Forum Standaardisatie

Expertadvies: Vervanging MD5 door SHA-2 op lijst met gangbare standaarden

Datum 5 augustus 2010

Colofon

Projectnaam	Expertadvies: Vervanging MD5 door SHA-2 op lijst met gangbare standaarden
Versienummer	1.4 (definitief)
Locatie	
Organisatie	Forum Standaardisatie Postbus 84011 2508 AA Den Haag forumstandaardisatie@logius.nl
Auteurs	dr. ir. Eddy Olk (TNO) ir. Dennis Krukkert (TNO)

Inhoud

1 Inleiding

Op 27 januari 2010 is door het Bureau Forum Standaardisatie melding gemaakt om de standaard MD5 (Message Digest Algorithm 5) te verwijderen van de lijst met gangbare open standaarden, en in plaats hiervan SHA-2 (Secure Hash Algorithm) op te nemen.

Aanleiding voor de melding is dat het gebruik van MD5 door diverse organisaties wordt afgeraden in verband met geconstateerde beveiligingsproblemen. Verschillende externe partijen hebben Bureau Forum Standaardisatie hierop geattendeerd.

Aan TNO Informatie- en Communicatietechnogie (TNO) is gevraagd om als expert advies te geven over de ingediende melding, rekening houdend met de criteria die gelden voor opname op de lijst met gangbare standaarden.

2 Advies

Het advies is om de SHA-2 familie van hash algoritmen als vervanger van MD5 op te nemen voor het voorgestelde toepassingsgebied op de lijst met gangbare open standaarden, omdat SHA-2 voldoet aan de criteria. De SHA-2 familie kent een aantal varianten met hetzelfde algoritme maar met verschillende lengtes voor de hash-waarde, namelijk SHA-224, SHA-256, SHA-384 en SHA-512 (met respectievelijk een lengte van 224, 256, 384, en 512 bits).

3 Toepassingsgebied en criteria

3.1 Toepassinggebied

Het voorgestelde, functionele toepassingsgebied van SHA-2 betreft het gebruik van een cryptografische hash-algoritme ten behoeve van authenticatie (bijvoorbeeld via digitale handtekeningen) en integriteitscontrole (bijvoorbeeld via checksums). Opgemerkt dient te worden dat het toepassingsgebied genoemd door indiener voor SHA-2 breder is dan (maar mede omvat) het huidige toepassingsgebied voor MD5.

3.2 Uitsluitingscriteria

Om in aanmerking te komen voor opname op de lijst met open standaarden (zowel voor de lijst met open standaarden voor "pas toe of leg uit" als voor de lijst met gangbare open standaarden), dient een standaard te voldoen aan de uitsluitingscriteria.

- Eenmalige opname
  Aan deze eis wordt voldaan, SHA-2 staat niet de lijst met open standaarden voor 'pas toe of leg uit', en ook niet op de lijst met gangbare open standaarden.

- Betrekking op informatie-uitwisseling
  Aan deze eis wordt voldaan, SHA-2 wordt bij het uitwisselen van gegevens gebruikt voor het beveiligen van gegevens.

- Geen beperkt werkingsgebied
  Aan deze eis wordt voldaan, SHA-2 is niet organisatie- of implementatiespecifiek.

- Wettelijk verplicht
  SHA-2 wordt niet verplicht gesteld in wet- of regelgeving, dus ook aan deze laatste eis wordt voldaan.

3.3 Openheid

De SHA-familie van hash algoritmen is oorspronkelijk door de Amerikaanse National Security Agency (NSA) ontworpen en door het Amerikaanse National Institute of Standards and Technology (NIST) gepubliceerd en beschikbaar gesteld in de FIPS PUB 180-3 [7]. De hash algoritmen van SHA-2 zijn vervolgens vastgelegd in de ISO 10118 standaard [5].

SHA-2 voldoet in voldoende mate aan de vier karakteristieken voor openheid.

- Het beheer van SHA-2 is ondergebracht bij ISO, een non-profit organisatie die een open besluitvormingsprocedure hanteert.
- Het specificatiedocument is bij ISO verkrijgbaar voor een nominale bijdrage van CHF 192,- (ongeveer EUR 130,-). Via de website van NIST is het gratis te downloaden.
- De Amerikaanse overheid heeft een patent op SHA-2, maar heeft het intellectuele eigendom van SHA-2 ter beschikking gesteld op een 'royalty-free' basis.

- Er zijn voor SHA-2 geen beperkingen omtrent het hergebruik van de standaard.

3.4 Consensus

Gebruik van de SHA-2 familie wordt op dit moment veilig geacht tot 2030 en SHA-256 wordt al breed toegepast. Mogelijke alternatieve hash algoritmen die zijn vastgelegd in de ISO 10118 standaard worden vrijwel (nog) niet toegepast (WHIRLPOOL) of zijn kwetsbaar voor aanvallen waardoor gebruik wordt afgeraden door beveiligingsexperts (SHA-1, RIPEMD-128, RIPEMD-160).

Door experts wordt in het algemeen aanbevolen om SHA-2 te gebruiken in plaats van MD5 (en SHA-1). Gebruikers van de MD5 en SHA-1 standaarden, zoals PKIoverheid, volgen breed dit advies op. Daarbij wordt wel de kanttekening gemaakt dat er op dit moment een overgangsfase bestaat waarbij MD5 (en SHA-1) nog wel gebruikt wordt, maar de algemene verwachting is dat het gebruik van deze standaard(en) sterk zal afnemen. Gezien bovenstaande is er consensus om SHA-2 te gebruiken in plaats van MD5.

4 Achtergrond

4.1 Cryptografische hash algoritmen

MD5 en SHA-2 zijn zogenaamde cryptografische hash algoritmen die op deterministische wijze uit een willekeurige hoeveelheid gegevens een unieke code (ook wel hash, digest, fingerprint genoemd) berekenen met vaste lengte. De hash-waarde is te beschouwen als een vingerafdruk van de gegevens. Een wijziging in de gegevens zal een compleet andere hash-waarde opleveren.

Het gebruik in het toepassingsgebied zoals aangegeven door de indiener, is gebaseerd op enkele krachtige eigenschappen van hash algoritmen:

- Het is praktisch onmogelijk om gegeven een bepaalde hash-waarde *h* een verzameling gegevens *g* te vinden die na toepassen van het hash algoritme deze hash-waarde oplevert: *hash(g)=h*. Op basis van een bekende hash-waarde kan dus niet de achterliggende gegevens worden achterhaald. Dit wordt *pre-image resistance* genoemd.
- Het is praktisch onmogelijk om bij een verzameling van gegevens *g1* en de hash-waarde *h* na toepassen van het hash algoritme, een andere verzameling van gegevens *g2* te vinden die dezelfde hash-waarde *h* oplevert: *hash(g1)=h, hash(g2)=h, g1≠g2*. Het is dus niet mogelijk om bij een verzameling gegevens een andere verzameling gegevens te vinden die dezelfde hash-waarde geeft. Dit wordt *2nd pre-image resistance* genoemd.
- Het is praktisch onmogelijk om twee willekeurige verzamelingen *g1* en *g2* van gegevens te vinden die na toepassen van het hash algoritme dezelfde hash-waarde opleveren: *hash(g1)=hash(g2), g1≠g2*. Dit houdt in dat ondanks dat een hash algoritme een hash geeft met een beperkte lengte, het toch niet te voorspellen is welke verzamelingen van gegevens dezelfde hash-waarde zullen opleveren. Dit wordt *collision resistance* genoemd.

Een aanval op de *collision resistance* is eenvoudiger dan op *pre-image resistance* en *2nd pre-image resistance* maar kan voldoende zijn voor bijvoorbeeld het vervalsen van een PKI certificaat [4]. Bij een zwakheid in *collision resistance* van een hash algoritme wordt in het algemeen door experts dan ook afgeraden deze te gebruiken bij een digitale handtekening.

4.2 Kwetsbaarheid MD5

Al enige jaren is bekend dat MD5 ernstige zwakheden heeft wat betreft collision resistance en het gebruik van MD5 voor beveiligingsdoeleinden zoals een digitale handtekening wordt daarom afgeraden door GOVCERT.NL [3]. Het blijkt op relatief eenvoudige wijze mogelijk om met een MD5 collision een PKI certificaat te vervalsen [4]. Daarmee voldoet een digitale handtekening op basis van MD5 niet meer om te kunnen controleren of de gegevens in een certificaat niet zijn gewijzigd.

4.3 Alternatieven voor MD5

Als alternatief algoritme voor MD5 kan gekeken worden naar de hash algoritmen die zijn vastgelegd in de ISO/IEC 10118-3 standaard [5]: RIPEMD-128, RIPEMD-160, SHA-1, SHA-224, SHA-256, SHA-384, SHA-

512, WHIRLPOOL. Voor al deze algoritmen geldt dat de werking is beschreven (en kosteloos of tegen nominale kosten beschikbaar is). Het gebruik van de algoritmen WHIRLPOOL, RIPEMD-128 en RIPEMD-160 is vrij toegestaan [12][13]. De SHA-2 familie van algoritmen (SHA-224, SHA-256, SHA-384, SHA-512) [6] vallen onder het U.S. Patent 6829355 [8] maar gebruik is voor eenieder vrij toegestaan door de Amerikaanse overheid [9].

Van de genoemde algoritmen wordt het gebruik van SHA-1 al enige tijd afgeraden voor digitale handtekeningen. Net als bij MD5 zijn in SHA-1 zwakheden gevonden wat betreft collision resistance [10] en door NIST worden daarom de SHA-256 en SHA-384 hash algoritmen aanbevolen voor toepassing in PKI na het jaar 2010 [2]. Ook RIPEMD-128 en RIPEMD-160 worden niet aanbevolen omdat ze zwakheden bevatten wat betreft collision resistance [6]. De andere algoritmen worden wel aanbevolen [6] waarbij voor SHA-224 en SHA-256 gebruik op basis van de collision resistance veilig wordt geacht tot 2030 en voor WIRLPOOL, SHA-384, en SHA-512 tot na 2030.

Van de SHA-2 familie, en met name SHA-256, is de verwachting dat deze op grote schaal gebruikt zullen gaan worden [1]. Gezien het dringende advies van NIST om SHA-1 niet meer te gebruiken voor ondertekening van PKI certificaten wordt op grote schaal overgestapt op SHA-256. Ook bij PKIoverheid heeft men de overstap van SHA-1 naar SHA-256 al gemaakt [11]. Op dit moment wordt de uitgifte van certificaten op basis van SHA-1 nog wel ondersteund. Aangezien PKIoverheid in principe de adviezen van GOVCERT.NL en NIST volgt is te verwachten dat in 2011 door PKIoverheid geen certificaten meer zullen worden uitgegeven op basis van SHA-1.

5 Referenties

[1] European Network of Excellence in Cryptology II, *ECRYPT2 Yearly Report on Algorithms and Keysizes (2008-2009)*, July 2009

[2] NIST Special Publication 800-57, *Recommendation for Key Management Part 3: Application-Specific Key Management Guidance*, December 2009

[3] GOVCERT.NL, *Zwakheden in de internet PKI door gebruik van MD5*, Factsheet FS-2009-01, versie 1.3, 30 maart 2009

[4] http://www.win.tue.nl/hashclash/rogue-ca/

[5] ISO/IEC JTC 1/SC 27, Information technology - Security techniques – Hash functions – Part 3: Dedicated hash-functions, ISO/IEC 10118-3:2003(E)

[6] ISO/IEC TC 68/SC 2, *Financial services – Recommendations on cryptographic algorithms and their use – Standing Document*, ISO/IEC GUIDE 2:2007(E), November 2007

[7] NIST, *Secure Hash Standard (SHS)*, FIPS PUB 180-3, October 2008

[8] http://www.patentstorm.us/patents/6829355.html

[9] https://datatracker.ietf.org/ipr/858/

[10] http://csrc.nist.gov/groups/ST/toolkit/documents/shs/NISTHashComments-final.pdf

[11] GBO.Overheid, *CPS Policy Authority PKIoverheid voor certificaten uit te geven door de Policy Authority van de PKI voor de overheid*, versie 3.0, januari 2009.

[12] http://www.larc.usp.br/~pbarreto/WhirlpoolPage.html

[13] http://homes.esat.kuleuven.be/~bosselae/ripemd160.html