

Lessons to be learned from a recent case of fraudulent SSL certificates

Stockholm (Sweden), 1 September 2011 - On August 29, 2011 it was revealed that at least one fraudulent digital certificate had been issued by DigiNotar¹.

Digital certificates are, today, ubiquitous and effectively the pillar of most security and trust in the global information society. Many hundreds of millions of certificates are issued every year so that network users (private individuals, companies and public institutions) can control access to, encrypt or sign trillions of messages, documents and transactions.

What lessons can be learned from the DigiNotar case? A publicly supervised certification authority governed by stringent security requirements, DigiNotar was attacked by a malicious hacker intending to enable unauthorized eavesdropping on private email traffic.

First of all, this case –the impact of which on e.g. political dissidents in one or more countries cannot at this stage be fully understood, but is likely to be significant– is extremely rare and extremely targeted. Contrary to popular perception, total security does not exist. Given the security controls that should have been and most likely were in place within DigiNotar, the attack serves as a painful reminder that even a highly protected system can remain vulnerable if significant efforts and resources are expended to find and exploit a relative weakness.

If a company like DigiNotar can be successfully manipulated by a hacker, so can almost any other organization. It would be incorrect to draw the conclusion from the DigiNotar case that there are fundamental flaws in the use of public key certificates for securing information society assets and rights. The lesson to learn is that we need more, not less security and vigilance. To safeguard our common digital future, we need to recognize the need for combining appropriate awareness and processes with appropriate technologies. Public key certificate-based encryption, digital signatures and access control are and will continue to be a critical component in that mix, on all levels of the information society.

In response to the news about DigiNotar, TrustWeaver has as a precautionary matter disabled the use or validation of DigiNotar certificates in its On Demand services.

¹ The official DigiNotar response to this incident is published on http://www.vasco.com/company/press_room/news_archive/2011/news_diginotar_reports_security_incident.aspx.