Are we safe From the DigiNotar's security incident?

Marcelo Carlomagno Carlos and Haitham S. Al-Sinani*
Information Security Group
Royal Holloway, University of London
[Marcelo.Carlos.2009, Haitham.Al-Sinani.2009]@rhul.ac.uk
http://www.isg.rhul.ac.uk

DigiNotar is a Netherlands-based certificate authority (CA) that provides Public Key Infrastructure (PKI) services. It hosts several CAs issuing digital certificates for several purposes, including default SSL certificates, Qualified Certificates and 'PKIoverheid' (Government-accredited) certificates[1]. Recently, several news stories reported a series of cyber attacks targeting DigiNotar. Internet hackers maliciously obtained unauthorised access to DigiNotar's CA servers, allowing the issuance of a series of rogue certificates. The attack is very serious since the DigiNotar's root certificate was trusted by the most widely-used web browsers and email clients, including Internet Explorer (IE), Firefox, Chrome, Safari and Opera.

By possessing such 'trusted' rogue certificates, the hackers were able to set up spoofed websites (e.g. Google Mail), without being detected as 'invalid' by users and applications. That is, if a user visits a spoofed website (which mimics a real site), the web browser would not display any security warning; indeed, to make matters worse, the browser would display indicators of a legitimate (perhaps secure) website, since the presented (fraudulently-issued) certificate would be treated as 'valid'.

As a consequence, a widely-known attack, known as 'man in the middle' (MITM), was made possible. In such an attack, a hacker sits between a user and a real website, thereby being able to eavesdrop (possibly in real-time) the user-site communication, including capturing sensitive credentials such as username-password pairs and authentication cookies. Shockingly enough,

*The supportive encouragements and helpful comments provided by Fred Piper, Kenny Paterson, Chris Mitchell and Keith Martin are gratefully acknowledged.

[1] http://www.rijksoverheid.nl/ministeries/bzk/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html

it may be the case that neither the user nor the site realises the existence of the attack.

To be successfully deployed, a MITM attack (using the fraudulently-issued certificates) requires the diversion of the victim's domain name translation from a correct DNS server to a 'poisoned' server[2]; otherwise there would be a mismatch between the URL typed by the user and the contents in the certificate, making it detectable as an invalid certificate by modern web browsers.

According to a report issued by Fox-IT[3], a company hired to investigate Diginotar's CAs, on the 10th of July 2011 the hackers were able to issue their first rogue certificate, whose CN (a field indicating a website's URL in a digital certificate) was *.google.com. A series of other certificates were later issued. The majority of them were detected by Diginotar's internal auditing and immediately revoked; however, the certificate issued with its CN being equal to *.google.com was not initially detected.

On the 29th of August (more than one month after the attacks were first detected), the fraudulent *.google.com certificate was finally revoked[4]; this was done after an Iranian user posted in a forum about a suspicious warning while visiting his Google mail[5]. Following the revocation, major browser vendors updated their browser software, removing the Diginotar's root certificate from their trusted certificate lists.

Further investigation showed an intensive activity of *.google.com on the Diginotar's OCSP (Online Certificate Status Protocol) responder[6] originating from Iran. In fact, more than 99% of such activity originated from Iran, suggesting that the discovered attack was likely targeting Iranian nationals, possibly to monitor anti-regime dissidents. A video was posted on YouTube, showing precisely where the malicious web requests were geographically distributed[7].

The incident revealed some interesting problems in the PKI system. Up to this attack, CAs had been portrayed as 'unbreakable'. The DigiNotar case reveals that some CAs are indeed vulnerable, in part due to mismanagement.

[2] Poisoned DNS servers translate domain names to incorrect IP addresses.

[3] http://www.rijksoverheid.nl/ministeries/bzk/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html

[4] http://www.vasco.com/company/press_room/news_archive/2011/news_diginotar_reports_security_incident.aspx

[5] http://www.google.co.uk/support/forum/p/gmail/thread?tid=2da6158b094b225a&hl=en

[6] The OCSP is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.

[7] nakedsecurity.sophos.com/2011/09/05/operation-black-tulip-fox-its-report-on-the-diginotar-breach/

It is, therefore, right to question the procedures under which Root CAs are added to browsers' trusted lists. This leaves us with an open question: was DigiNotar properly audited and sufficiently checked before being marked as 'trusted' by vendors?

According to Fox-IT's report[8], 'the successful hack implies that the current network setup and/or security procedures at DigiNotar are not sufficiently secure to prevent this type of attack'. Fox-IT further states 'the most critical servers contain malicious software that can normally be detected by anti-virus software. The separation of critical components was not functioning or was not in place. We have strong indications that the CA Servers, although physically very securely placed in a tempest proof environment, were accessible over the network from the management LAN'. Moreover, the Fox-IT report reveals that 'the network has been severely breached. All CA servers were members of one Windows domain, which made it possible to access them all using one obtained user/password combination. The password was not very strong and could easily be brute-forced'. Also, Fox-IT states that the software installed on the public web servers was outdated and not patched. Finally, Fox-IT claims that no antivirus protection was present on the investigated server and that no secure central network logging is in place. This prompts the question whether or not DigiNotar followed the most basic security procedures/standards. It is important to emphasise that DigiNotar is just an example here; how about other root CAs? Is it not about time that we reviewed them all? In addition, the process of authorising CAs to operate as root CAs needs to be reviewed.

The latest versions of IE[9], Firefox[10], Chrome[11], Safari and Opera are currently immune to attacks using the discovered fake certificates[12]. However, we could observe that some implementations do not run proper checks of revocation lists when verifying digital certificates. For example, older versions of IE or the current version of Apple's Safari[13] do not check CRLs (certificate revocation lists) or OCSP responders, leaving their users vulnerable until manually updating their browser's trusted certificate list (or adopting an operating system update); this is what exactly happened in the

[8] http://www.rijksoverheid.nl/ministeries/bzk/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html

[9] http://technet.microsoft.com/en-us/security/advisory/2607712

[10] http://blog.mozilla.com/security/2011/09/02/diginotar-removal-follow-up/

[11] http://googleonlinesecurity.blogspot.com/2011/09/gmail-account-security-in-iran.html

[12] http://en.wikipedia.org/wiki/DigiNotar

[13] http://support.apple.com/kb/HT4920

DigiNotar case.

The DigiNotar incident exposed an important issue regarding trust anchor management. It is argued that the current methods of embedding trusted certificate lists in applications and operating systems are far from perfect. However, this practice has been used for a long time, and, until now, there has been little evidence of more effective implementations. It is, now, high-time to review this practice. The DigiNotar incident reminds us all that trust anchor management should be, once again, the focus of current academic/industrial research. The proposition of new schemes/concepts is necessary to enhance the security properties of the CA business model. There are, already, some studies[14,15] in this area; however, further investigation and research remains a priority in this field, given its wide usage.

To conclude, most users are not currently vulnerable to the DigiNotar certificate-base attack. All known fraudulently-issued certificates have been revoked; the most widely-used web browsers and email clients have been updated, and will therefore no longer trust Diginotar's Root CA. However, users employing outdated web browsers and operating systems may be still at risk, particularly if their ISPs (Internet Service Providers) conspired to divert their web requests to a spoofed server.

[14] http://convergence.io/

[15] http://perspectives-project.org/