Experts uncover weakness in Internet security

December 30 2008

Independent security researchers in California and researchers at the Centrum Wiskunde & Informatica (CWI) in the Netherlands, EPFL in Switzerland, and Eindhoven University of Technology (TU/e) in the Netherlands have found a weakness in the Internet digital certificate infrastructure that allows attackers to forge certificates that are fully trusted by all commonly used web browsers.

As a result of this weakness it is possible to impersonate secure websites and email servers and to perform virtually undetectable phishing attacks, implying that visiting secure websites is not as safe as it should be and is believed to be. By presenting their results at the 25C3 security congress in Berlin on the 30th of December, the experts hope to increase the adoption of more secure cryptographic standards on the Internet and therewith increase the safety of the internet.

When you visit a website whose URL starts with "https", a small padlock symbol appears in the browser window. This indicates that the website is secured using a digital certificate issued by one of a few trusted Certification Authorities (CAs). To ensure that the digital certificate is legitimate, the browser verifies its signature using standard cryptographic algorithms. The team of researchers has discovered that one of these algorithms, known as MD5, can be misused.

The first significant weakness in the MD5 algorithm was presented in 2004 at the annual cryptology conference "Crypto" by a team of Chinese researchers. They had managed to pull off a so-called "collision attack"

and were able to create two different messages with the same digital signature. While this initial construction was severely limited, a much stronger collision construction was announced by the researchers from CWI, EPFL and TU/e in May 2007. Their method showed that it was possible to have almost complete freedom in the choice of both messages. The team of researchers has now discovered that it is possible to create a rogue certification authority (CA) that is trusted by all major web browsers by using an advanced implementation of the collision construction and a cluster of more than 200 commercially available game consoles.

The team of researchers has thus managed to demonstrate that a critical part of the Internet's infrastructure is not safe. A rogue CA, in combination with known weaknesses in the DNS (Domain Name System) protocol, can open the door for virtually undetectable phishing attacks. For example, without being aware of it, users could be redirected to malicious sites that appear exactly the same as the trusted banking or e-commerce websites they believe to be visiting. The web browser could then receive a forged certificate that will be erroneously trusted, and users' passwords and other private data can fall in the wrong hands. Besides secure websites and email servers, the weakness also affects other commonly used software.

"The major browsers and Internet players - such as Mozilla and Microsoft - have been contacted to inform them of our discovery and some have already taken action to better protect their users," reassures Arjen Lenstra, head of EPFL's Laboratory for Cryptologic Algorithms. "To prevent any damage from occurring, the certificate we created had a validity of only one month - August 2004 - which expired more than four years ago. The only objective of our research was to stimulate better Internet security with adequate protocols that provide the necessary security."

According to the researchers, their discovery shows that MD5 can no longer be considered a secure cryptographic algorithm for use in digital signatures and certificates. Currently MD5 is still used by certain certificate authorities to issue digital certificates for a large number of secure websites. "Theoretically it has been possible to create a rogue CA since the publication of our stronger collision attack in 2007," says cryptanalyst Marc Stevens (CWI). "It's imperative that browsers and CAs stop using MD5, and migrate to more robust alternatives such as SHA-2 and the upcoming SHA-3 standard," insists Lenstra.

More information on the discovery may be found on the websites of the researchers:
www.win.tue.nl/hashclash/rogue-ca/
www.phreedom.org/research/rogue-ca/
www.appelbaum.net/research/rogue-ca/

Source: Ecole Polytechnique Fédérale de Lausanne