

Centrum Wiskunde & Informatica (CWI) – Amsterdam
École Polytechnique Fédérale de Lausanne (EPFL),
en Technische Universiteit Eindhoven

PERSBERICHT

30 december 2008

Experts onthullen zwakke plek in internetbeveiliging

Onderzoekers van het Centrum Wiskunde & Informatica in Amsterdam, EPFL in Zwitserland en de Technische Universiteit Eindhoven en onafhankelijke security-onderzoekers in Californië hebben een zwakke plek gevonden in de internetbeveiliging. Door deze kwetsbaarheid in de infrastructuur van digitale certificaten op het internet, kunnen vervalste certificaten uitgegeven worden die volledig vertrouwd worden door alle gebruikelijke webbrowsers. Hiermee is het mogelijk om beveiligde websites en mailservers na te bootsen en om vrijwel ondetecteerbare 'phishing aanvallen' te doen. De onderzoekers presenteren hun resultaten op 30 december tijdens het 25C3 security congres in Berlijn. Ze hopen daarmee te bereiken dat betere beveiligingsstandaarden op het internet gebruikt worden.

Als iemand een website bezoekt waarvan de URL met 'https' begint, dan verschijnt er een klein hangslot-symbool in het browserscherm. Dit geeft aan dat de website beveiligd is door middel van een digitaal certificaat, dat uitgegeven wordt door een van de vertrouwde Certificate Authorities (CA's). Om er zeker van te zijn dat dit een authentiek digitaal certificaat is, verifieert de browser de digitale handtekening ervan met standaard cryptografische algoritmes. Het team van onderzoekers ontdekte dat een van deze algoritmes – MD5 – vatbaar is voor misbruik.

De eerste belangrijke zwakke plek in het MD5 algoritme werd in 2004 tijdens het jaarlijkse Crypto-congres over cryptologie gepresenteerd door een team van Chinese onderzoekers. Zij slaagden erin om twee verschillende bestanden te creëren met dezelfde digitale handtekening. Dit resultaat was nog beperkt: een veel sterker resultaat werd in mei 2007 aangekondigd door de onderzoekers van het CWI, EPFL en de TU/e. Met hun methode lieten zij zien dat het zelfs mogelijk was om beide bestanden bijna geheel vrij te kiezen. Het team van onderzoekers heeft nu ontdekt dat het mogelijk is om een fictieve CA te creëren die door alle belangrijke webbrowsers vertrouwd wordt. Dit deden ze door gebruik te maken van geavanceerde wiskunde en een cluster van meer dan 200 commercieel beschikbare spelcomputers.

De onderzoekers hebben hiermee aangetoond dat een essentieel deel van de internet-infrastructuur niet veilig is. Een vertrouwde fictieve CA, in combinatie met bekende zwakke plekken in het DNS (Domain Name System) protocol, kan de deur openzetten voor vrijwel ondetecteerbare phishing-aanvallen. Een gebruiker kan bijvoorbeeld zonder het te weten naar een onbetrouwbare site geleid worden die er precies hetzelfde uitziet als de beveiligde bank- of e-commerce website die hij denkt te bezoeken. Zijn webbrowser kan dan een vervalst certificaat ontvangen dat

ten onrechte vertrouwd wordt. Zo kunnen wachtwoorden en andere persoonlijke gegevens in verkeerde handen vallen. Naast beveiligde websites en e-mailservers kan de zwakke plek ook andere veelgebruikte software beïnvloeden.

"De belangrijke browser- en internetbedrijven – zoals Mozilla en Microsoft – zijn geïnformeerd over onze ontdekking en sommige hebben al maatregelen genomen om hun gebruikers beter te beschermen," benadrukt Arjen Lenstra, hoofd van EPFL's Laboratory for Cryptologic Algorithms. "Om te voorkomen dat er schade wordt geleden, had het certificaat dat we creëerden een geldigheid van slechts één maand – augustus 2004 - en verliep dus meer dan vier jaar geleden. Het enige doel van ons onderzoek was om betere internetveiligheid te stimuleren, met adequate protocollen die de noodzakelijke veiligheid garanderen."

Volgens de onderzoekers laat hun ontdekking zien dat MD5 niet langer meer beschouwd kan worden als een veilig cryptografisch algoritme voor gebruik in digitale handtekeningen en certificaten. MD5 wordt momenteel nog steeds door enkele CA's gebruikt bij de uitgifte van digitale certificaten voor een groot aantal beveiligde websites. "Theoretisch was het al mogelijk om een fictieve CA te creëren sinds onze publicatie in 2007," zegt cryptanalist Marc Stevens (Cryptology Group, CWI). "Het is noodzakelijk dat browsers en CA's stoppen met het gebruik van MD5 en overstappen op robuustere alternatieven, zoals SHA-2 en de komende SHA-3 standaard," beklemtoont Lenstra.

ENGLISH VERSION

Centrum Wiskunde & Informatica (CWI),
École Polytechnique Fédérale de Lausanne (EPFL),
and Eindhoven University of Technology (TU/e)

PRESS RELEASE
December 30, 2008

Experts uncover weakness in Internet security

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 (Cryptology Group, 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.