Publicatie : Quest specials
Datum : 30 nov 2016
cm2 : 1.289
Pagina : 18
Advertentiewaarde : € 14.000,00
Regio : Nederland
Frequentie : incidenteel
Oplage : 161.819

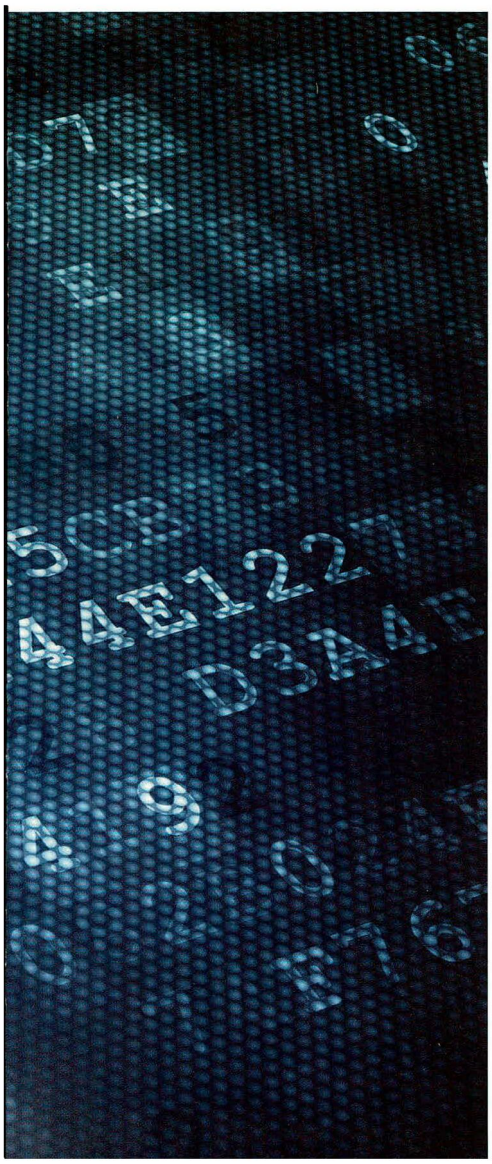
Amsterdamse crypto-analisten kraken software om spionnen voor te zijn

Kritisch kraken

Het wekt soms verbazing: wetenschappers die computersystemen aanvallen. Ze sporen lekken op in de beveiligingssoftware of onderzoeken mogelijkheden om toegangspasjes te vervalsen. Dat is heilzaam, zeggen ze. Hoe kan dat?

Tekst: Jop de Vrieze

Publicatie : Quest specials
Datum : 30 nov 2016
cm2 : 1.289
Pagina : 18
Advertentiewaarde : € 14.000,00
Regio : Nederland
Frequentie : incidenteel
Oplage : 161.819



Een aantal jaar geleden had Marc Stevens een probleem. De crypto-analist van het CWI (Centrum Wiskunde & Informatica) in Amsterdam legt zwakheden bloot in veiligheidssoftware om producenten daarvan ertoe aan te zetten om die te verbeteren. Maar in mei 2012 leek Stevens' methode gebruikt voor spionage. Medewerkers van het Russische antivirusbedrijf Kaspersky deden een opmerkelijke ontdekking: in Iran en enkele omringende landen waren duizenden computers besmet met Flame, een virus dat zou zijn gebruikt om het nucleaire programma van Iran te bespioneren. Een maand daarna meldde *The Washington Post* dat de geheime diensten van de VS en Israël achter deze aanval zaten. Stevens krabde zich op zijn achterhoofd. De manier waarop de krakers te werk waren gegaan, leek verdacht veel op de wijze waarop hij vier jaar eerder had aangetoond dat de beveiliging van veel websites niet meer voldeed. In 2009 had hij zijn software zelfs openbaar gemaakt. Had hij de hackers ongewild in de kaart gespeeld?

Wachtwoord wordt hash

Niet veel later belde een beveiligingsman die de Flame-aanval onderzocht. Of Stevens kon aantonen dat de aanval niet met zijn software was uitgevoerd. Dat kon Stevens. Met een wiskundige methode liet hij zien dat de software van de virusverspreiders helemaal door henzelf was ontwikkeld. Vermoedelijk gebeurde dat al voor Stevens zijn software openbaarde. De computers in Iran konden worden gehackt doordat een specifiek deel van de beveiliging, MD5, was gekraakt. MD5 is jarenlang gebruikt om websites te beveiligen. Het wordt geleverd door gespecialiseerde bedrijven, om onder andere te kunnen voorkomen dat er iemand anders op jouw account kan inloggen.

Hoe? Bijvoorbeeld door van je wachtwoord een soort digitale vingerafdruk te maken, een zogeheten 'hash' die uit een groot aantal cijfers bestaat. Deze vingerafdruk kan niet meer terug worden gezet in de oorspronkelijke boodschap (zoals je wachtwoord), maar hij kan wel worden gecontroleerd: de hash van jouw wachtwoord wordt naast de hash gelegd die de site heeft gemaakt toen je je wachtwoord instelde. De kans dat je de hash bij toeval juist gokt, is enorm klein. Bij een cijferslot ben je al lang bezig om alle mogelijkheden af te gaan, hetzelfde geldt ook voor een computer die willekeurige hashes uitprobeert. MD5 gebruikt codes van 128 bits met elk een één of een nul. Dat houdt in dat er twee tot de macht 128 mogelijkheden zijn, een getal van 39 cijfers. Ter vergelijking: een cijferslot met drie cijfers heeft 'slechts' tien tot de macht drie, maar toch al duizend mogelijkheden.

Update bleek vals

Het is de kunst om hash-algoritmen met zo veel mogelijkheden te ontwikkelen, dat het ondoenlijk wordt om ze allemaal af te gaan. Voor MD5 was dat oorspronkelijk het geval, maar doordat de rekenkracht van computers enorm toenam, is het nu wel mogelijk om met 'brute rekenkracht' MD5 te kraken, zegt Stevens. Dat is echter niet wat hij en zijn groep doen. 'Wij vinden methoden waarmee het nog sneller kan, door slimme wiskunde te ontwikkelen.' Zijn team haalde in 2008 de wereldpers door aan te tonen dat MD5 met zulke wiskunde te kraken is. In no time werd MD5 voor de beveiliging van websites afgeschaft. Maar het werd nog wel gebruikt voor onschuldiger toepassingen, bijvoorbeeld om te controleren of een attachment wel correct gedownload is. En door het virus in Iran bleek dat Microsoft ergens één toepassing over het hoofd had gezien, maar dat was wel een toepassing die uiteindelijk de beveiliging van Windows aantastte. Stevens: 'De door de geheime diensten ontwikkelde software deed zich als een echte Windows-update voor, omdat de software beveiligd was met een valse hash die van Microsoft afkomstig leek.'

Niet gek dus dat ook Microsoft contact opnam met Stevens. Het bedrijf is dan wel geen vriend van het Iraanse regime, maar het wil gegarandeerd veilige software bieden. Het team van Stevens ontwikkelde software die vervalsingen kan herkennen. Die software wordt gebruikt voor Internet Explorer, en zit, zo heeft Stevens vernomen, nu zelfs in de broncode van Windows. 'Ja, dat kan ik op mijn cv zetten', glimlacht hij.

Complexe software te lijf

'Hij crasht!' 'Wat doet hij nu weer?!' Zo'n kreet slaan we allemaal wel eens. Software gebruik je voor van alles en nog wat, maar soms kan het je werk ook onmogelijk en zelfs onveilig maken. Alle reden om programma's te analyseren: om te leren wat het verwachte gedrag is van complexe software en waarom die zich anders gedraagt dan je verwacht, stelde hoogleraar Jurgen Vinju van het CWI en de TU Eindhoven in zijn oratie, in 2016. Het lijkt wel wat op het analyseren van een literaire tekst, legt Vinju uit, want software is een taal. Wie software analyseert, doet dat als een criticus bij een roman: vanuit allerlei perspectieven. Zoals een mooi plot van een roman teniet kan worden gedaan door een slechte zinsbouw, kan een briljante software-architectuur verpest worden door een klein privacy-lekje. Software-analyse is kostbaar en tijdrovend. Daarom pleit Vinju voor automatisering: slimme programma's kunnen de grote hoeveelheden software-informatie snel doorzoeken, of doorrekenen wat er gebeurt bij een wijziging. Dit wordt hier en daar al een beetje gedaan, maar voorlopig zullen we soms nog zuchten vanwege software die toch niet doet wat we willen.

Publicatie : Quest specials
Datum : 30 nov 2016
cm2 : 1.289
Pagina : 18
Advertentiewaarde : € 14.000,00
Regio : Nederland
Frequentie : incidenteel
Oplage : 161.819

Chips worden steeds sneller en goedkoper: wat enkele jaren terug veilig was, is nu met brute kracht te kraken


Het datacenter van de NSA in Bluffdale (VS). Geheime diensten blijken graag rond te neuzen in de geheimen van zo ongeveer iedereen.

Rekenkracht daalde in prijs

Tegen de tijd dat MD5 bijna overal was afgeschaft, hadden crypto-analist Stevens en zijn collega's hun pijlen al gericht op een ander beveiligingsalgoritme: SHA-1. Ook dat begon barsten te vertonen. Het algoritme werd in de jaren negentig door de National Security Agency (NSA) in de VS ontwikkeld. SHA-1 is complexer dan MD5, waardoor er veel meer brute rekenkracht nodig is om het te kraken. In 2005 was al bewezen dat dat met slimme wiskunde ook kan, maar de leveranciers maakten zich nog geen zorgen: het zou miljoenen kosten om het aantal computerchips aan te schaffen dat nodig is om SHA-1 te kraken. Maar die chips werden alsmaar goedkoper: in 2012 berekenden twee Amerikanen op basis van Stevens' werk en de chipprijzen op Amazon.com dat dat 'nog maar' twee miljoen dollar kostte. En in 2015, zo voorspelden ze, zou het voor zeven ton lukken.

Maar de industrie maakte nog geen haast. In 2015 wilden ze de overstap op SHA-2, de nieuwere software, zelfs nog met een jaar uitstellen, tot 2017. Op dat moment berekende Stevens' team dat de kostprijs voor het kraken van SHA-1 was gedaald naar minder dan 100.000 dollar. Stevens had naast wiskundige verbeteringen een manier bedacht om in plaats van gewone computerchips, grafische kaarten in te zetten voor het rekenwerk. Die kaarten leveren meer rekenkracht per dollar op, omdat ze simpeler in elkaar zitten dan gewone chips. Het zijn een soort rekenkundige spierbundels.

Kraken is geen spel

Binnen enkele dagen waren producenten van beveiligingssoftware vrijwel volledig overgestapt op SHA-2. Die software was al jaren beschikbaar, maar hij was niet geschikt voor oudere computers. Stevens is tevreden over het besluit. 'Je moet niet de veiligheid van iedereen verkleinen om achterblijvers tegemoet te komen.'

Ondertussen is de onderzoeker alweer op zoek naar de volgende zwakke schakel. Soms lijkt het op een spelletje, dat wetenschappers de veiligheid van systemen van overheden en bedrijven testen. Maar dan denkt Stevens weer aan dat telefoontje over MD5 terug. 'Juist in deze tijd waarin overheden machtiger en angstiger worden, gaat het echt ergens over', benadrukt hij. 'De onthullingen van Edward Snowden (die in 2013 grote hoeveelheden geheime documenten aan kranten gaf, red.) laten zien dat de NSA echt alles en iedereen bespioneert en alle middelen daarvoor inzet. En de andere grootmachten blijven natuurlijk ook niet achter.' □

Het lek in de e.dentifier2 had geen grote gevolgen voor klanten van de bank.

E.dentifier met een lekje

Het begon met een afstudeeronderzoek van de informatica-student Arjan Blom, om het apparaatje te doorgronden waar de klanten van ABN AMRO online mee bankieren: de e.dentifier2. Het eindigde met een telefoontje waar de bank niet blij mee, maar wel dankbaar voor was. Er bleek een beveiligingslek in het apparaat te zitten. Wie het via een usb-kabeltje aansluit op de pc, moet voor het uitvoeren van een transactie daarop eerst zijn pincode invoeren. Vervolgens komt het bedrag op de display van de e.dentifier2 te staan, wat de gebruiker kan accorderen door op de knop 'OK' te drukken. Wat bleek? Dit accorderen kon de klant ook op zijn pc doen. Dat klinkt onschuldig of misschien zelfs handig, vertelt Joeri de Ruiter van de Radboud Universiteit in Nijmegen, maar als er op de computer een virus staat, dan kan er in theorie een heel andere transactie plaatsvinden, met een ander bedrag en een andere rekening als bestemming. Een paar maanden na de ontdekking van Blom was een nieuwe versie beschikbaar van het apparaatje. Zonder het lek: wie deze nieuwe e.dentifier2 aansluit op de computer kan alleen nog via het apparaatje op 'OK' drukken.