Centrum Wiskunde & Informatica wil eerder einde van SHA-1

donderdag 8 oktober 2015, 14:27 door **Redactie**, 9 **reacties**

Onderzoekers van het Centrum Wiskunde & Informatica (CWI) uit Amsterdam, het Franse inria en de Nanyang Technological University in Singapore willen dat het SHA-1-algoritme eerder wordt uitgefaseerd, omdat het goedkoper en daardoor ook realistischer is geworden om het algoritme aan te vallen.

Hashfuncties zoals SHA-1 worden gebruikt om een unieke fingerprint van data of een bericht te maken.Het wordt gebruikt voor het beveiligen van creditcardtransacties, internetbankieren en de distributie van software. Op dit moment zullen browsers SHA-1-hashes pas in januari 2017 als onveilig markeren, ten gunste van de veilige opvolger SHA-2.

Marc Stevens van het Centrum Wiskunde & Informatica (CWI) uit Amsterdam, Pierre Karpman van inria en Thomas Peyrin van NTU Singapore ramen nu dat vervalste digitale handtekeningen veel eerder kunnen worden gemaakt. "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", aldus Stevens.

Onderzoek

Op 22 september leidde **gezamenlijk onderzoek** van Stevens, Karpman en Peyrin tot een succesvolle 'freestart collision attack' op SHA-1. Collisions, verschillende berichten met dezelfde hash, 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.

In 2012 schatte beveiligingsexpert Bruce Schneier dat een volledige SHA-1-aanval in 2015 ongeveer 700.000 dollar zou kosten. Dit bedrag zou dalen tot ongeveer 173.000 dollar in 2018. Op dit moment kost volledige SHA-1-botsing tussen de 75.000 en 120.000 dollar, zo schatten de onderzoekers.

"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 internetbrowsers. 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", **aldus** de bezorgde onderzoekers.

Politie achterhaalt wachtwoord verdachte via telefoontap
EU-liberalen willen nieuwe regels na Safe Harbor-uitspraak

08-10-2015, 14:33 door Anoniem Reageer met quote

> "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", aldus Stevens.

Of je laat het gratis doen door een nieuwe cryptovaluta te releasen met hiervoor gemaakt code. Tegenwoordig is toch niet meer elke coin opensource.

08-10-2015, 15:29 door Briolet Reageer met quote

> Op dit moment zullen browsers SHA-1-hashes pas in januari 2017 als onveilig markeren,

Ik zag in de nieuwe Safari 9.0 browser dat je in het ontwikkelmenu kunt instellen om nu al de SHA-1 certificaten als onveilig weer te geven. (Hij laat dan gewoon het slotje niet meer zien)