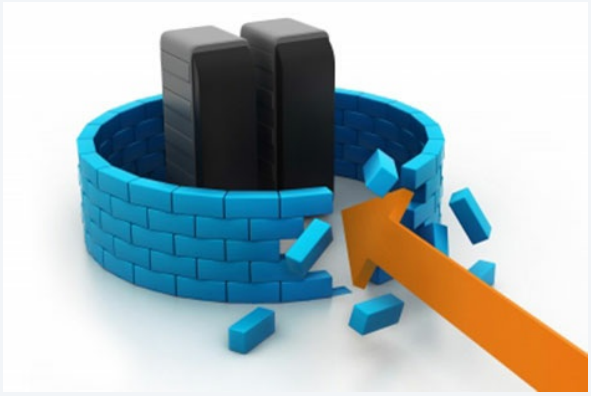
Opvolger internet security standaard SHA-1 sneller implementeren

ECONOMIE 12/10/2015 13:14:45



Een internationaal team van cryptanalysten dringt er op aan om de SHA-1 internet security standaard sneller te vervangen door veilige opvolger SHA-2.

ENGINEERINGNET.NL - Deze industriële standaard SHA-1 wordt momenteel 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.

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: "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."

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 (SSL) security, elektronisch bankieren, het ondertekenen van digitale documenten en software.

Verschillende berichten met dezelfde message fingerprint (botsingen) kunnen leiden tot vervalsingen van digitale handtekeningen. Een freestart collision breekt de binnenlaag van SHA-1.

Karpman: "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."

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.

Dimension Data waagt zich aan IT-voorspellingen voor 2016

>> Meer verwant nieuws

Carrièrekansen (meer)

Technical Supervisor
Camber | Overijse

Europe Lean Six Sigma ISO TS Process Coordinator
Chevron Belgium | Zwijnaarde

Assetmanager
BASF Antwerpen NV | Berendrecht-Zandvliet-Lillo

Project Manager
Bouwmaatschappij Ronse | Ronse

System Engineer
BMSvision | Meerdere regio's

Projectleider Bouw
CV Verwaest | Dessel

(Junior) Technisch Projectmanager
Agristo | Meerdere regio's

Application Support Engineer
Ordina Belgium | Mechelen of Hasselt

Regionaal Project Ingenieur
Hilti | Meerdere regio's

Technical Procurement Specialist
Ineos Manufacturing Belgium | Geel

Engineeringnet techpost

Je bent niet aangemeld bij Engineeringnet Techpost

Aanmelden

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.

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 websites ter wereld, zoals duidelijk blijkt uit de kraak van 2008. << (Guy Leysen) (bron: CWI) (Image courtesy of [hywards] at FreeDigitalPhotos.net)

TIP

Lees een online technisch rapport met deze aanbevelingen

Reageer of publiceer aanvullende informatie

Mis ook dit niet...

Colruyt Group introduceert duurzame koelkar

Colruyt Group gebruikt sinds kort de zelf ontwikkelde 'liquid ice container' voor het transport van verse producten naar de winkels. Deze werkt met vloeibaar ijs, wat uniek in de sector is.

Unilever helpt LNG doorbreken als schone brandstof

Unilever en het Innovation & Network Executive Agency ondertekenden een driejarig contract voor het verder ontwikkelen van een Europese LNG-infrastructuur.

Gentse havenbedrijven klagen over gebrek aan scholing - artikel

De Gentse havenbedrijven klagen over een gebrek aan scholing bij onderhoudstechnici en over de lange invultijden voor onderhoudselektriciens, -mecaniciens en