SECURITY ALERT : Fraudulent Digital Certificates
Ferdinand Gomes
07 June, 2001.

Vulnerability : VeriSign discovers a fraud in its “Digital Certificate” issue

In March 2001, VeriSign Inc. discovered through its routine fraud-screening audit that it had inadvertently issued two VeriSign Class 3 code-signing digital certificates on 29th and 30th January 2001 to an impostor who fraudulently claimed to be an employee of Microsoft Corporation.

Microsoft Corporation immediately issued a Security Bulletin MS01-017 describing the security threat created by these software certificates falsely identified as Microsoft certificates. The bulletin stated that the vulnerability could affect all customers using Microsoft products. Microsoft also made it clear that this was not a security problem with any Microsoft product nor did it indicate that any of Microsoft’s official certificates had been compromised.

Digital certificates are critical for businesses and customers who download patches, updates and various other forms of software from the Internet, because they allow software developers to digitally sign their software for secure delivery over the Internet, on the one hand, and verify to the end-user that the software is being supplied from a particular company, such as Microsoft, on the other.

In my opinion, this vulnerability is very serious because most people would not think twice about installing software that appeared to be digitally signed by Microsoft.

How did this happen ?

Under normal circumstances, VeriSign receives an appropriate request from its customer and assigns a new certificate based on this request. Mahi de Silva, Vice President and General Manager of Applied Services at the Mountain View, California company, would not elaborate on how the company verifies requests, but said, "Due to human error we did not detect that the individual concerned misrepresented that they worked for Microsoft when, in fact, they did not."

After granting a request for new certificates, VeriSign verifies by e-mail that its customer has ordered the new codes. In this case, "it took awhile for the feedback loop from (Microsoft) to get back to us," de Silva said. Once VeriSign did hear from Microsoft, the company realized that the certificates should not have been issued.

"However, our second-stage fraud protection caught that mistake. We are not trying to shift the blame" said Mahi de Silva.

“The two certificates represent the first time VeriSign has falsely issued such codes” de Silva added, noting that the company has handed out more than 500,000 certificates. "Class 3" certificates come with up to $100,000 in liability protection for the customer - in this case, Microsoft.

So what is the Threat ?

The reason why this issue presents a security risk is because even a user who is reasonably cautious could be deceived into trusting the bogus certificates, since they appear to be from Microsoft. Once accepted, these certificates may allow an attacker to execute malicious code on the user's system.

The problem was created as the result of a failure by the certificate authority to correctly authenticate the recipient of a certificate. VeriSign has taken the appropriate action by revoking the certificates in question. However, this, in itself, is insufficient to prevent the malicious use of these certificates until a patch has been installed, because Internet Explorer does not check for such revocations automatically. Indeed, because the certificates issued by VeriSign do not contain any information regarding where to check for a revocation, Internet Explorer, or any other browser, is unable to check for revocations of these certificates. Microsoft has developed an update that will enable revocation checking and install a revocation handler that compensates for the lack of information in the certificate.

The impostor with these certificates could produce digitally signed code using the name “Microsoft Corporation”. This code could be in the form of a destructive program, ActiveX control or any other form of malware. He could then sign it using either certificate and host it on a Web site or distribute it to other Web sites.

Although programs signed using these certificates would not be able to run automatically or bypass any normal security restrictions, the warning dialogue that appears before such programs could run would claim that Microsoft had digitally signed them.

The ability to sign executable content using keys that purport to belong to Microsoft would clearly be advantageous to an attacker who wished to convince users to allow the content to run.

How do VeriSign digital certificates work ?

To understand how digital certificates work, we need to first understand cryptography and in particular, public key cryptography. Cryptography is the science of securing information by converting it between its normal, readable state (called plaintext) and one in which the data is obscured (known as ciphertext).

With all forms of cryptography, a value known as a key is used in conjunction with a procedure called a cryptoalgorithm to transform plaintext data into ciphertext. In the most familiar type of cryptography, secret-key cryptography, the ciphertext is transformed back into plaintext using the same key. However, in a second type of cryptography, public key cryptography, a different key is used to transform the ciphertext back into plaintext.

In public key cryptography, one of the keys, known as the private key, must be kept secret. The other key, known as the public key, is intended to be shared with the world. However, there must be a way for the owner of the key to tell the world who the key belongs to.

Digital certificates provide a way to do this. A digital certificate is a tamperproof piece of data that packages a public key together with information about it like who owns it, what it can be used for, when it expires, and so forth.

VeriSign, as well as other companies, issue digital certificates to prove an identity in a digital era where commerce is increasingly transacted anonymously over computer networks. They are intended to ensure computer users that Web sites and software are who and what they say they are.

Digital certificates are generated and themselves digitally signed by organisations known as certificate authorities. It is the job of a certificate authority to verify the identity of the person requesting a digital certificate before issuing one to them.

To understand this vulnerability & the associated threat, let us first try and understand how VeriSign digital certificates work.

VeriSign Code Signing Digital ID's enable software developers to digitally sign software and macros for secure delivery over the Internet.

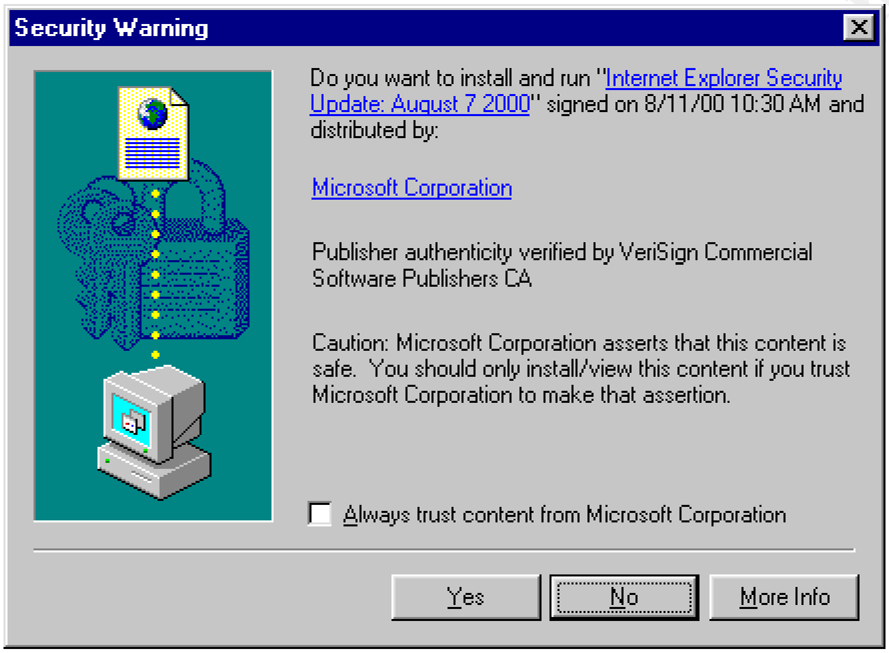
Customers who download digitally signed Active X controls, Java applets, dynamic link libraries, .cab files, .jar files, or HTML content from your site can be confident that code really comes from you and hasn't been altered or corrupted since it was created and signed.

Digital IDs serve as a virtual "shrinkwrap" for your software. Once you sign your code, if it is tampered with in any way, the digital signature will break and alert customers that the code has been altered and is not trustworthy.

What do users need to look for ?

Customers need to visually inspect the certificates cited in all warning dialogues. The two certificates in discussion here were issued on 29 and 30 January, 2001, respectively. No bona fide Microsoft certificates were issued on these dates.

The dialog box below displays what you might see when encountering digitally signed content. In the case below, a legitimate certificate from ‘Microsoft Corporation’ signed on 11 August, 2000 for the software “Internet Explorer Security Update: August 7 2000” was used to sign the content to be downloaded.



Do you want to install and run "Internet Explorer Security Update: August 7 2000" signed on 8/11/00 10:30 AM and distributed by:

Microsoft Corporation

Publisher authenticity verified by VeriSign Commercial Software Publishers CA

Caution: Microsoft Corporation asserts that this content is safe. You should only install/view this content if you trust Microsoft Corporation to make that assertion.

☐ Always trust content from Microsoft Corporation

<u>How does a user check the Digital Certificate</u> ?

1. Do not click "Yes" in the "Security Warning" dialog box. Instead, click on the link "Microsoft Corporation" to get more information about the certificate.

2. Select the "Details" tab. In the "Details" view, look for the "Serial number" field.

3. Check the serial number and validity period of the certificate to ensure that the certificate is legitimate and not fraudulent.

The details of the fraudulent certificates are:
Certificate 1: Issued by VeriSign Commercial Software Publishers CA
Validity period is 1/29/2001 to 1/30/2002
Serial number is 1B51 90F7 3724 399C 9254 CD42 4637 996A

Certificate 2:
Issued by VeriSign Commercial Software Publishers CA
Validity period is 1/30/2001 to 1/31/2002
Serial number is 750E 40FF 97F0 47ED F556 C708 4EB1 ABFD

4. If the serial number of the certificate is not one of the serial numbers listed

above, the certificate is valid and the content or code is truly from Microsoft and is safe to download. If the certificate's serial number is one of the two listed above, do NOT click "yes" in the "Security Warning" dialog box. Instead, click "No" and contact VeriSign's Emergency Response Team immediately at vest@VeriSign.com.

Is there a better SOLUTION than the manual check ?

VeriSign has “blacklisted” the certificates by placing them on a revocation list. They are listed in VeriSign’s current CRL (Certificate Revocation List). However, because VeriSign’s code-signing certificates do not specify a CDP (CRL Distribution Point), it is not possible for any browser’s CRL-checking mechanism to locate and use the VeriSign CRL. Thus, this solution does not automatically protect customers against the fraudulent codes.

Fortunately, leading antivirus vendors, **Symantec** & **Network Associates** rushed to develop definitions for their respective antivirus software that would detect and prevent the download of these certificates in real-time as well as be able to scan the complete file system for existing traces of these certificates.

Symantec also developed a special template for its host-based vulnerability assessment software, Enterprise Security Manager (ESM) that would be capable of reporting if that host had executed one or both of the fraudulent certificates.

Microsoft developed an update that will help customers ensure that content signed by the two certificates is recognized as being invalid. The update installs a CRL (Certificate Revocation List) onto the local machine. The CRL lists the two bogus certificates as having been revoked, adds new functionality via a piece of software called an installable revocation handler that causes the system to check the CRL on the machine if the CDP (CRL Distribution Point) data is missing or invalid and turns on CRL checking in Internet Explorer software publisher's certificates.

SonicWALL released a firmware patch for its Internet appliance that identifies and blocks files signed by the fraudulent digital certificates. This effectively protects Internet users from downloading or transferring files that could potentially destroy critical data or enable security breaches.

Overall, the integrated antivirus solution would seem to be a better solution than the security patch provided by Microsoft, since almost all organisations already do have anti-virus software installed.

Conclusions

This incident has highlighted to the corporate IT world how a simple human error can undo even the best of the technology-based security schemes.

The mistaken issuance of the digital certificates to an imposter, which led Microsoft to release a software update for all Windows releases dating right back to 1995, also made companies realise the importance of having both preventive and reactive processes in place to deal with such security lapses.

In addition, users and analysts said, VeriSign's goof points out some of the broader challenges associated with reliably establishing identities within public-key infrastructure (PKI) networks.

VeriSign’s honesty about its mistake should help prevent backlash against the use of digital certificates” said Wayne Pierce, Director of Service Development, Athena Security, adding that it’s hard to tell how big of a security risk the use of false certificates poses.

Still, concern about the incident may open the door for better ways of digital identity authentication and that can only help to make the community more secure.

Sources

Savage, Marcia. CRN. CMP Media Inc. “VeriSign’s Gaffe Spurs Debate”. 30 March, 2001.
URL: http://www.crn.com/sections/news/top_news.asp?ArticleID=25334

Lemos, Robert. CNET Networks, Inc. “Microsoft warns of hijacked certificates”. 22 March, 2001.
URL: http://news.cnet.com/news/0-1003-200-5222484.html?tag=tp_pr

Vijayan, Jaikumar. Computerworld Inc. “VeriSign certificate snafu highlights threat of human errors”. 30, March, 2001.
URL:
http://www.computerworld.com.sg/dev/idgcwarc.nsf/CWList/48256944002C5B8A48256A23002E297E?opendocument

Microsoft Corporation. “Microsoft Security Bulletin MS01-017”. 22 March, 2001.
URL: http://www.microsoft.com/technet/security/bulletin/ms01-017.asp?frame=true

Network Associates, Inc. “Invalid Certificate”. 24 March, 2001
URL: http://vil.nai.com/vil/dispVirus.asp?virus_k=99058

SonicWALL. “SECURITY ALERT: Fraudulent Microsoft Digital Certificates”.
URL: http://www.sonicwall.com/support/security_alert327.html

Symantec AntiVirus Research Center (SARC). Symantec Corporation. “Fraudulent

Digital Certificate”. 23 March, 2001.
URL: http://www.symantec.com/avcenter/sirc/pf/fraudulent.digital.certificate.html

VeriSign Inc. “VeriSign Security Alert Fraud Detected in
Authenticode Code Signing Certificates”. 22 March, 2001.
URL: http://www.VeriSign.com/developer/notice/authenticode/index.html

VeriSign Inc. “Q&A for Fraudulent Authenticode Certificates”. 22 March, 2001.
URL: http://www.verisign.com/developer/notice/authenticode/faq.html

VeriSign Inc. “Authenticode Warning Dialogue Box”. “What to Look For”
URL: http://www.verisign.com/developer/notice/authenticode/how.html
URL: http://www.verisign.com/developer/notice/authenticode/how2.html
URL: http://www.verisign.com/developer/notice/authenticode/how3.html