Nederlandse samenvatting

Cryptografische hashfuncties, of simpelweg hashfuncties, zijn een van de belangrijkste bouwstenen binnen de cryptografie. Een hashfunctie is een algoritme dat voor elk willekeurig bericht een korte hash-waarde van een vast aantal bits (bv. 256 bits) berekent. Zulke hash-waarden worden gebruikt als een soort van vingerafdruk om het originele bericht mee te identificeren. Een belangrijke toepassing van hashfuncties is in digitale handtekeningen, waardoor documenten en software ondertekend kunnen worden en digitale communicatie beveiligd wordt.

Een belangrijke veiligheidseis is dat het praktisch onmogelijk moet zijn om collisions (twee berichten met dezelfde hash-waarde) te vinden. Een hashfunctie is gebroken wanneer er een efficiëntere aanval om collisions te vinden bestaat dan de generieke aanval gebaseerd op de birthday paradox.

Rond 2005 hebben Wang en coauteurs MD5 en SHA-1, twee belangrijke internationale cryptografische hashfunctie standaarden, gebroken met zogenaamde identical-prefix collision aanvallen. Niettemin, was de software industrie initieel sceptisch over de gevaren in de praktijk van deze eerste aanvallen op MD5 en SHA-1 omdat deze aanvallen technisch beperkt waren.

Dit proefschrift omhelst de volgende vijftal bijdragen op het gebied van de analyse van zwakheden van internationale cryptografische hashfunctie standaarden.

Ten eerste het verfijnen van de exacte differentiële analyse die ten grondslag ligt van bovenstaande collision aanvallen. En dan met name het introduceren van algoritmische methoden voor het vinden van de benodigde zogenaamde differentiële paden voor een grote klasse van hashfuncties die MD5 en SHA-1 omhelst, met specifieke verbeteringen toegespitst op MD5 en SHA-1.

Ten tweede het construeren van efficiëntere en met name flexibelere aanvallen op MD5. In het bijzonder introduceren we de zogenaamde chosen-prefix collision aanval op MD5, waarin een grote technische beperking van identical-prefix collision aanvallen geëlimineerd wordt: namelijk de eis dat de twee botsende bestanden volledig identiek zijn tot aan de 128 bytes die gegenereerd worden in de identical-prefix collision aanval en die tot de botsing lijden. Chosen-prefix collision aanvallen staan daarmee significant meer praktische aanvallen toe op cryptografische systemen.

De derde bijdrage is dan ook het aantonen van het gevaar van collision aanvallen op huidige cryptografische systemen met het doel de industrie zodanig te informeren dat het tijdig en op gepaste wijze zwakke hashfuncties kan vervangen door veiligere hashfuncties. Hoewel destijds het gevaar van deze verbeterde en efficiëntere aanvallen door de industrie nog enigszins onderschat werd, hebben wij in 2009 bewezen dat MD5's zwakheden wel degelijk een groot gevaar opleveren door een MD5-gebaseerde handtekening van een wereldwijd vertrouwde Certification Authority te gebruiken om zelf een vertrouwde Certification Authority te creëren. Met de geconstrueerde ver-

trouwde Certification Authority zouden we in principe – indien we deze niet bij voorbaat nietig hadden geconstrueerd – beveiligde digitale communicatie met beveiligde websites kunnen corrumperen op zodanige wijze dat webbrowsers de gecorrumpeerde digitale communicatie alsnog als veilig bestempelen ten overstaan van de gebruiker. Ons beoogde doel hiermee werd snel behaald: MD5 werd een verboden hashfunctie voor Certification Authorities.

De vierde bijdrage is het introduceren van nieuwe exacte differentiële analytische methoden voor SHA-1 en het construeren van identical-prefix en chosen-prefix collision aanvallen op SHA-1. Echter in tegenstelling tot MD5 zijn deze aanvallen niet praktisch uitvoerbaar vanwege de belemmerende hoge computationele kosten. Sinds de eerste theoretische aanval op SHA-1 door Xiaoyun Wang en coauteurs zijn er meerdere efficiëntere aanvallen geclaimd. Echter de claims die later wel gesubstantieerd zijn, blijken niet volledig correct te zijn wat zelfs geleid heeft tot terugtrekking van een zekere publicatie. Ten einde de correctheid van onze aanvallen op SHA-1 aan te tonen, alsmede een beter begrip en verdere verbeteringen van onze aanvallen mogelijk te maken, hebben wij als eerste ook de daadwerkelijke implementatie van onze aanvallen en onze analytische algoritmen gepubliceerd.

Voor een collision aanval zijn bepaalde vergelijkingen nodig die de zoekruimte voor een collision beperkt tot een specifieke ruimte waarin een bekende succeskans behaald kan worden, huidige methoden bepalen dit benodigde systeem van vergelijkingen en een schatting van de bijbehorende succeskans op basis van heuristieken. Onze aanvallen op SHA-1 zijn gebaseerd op een nieuwe exacte analyse welke sterk leunt op computationele combinatoriek en die in tegenstelling tot huidige methoden de interactie tussen zogenaamde local collisions op een exacte en uitputtende manier kan analyseren. Met behulp van onze nieuwe analyse is het mogelijk om voor alle geldige systemen van vergelijkingen exact te bepalen wat de bijbehorende succeskans is en daarmee hét systeem van vergelijkingen te kiezen dat leidt tot de hoogste succeskans en tevens de meeste vrijheidsgraden toelaat.

De laatste bijdrage is het introduceren van een efficiënte methode die cryptografische systemen kan beschermen tegen potentiële kwaadwillenden die gebruik maken van bovenstaande collision aanvallen. Hoewel zwakke hashfuncties zoals MD5 en SHA-1 dienen vervangen te worden door veiligere hashfuncties, lijken er een aantal praktische belemmeringen te zijn. Ten einde cryptografische systemen die gebruik maken van MD5 en/of SHA-1 veilig te houden tot aan die tijd dat MD5 en SHA-1 vervangen zijn, hebben wij een efficiënte methode geïntroduceerd die kan detecteren of dat bestanden en/of digitale communicatie met bekende collision aanvallen geconstrueerd zijn en daardoor het verder verwerken van boosaardige bestanden en/of digitale communicatie kan blokkeren.