BLOG | Kim Tiedemann

EMNER *It-drift, Kryptering, Offentlig it, Sikkerhedshuller, SSL*

Så skal der bestilles SSL certifikater

Af Kim Bjørn Tiedemann 21. september 2014 kl. 12:51

Det har længe været kendt, at SHA-1 hashing algoritmen begynder at vise alderdomstegn og må betragtes som værende så usikker, at den ikke længere skal være vores førstevalg, når der skal implementeres sikkerhed. Den lider samme skæbne som MD5 algoritmen, som vi begyndte at bevæge os væk fra for snart mange år siden.

Allerede i 2005 blev det påvist (https://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html) at der findes en metode til at genere en hash kollision (http://en.wikipedia.org/wiki/Collision_attack) , som er 2000 gange hurtigere end brute force.

Bruce Schneier skrev for 2 år siden et blog-indlæg (https://www.schneier.com/blog/archives/2012/10/when_will_we_se.html) om at omkostningerne ved at producere en hash-kollision til stadighed bliver billigere og billigere. Det skyldes, at hardwaren fra i dag er billigere næste år grundet Moores lov. I blogindlægget estimeres, at det vil være muligt at skabe en kollision for USD 43.000 i 2021.

SSL certifikater

I SSL certifikater benyttes SHA-1 hashing algoritmen til at skabe en hashværdi af certifikatet, som efterfølgende signeres af det certifikat, som befinder sig i stien ovenover (typisk et intermediate eller CA certifikat). Når det viser sig praktisk muligt at skabe en hash-kollision kan man altså skabe et nyt certifikat, som har samme SHA-1 hash værdi som et andet certifikat. Det bliver med andre ord muligt at skabe et rogue certifikat, som kan bruges i stedet for det oprindelige (og rigtige) certifikat.

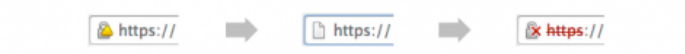
I 2008 viste (http://www.win.tue.nl/hashclash/rogue-ca/) forskere at dette kunne lade sig gøre med MD5 hashing algoritmen, og i nogle år har IT sikkerhedsfolk haft samme bekymring for SHA-1.

Microsoft reagerer

Den 12. november sidste år valgte Microsoft at fraråde brugen (https://technet.microsoft.com/en-us/library/security/2880823.aspx) af SHA-1 hashing algoritmen og tillader ikke at root CA efter 1. januar 2016 udsteder certifikater med SHA-1 hash algoritmen. Microsoft har ikke konkret beskrevet, hvad de har tænkt sig at gøre med fx brugergrænsefladen i Internet Explorer.

Google reagerer

I et blogindlæg (http://googleonlinesecurity.blogspot.co.uk/2014/09/gradually-sunsetting-sha-1.html) fra den 5. september skriver Google, at de langsomt (men hurtigere end Microsoft) vil udfase brugen af SHA-1 algoritmen. Det vil de gøre ved at deres Chrome browser over tid vil vise sikkerhedsadvarsler overfor brugere af sites, som benytter SHA-1 i deres SSL certifikat. Deres politik er, at Chrome vil vise mere og mere alvorlige sikkerhedsadvarsler for brugeren, for certifikater som udløber efter 1. januar 2016 og som stadig benytter SHA-1 algoritmen. Dette rangerer fra "lås med trekant advarsel" til den helt alvorlige "lås med rød streg over".



De offentlige sider

Der er mange offentlige sider der benytter SSL certifikater med SHA-1 hashing algoritmen.

Jeg har listet en række af dem her (i parentes vises gyldighed for certifikatet):

- nemlog-in.dk (2014-02-25 til 2015-01-06)
- www.tastselv.skat.dk (http://www.tastselv.skat.dk) (2013-09-27 til 2015-09-28)
- www.sundhed.dk (http://www.sundhed.dk) (2012-09-11 til 2015-09-13)
- indberet.virk.dk (2011-J07-04 til 2016-07-04)
- www.nemadgang.dk (http://www.nemadgang.dk) (2012-08-08 til 2015-10-15)
- www.e-boks.dk (http://www.e-boks.dk) (2013-08-15 til 2016-10-18)
- jobnet.dk (2012-10-02 til 2014-10-03)
- www.ug.dk (http://www.ug.dk) (2014-07-09 til 2017-07-08)

Jeg kunne kun finde et site hvis certifikat allerede benytter en SHA-2 hashing algoritme:

- www.borger.dk (http://www.borger.dk)

Som det kan ses vil kun e-boks.dk, virk.dk og ug.dk blive påvirket af ændringerne i Chrome, da de andre sites er tvunget til at skifte certifikat inden 2016.

For borger.dk gælder det, at indhold for selvbetjeningsløsninger tit vises i en iframe, og hvis disse sites benytter certifikater med SHA-1 algoritmen, så vil Chrome formentligt også vise en fejl (det fremgår dog ikke eksplicit af deres blogindlæg).

De berørte sites kan selvfølgelig vælge at genudstede deres certifikat, men historien peger desværre på, at SSL certifikater på offentlige sites når at udløbe, inden de skiftes: SU-lån (http://www.version2.dk/artikel/foraeldet-krypteringscertifikat-sender-studielaanere-ud-i-

kulden-51674) , PET (http://www.version2.dk/artikel/pets-hjemmeside-doemt-usikker-af-browseren-bruger-udloebet-ssl-certifikat-31527) og borger.dk (http://www.version2.dk/artikel/fem-aar-gammelt-tdc-certifikat-er-udloebet-borgerdk-gaar-i-roedt-31467)

Er det fornuftigt?

Der er megen debat på nettet om Googles beslutning. Er det for radikalt, når man tager i betragtning at SHA-1 endnu ikke i praksis er usikker?

Jeg kan godt lide, at Google bekymrer sig for Internettets sikkerhed, hvor de senest har valgt at benytte brug af SSL som en faktor (http://googlewebmastercentral.blogspot.dk/2014/08/https-as-ranking-signal.html) i deres ranking algoritme.

Jeg synes dog, hastigheden hvor med det implementeres er lidt voldsom. Specielt når man tager i betragtning at Chrome allerede om to versioner begynder at vise sikkerhedsadvarsler for certifikater, som udløber i 2017. Google har valgt at lave en trinvis implementering (de kalder det slow motion emergency) i stedet for en big bang løsning, og dermed tvinge sites der har et 2017 certifikat til at tage stilling snart.

Ovenstående liste af sites med SHA-1 hash algoritme certifikater viser også, at det er nødvendigt. På trods af at vi har vidst, at SHA-1 har begrænset levetid og CA/Browser forum har frarådet brugen af SHA-1 siden 2011, så udstedes der stadig gladeligt certifikater der benytter SHA-1 hash algoritmen. Så sent som i år blev certifikaterne til nemlog-in.dk og ug.dk udstedt med SHA-1 hash algoritmen.

Jeg synes at historien viser, at der er behov for at gribe ind. Certifikatudstederne ser ikke ud til at kunne håndtere dette selv og jeg mener, at implementeringen faktisk er en god måde at tvinge udbyderne til at udfase SHA-1 - ved at brugerne gradvist bliver gjort opmærksom på sikkerhedsproblemerne - man har jo ikke lyst til at handle et sted der har en adresselinje med rød streg igennem.

Er det fornuftigt? Hvad synes du?

Ps. Du kan bruge shaaaaaaaaaaaa.com (https://shaaaaaaaaaaaa.com) til at teste dit nuværende SSL certifikat.

Om Kim Bjørn Tiedemann

Kim er udviklingschef hos Schultz og arbejder også som løsningsarkitekt og scrum coach. Han har arbejdet med agil udvikling de seneste 5 år, teknologi er hans store passion, og i sin fritid koder han på en Windows 8-app. Han er uddannet i datalogi fra AAU.

Følg @kimtiede 96 følgere