in the event of a certificate authority compromise in the context of a security incident.

Analysis

Organizations are reliant on digital communications secured using X.509 certificates for their day-to-day operations. Certificates are used for user authentication, secure communications using Secure Sockets Layer (SSL), program-to-program and machine-to-machine communications, digital signature, and code signing. Many unseen internal and external services performing their daily duties are authenticated and trusted based on a relatively simple process involving the verification that an issued certificate is still active.

Expired X.509 certificates result in a number of system maladies, ranging from a simple error message on a screen to an abrupt termination of service. This can lead to abandoned e-commerce transactions or the loss of trust in a company's Web presence. Many organizations that have an unplanned certificate expiry typically focus on other systemic causes, such as hardware/software issues, long before they begin to consider an expired X.509 certificate as the source of troubles. This typically results in significant delays in identifying and resolving the root cause of a system outage.

During the past 18 months, another form of X.509 certificate-related problem has come forward in security news — that of the compromised public certificate issuing authority. Because of threatened or actual compromises at DigiNotar, Comodo and others, previously issued certificates from these public providers have had to be revoked, either individually or, at worst, en masse, with an entire certificate issuance infrastructure losing complete trustworthiness. This latter case invalidated all currently issued and active X.509 certificates from that certificate authority, and necessitated a complete reissuance of X.509 certificates from an alternate issuer. Organizations should be explicitly aware of the potential for significant impact on their operations should they be associated with such an incident. Knowing the specific provenance of each and every X.509 certificates in use within an organization is critical in ensuring the timely reissuance of certificates, thus minimizing downtime. It is also necessary to have a suitable management interface to remotely installed certificates, and to trust root certificate lists so they too can be replaced if compromised (see "Certificate Authority Breaches Impact Web Servers, Highlighting the Need for Better Controls"). Many organizations scramble to remove a trusted root when a compromise takes place. Organizations need to understand their internal process for removing a trusted certificate or root from browsers and applications. While browsers are relatively easy to fix by waiting for the browser patch with the removed/deleted/revoked root, applications typically involve more work and, thus, more planning.

One of the first steps in identifying compromised certificates is to identify ALL certificates and evaluate each relying server for certificate validity. However, many organizations do not have a good understanding of their inventory of digital certificates or where they are. They may rely on spreadsheet-based manual methods to track certificates, but the spreadsheet method is deficient in that it does not record or track anything that is not entered into it. The commercial certificate

authorities and public key infrastructure (PKI) software vendors do provide some rudimentary certificate management. For example, they may notify the original individual corporate purchaser of an imminent certificate expiry, but not be able to handle cases where that individual has changed roles or left the organization. Gartner's research also identified cases where the vendor product did not keep the customer informed of updates to its inventory or the location of issued certificates. Further, some vendors' solutions only manage their own certificates.

X.509 Certificate Management Functions

Several commercial certificate authorities, PKI and certificate management solution providers offer Certificate Management System (CMS) software that can be used to discover, identify, track, notify, and ultimately automatically renew and audit the installation of new X.509 certificates. In general, the functions of this software are:

- Discovery:
 - Discovery is a primary function of a CMS. It scans the network, systems and applications; logs all instances of X.509 certificates; and may include all or some of the following: SSL, Transport Layer Security, Secure Socket Shell (SSH), Pretty Good Privacy and others. Filters can be set to limit "noise" in discovery, but overall discovery should be able to support a deep dive understanding of where cryptographic keys are stored, their strength, the issuer, validity period and expiry date. There is a potential problem with discovery "crawlers" that may occasionally cause a target platform to malfunction. Further, some keys, such as those supporting Microsoft's Encrypting File System, are stored in the registry, meaning the discovery agent cannot access them unless the local user is logged on.
- Ownership:
 - Identify who the certificate owners are for a given certificate and the approval structure for the issuance and renewal. Billing and chargeback processes can also be associated for a certificate as part of this activity.
- Validate:
 - A CMS may eventually have a feature that regularly checks certificates against certificate revocation lists (CRLs) and Online Certificate Status Protocol (OCSP) responders to recertify trust both inside and outside the context of a live interaction between servers, or between a browser and a server. Currently, validation is a function of the client (such as a browser), but is not typically turned on for performance or other reasons. Ultimately, CRL and OCSP functionality will become a mature CMS feature.
- Renewal/provisioning:
 - Some CMSs can support the automatic renewal of a certificate within a prescribed period prior to expiry. What is important to note is that the renewal process from most certificate issuers and PKI vendors typically favor their own brands, meaning that certificates slated

for renewal will be renewed using only their own certificate authority. At this time, only Venafi supports renewal using any certificate authority (internal or external).

- Audit:
 - When a certificate is renewed, it is critically important to ensure that the new X.509 certificate itself was both installed and rendered active within the target system, otherwise the previous X.509 certificate can remain active even after a new certificate has been installed.
 - Verify the actual in-use certificates against those charged by a third party or an internal a provider list.

A limited number of certificates can be managed manually using a spreadsheet or other basic tools, but many features, such as discovery, will be missing. If this method is chosen, specific individuals or roles need to be assigned to managed certificates on groups of machines, and scheduling reminders set for certificate renewal before the installed certificates expire.

The few companies now offering CMSs that are more robust than the rudimentary capabilities of simple spreadsheet tools or those typically offered by many certificate authorities and PKI software vendors include:

- **Trustwave (Trustwave Certificate Lifecycle Manager)** — Trustwave CLM supports the discovery of X.509 certificates used for SSL and SSH can identify Microsoft certificate authority installations. It has the ability to renew certificates originally issued by any certificate authority, but will renew and replace certificates only via the certificate authority built into CLM, if using the automated solution.
- **Venafi (Venafi Director Series)** — Venafi, named a Gartner "Cool Vendor" in 2010, is a point solution provider. Venafi is the leader in X.509 certificate management for internal and external systems and applications. Unlike certificate authority certificate management solutions, Venafi supports virtually all certificate issuers natively and can renew certificates from nearly any type of certificate issuer, providing flexibility for complex heterogeneous environments composed of certificates issued by various certificate authorities. The product was formerly resold by VeriSign (now Symantec). The company has branched out into cryptographic key management for large, heterogeneous enterprise deployments and SSH key management.
- **VeriSign (Symantec) (VeriSign Certificate Intelligence Center)** — In 2Q11, VeriSign announced a certificate management offering that supports the discovery of X.509 certificates within an enterprise, and offers the ability for the automated renewal of certificates. However, while certificates originally issued by any certificate authority can be renewed, the tool only allows renewal using a VeriSign-Symantec-branded certificate authority.

Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Certificate Authority Breaches Impact Web Servers, Highlighting the Need for Better Controls"

"Evaluating SSL Certificates for E-Business"

"Six Decisions You Must Make to Prepare for a Security Incident"

"How to Build a Computer Security Incident Response Team"

"A New Hacking Tool Makes SSL Attacks Easier Than Ever"

"Cryptographic Systems: An Information Security Foundation"

"Field Research Summary: Public Key Infrastructure Deployment Experiences"

Evidence

¹ Based on several conversations with Gartner clients and vendors offering certificate management solutions, organizations constantly underestimate the work needed to track and manage certificates. When they dig in and actually start accounting the time, they are surprised it is so high. On average, clients tell us it takes three to six hours to generate a key pair on a server (depending on location and access), export the public key, get it certified with a certificate authority so it is now in an X.509 certificate format, installed, verified it is active, and then returned to live operation. Additionally, organizations report that they need to take into account the time required for the manual tracking down of assets that have certificates and the general maintenance of this list. This process itself can result in a significant effort. According to clients and CMS providers, organizations typically have several people managing different pools of certificates. Larger organizations with many hundreds or thousands of certificates have been known to have 10 or more people performing this manual activity part time for different groups of servers. When downtime occurs, the number of FTE hours can go up dramatically — obviously to address the issue.

Regional Headquarters

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

© 2011 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity" on its website, http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp.