Onderzoekers dringen aan: 'Industriestandaard SHA-1 moet eerder worden teruggetrokken'

12 oktober 2015 om 21:43 uur - Amsterdam

Een internationaal team van cryptanalysten dringt er bij de industrie op aan dat om de SHA-1 internet security standaard eerder in te trekken, omdat de kosten van het breken aanzienlijk lager blijken te zijn dan gedacht. Deze industriële standaard wordt gebruikt voor digitale handtekeningen, die credit card transacties, online bankieren en de distributie van software beveiligen. Op dit moment zullen browsers de SHA-1 handtekeningen pas in januari 2017 als onveilig markeren, ten gunste van de veilige opvolger SHA-2.

Meer over

- Nieuwe reconstructiemethode moet gezichtsherkenning voor forensische doeleinden verbeteren
- Universiteit Twente bij hoorzitting MH17 in Tweede Kamer
- Wordt software voor toeleveranciers belangrijker dan de hardware?

Marc Stevens van Centrum Wiskunde & Informatica (CWI) uit Amsterdam, Pierre Karpman van Inria uit Frankrijk en NTU Singapore en Thomas Peyrin van NTU Singapore ramen nu dat vervalste digitale handtekeningen veel eerder kunnen worden gemaakt. Stevens zegt: "We hebben net met succes de volledige binnenste laag van SHA-1 gebroken. We denken nu dat de state-of-the-art aanval op heel SHA-1, zoals beschreven in 2013, maar ongeveer 100.000 dollar zal kosten aan het huren van grafische kaarten in de cloud."

Grafische kaarten

Op 22 september leidde gezamenlijk onderzoek van Stevens, Karpman en Peyrin tot een succesvolle 'freestart collision attack' op SHA-1. Dit is een cryptografisch algoritme ontworpen door de NSA in 1995 om veilige digitale vingerafdrukken voor berichten te kunnen berekenen. Deze vingerafdrukken worden gebruikt in de berekening van digitale handtekeningen, die het fundament vormen van internetbeveiliging, zoals bij HTTPS (SSL) security, elektronisch bankieren, het ondertekenen van digitale documenten en software.

Botsingen - verschillende berichten met dezelfde message fingerprint - kunnen leiden tot vervalsingen van digitale handtekeningen. Een freestart collision breekt de binnenlaag van SHA-1. "We hebben net laten zien hoe grafische kaarten zeer efficiënt kunnen worden gebruikt voor dit soort aanvallen. Nu kunnen we dit ook gebruiken om ook een state-of-the-art collision attack voor de complete SHA-1 meer kostenefficiënt te maken", legt Karpman uit.

Internationaal beleid

Het onderzoeksteam zegt: "In 2012 schatte beveiligingsexpert Bruce Schneier dat de kosten van een volledige SHA-1 aanval in 2015 ongeveer 700.000 dollar zouden bedragen. Dit bedrag zou dalen tot ongeveer 173.000 dollar in 2018, wat hij binnen de financiële mogelijkheden van criminelen achtte. We hebben nu echter aangetoond dat voor deze aanvallen grafische kaarten veel sneller zijn en we schatten nu, in de vroege herfst van 2015, dat een volledige SHA-1 botsing tussen de 75.000 en 120.000 dollar kost voor het huren van een paar maanden rekentijd op Amazon EC2 cloud computers. Dit impliceert dat

botsingen nu al binnen de middelen van criminele organisaties vallen, bijna twee jaar vroeger dan werd verwacht, en een jaar voordat SHA-1 als onveilig zal worden gemarkeerd in moderne internet browsers."

"Daarom raden wij aan om op SHA-1 gebaseerde digitale handtekeningen al veel eerder als onveilig aan te merken dan het huidige internationale beleid voorschrijft. In het bijzonder doen we een dringend beroep op het het CA / Browser Forum om tegen een recent voorstel te stemmen om uitgifte van SHA-1-certificaten met nog een jaar uit te breiden."

Zinkend schip

"Hoewel dit nog niet een volledige aanval is, is de huidige aanval niet het gebruikelijke deukje in een security-algoritme, waardoor het in de verre toekomst kwetsbaarder wordt," zegt Ronald Cramer, hoofd van de CWI's Cryptology-groep. "Vergelijk SHA-1 met een schip dat een ijsberg heeft geraakt en snel water aan het maken is. Wij weten hoe groot het gat is, hoe snel het water zal stromen en wanneer het schip zal zinken: binnenkort. Het is tijd om het schip van SHA-2 te springen."

Thomas Peyrin van hetf Symmetric and Lightweight cryptography Lab (Syllab) aan NTU, legt uit: "SHA-1 was al theoretisch gebroken, maar nu is een zeer praktische kosteneffectieve toepassing in zicht. SHA-1's opvolgers SHA-2 en SHA-3 worden niet beïnvloed door deze recente cryptanalytische ontwikkelingen en blijven veilig."
Daniel Augot, hoofd van het Grace team bij Inria Saclay - Ile-de-France waaraan Karpman verbonden is, zegt: "De impact van de werkelijke toekomstige SHA-1 botsingen zal misschien niet zo ernstig zijn als het geval was met het HTTPS-kraak in 2008 en de Flame malware in 2012. Maar botsingen luiden wel het einde in van het vertrouwen in digitale handtekeningen die op SHA-1 zijn gebaseerd."

Huaxiong Wang, hoofd van NTU's afdeling Mathematical Sciences, zegt: "Certification Authorities (CA's), browser vendors en de industrie in het algemeen wordt aanbevolen om de migratie naar SHA-2 te versnellen. Helaas kan zelfs een enkele onveilige CA de veiligheid bedreigen van alle HTTPS websites ter wereld, zoals duidelijk blijkt uit de HTTPS kraak van 2008. Desondanks adviseren we ook websites om snel naar SHA-2 te migreren, om waarschuwingen voor bezoekers te vermijden wanneer internetbrowsers SHA-1 niet meer vertrouwen."

Stevens:"We hopen dat de industrie heeft geleerd van de gebeurtenissen met SHA-1's voorganger MD5 en in dit geval SHA-1 zal intrekken voordat in de nabije toekomst voorbeelden van vervalste ondertekeningen verschijnen. "

De groep beschreef hun aanbevelingen in een technisch rapport, dat online beschikbaar is: https://sites.google.com/site/itstheshappening/ . Het onderzoek werd deels gefinancierd door de 2014 Veni grant van de Nederland Organisatie voor Wetenschappelijk Onderzoek (NWO) voor Marc Stevens, door de Direction Générale de l'Armement voor Pierre Karpman, en door de Singapore National Research Foundation Fellowships 2012 voor zowel Pierre Karpman als Thomas Peyrin.

http://www.cwi.nl/.
http://www.inria.fr/.
http://www.ntu.edu.sg/

Reacties geplaatst op de website van het CA/Browser Forum: https://cabforum.org/pipermail/public/2015-October/006065.html

Voeg reactie toe **print** **mail door**