'Trek zwakke SHA-1 standaard sneller in'

13 OKTOBER 2015 11:35 | RIK SANDERS | 0

Een internationaal team van cryptanalysten dringt er bij de industrie op aan om de SHA-1 internetbeveiligingsstandaard 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.

Lees meer over:

Internet

Security

Browsers

CWI

Gerelateerde artikelen:

CWI verbetert ICT voor kankerbestraling

CWI-spin-off koppelt erfgoed-databases

CWI verhelpt bug in Java met formele

De wetenschappers Marc Stevens van Centrum Wiskunde & Informatica (CWI) uit Amsterdam, Pierre Karpman van het Franse nationale instituut voor computerwetenschappen Inria en Thomas Peyrin van de technische universiteit NTU Singapore, stellen dat er veel eerder dan geraamd vervalste digitale handtekeningen 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,

Meer Nieuws

Eurofiber bouwt glasvezelnet Aeres Groep

28-01-2016

KPN versnelt landelijke uitrol LoRa-netwerk

28-01-2016

Aareon levert Rochdale nieuw ERP-systeem

28-01-2016

Start-up Teamleader boekt goed jaar

28-01-2016

Ctac gaat partnership aan met inRiver

27-01-2016

Overzicht Nieuws

aan het huren van grafische kaarten in de cloud.'

Freestart collision

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 een state-of-the-art collision attack voor de complete SHA-1 meer kostenefficiënt te maken', legt Karpman uit.

Criminelen

Het onderzoeksteam wijst er op dat in 2012 beveiligingsexpert Bruce Schneier de kosten van een volledige SHA-1 aanval in 2015 schatte op ongeveer zevenhonderdduizend dollar. Dit bedrag zou dalen tot ongeveer 173.000 dollar in 2018, wat hij binnen de financiële mogelijkheden van criminelen achtte. Het team zegt nu te hebben aangetoond dat voor deze aanvallen grafische kaarten veel sneller zijn en dat volgens zijn

ESET beveiligt virtuele omgevingen

28-01-2016

Elke dag is Data Privacy-Dag

28-01-2016

Data Protection Day in tijden van verandering

28-01-2016

IoT en security: deze beelden zeggen genoeg

27-01-2016

Desastreuse cyberaanvallen liggen op de loer

27-01-2016

Overzicht Security

previou Next

1 2 3 4 5

schatting een volledige SHA-1 botsing momenteel 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 eerder 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.'

CA/Browser Forum

Het internationale onderzoeksteam heeft een dringend beroep gedaan op het CA/Browser Forum om tegen een recent voorstel te stemmen om uitgifte van SHA-1-certificaten met nog een jaar uit te breiden. De stemming hiervoor sluit op 16 oktober.

De groep beschreef hun aanbevelingen in een technisch rapport, dat online beschikbaar is.

BEOORDELING: ?