(34)

[redacted]

Van: [redacted]
Verzonden: dinsdag 12 augustus 2008 8:30
Aan: [redacted]
CC: [redacted]
Onderwerp: FW: Bevindingen over generen stemcodes


review.pdf

[redacted]

Ter info.

Zie de vragen die hij onder 2.2 stelt.

Aanbeveling van [redacted] is om het referentiebestand niet voor de stemperiode te publiceren.

Met vriendelijke groet,

[redacted]

Programmamanager

Het Waterschapshuis
p/a Breestraat 59, Leiden
Postbus 130
1135 ZK Edam
[redacted]
www.hetwaterschapshuis.nl

-----Oorspronkelijk bericht-----
Van: [redacted]
Verzonden: dinsdag 12 augustus 2008 1:25
Aan: [redacted]
CC: [redacted]
Onderwerp: Re: Bevindingen over generen stemcodes

Hoi [redacted],

In de bijlage vind je mijn bevindingen.

In het kort kan ik concluderen dat het mij lukt om op een ongeveer 5 jaar oude PC 2^36 RnPID's te berekenen in ongeveer 40 uur. Dus ongeveer een factor 2 langzamer dan wat Fox-IT aangeeft, maar ik denk dat die factor wel weg te werken is door een moderne PC te gebruiken.

Verder heb ik niet genoeg informatie om daadwerkelijk te kunnen controleren of de aangegeven tijd om de vergelijkingen reeel is of niet.

Overigens denk ook ik dat het niet vooraf publiceren van de referentietabel, maar slechts de bijbehorende hashes, geen problemen voor het systeem oplevert en wel deze aanval voorkomt.

Met vriendelijke groet,
[redacted]

[redacted] wrote:

> [redacted]
>
>
>
> Bijgevoegd de reactie van [redacted] van een bevindingen van
> Fox-IT naar RIES. Het zou mogelijk zijn volgens Fox met een eenvoudige
> PC in korte tijd geldige stemcodes te generen op het gepubliceerde
> referentiebestand. Er wordt niet door ons ontkend dat dat niet mogelijk
> zou zijn. Maar Fox-IT claimt dat het binnen een zeer korte tijd kan -
> zonder de hulp van insiders - en met een eenvoudige PC. Dus ze gaan
> verder, waar het onderzoek van EiPSI is gestopt. Maar kloppen hun claims
> eigenlijk wel?!
>
>
>
> Bijgevoegd heb ik ook een korte appendix van Fox. De overige informatie
> uit het conceptrapport moet [redacted] aan je toezenden.
>
>
>
> Ik stel het zeer op prijs dat je op korte termijn hier tijd voor wilt
> vrijmaken. Als je nog vragen hebt, kan je die stellen aan [redacted]
> [redacted] of [redacted]. Aanstaande
> dinsdag dient Fox-IT het rapport definitief op te leveren en dan moeten
> we weten of hun claim inderdaad klopt.
>
>
>
> Overigens ga ik er van uit dat een en ander vertrouwelijk wordt behandeld.
>
>
>
> Met vriendelijke groet,
>
>
>
> [redacted]
>
>
>
> Programmamanager
>
>
>
> **Het Waterschapshuis**
>
> p/a Breestraat 59, Leiden
>
> Postbus 130
>
> 1135 ZK Edam
>
> [redacted]
>
> [redacted]
>
> www.hetwaterschapshuis.nl
>
>
>

Onafhankelijke review 'Hoofdstuk5' van [1]

Engelbert Hubbers
Digital Security
Radboud Universiteit Nijmegen

12 augustus 2008

Inleiding

Op vrijdag 8 augustus ben ik door Simon Bouwman namens de waterschappen gevraagd te kijken naar de claim die Fox-IT doet in haar rapport [1]. In dat rapport stelt Fox-IT dat het met een normale PC mogelijk is om binnen een dag zonder hulp van insiders een geldige stemcode, de sleutel `Kp`, te achterhalen.

Eveneens op die vrijdag heb ik van Bartek Gedrojc van Fox-IT de beschikking gekregen over hoofdstuk 5 uit hun rapport [1], samen met de code die bij de beschrijving van hun aanval hoort.

Het waterschap wilde mijn reactie graag voor dinsdag 12 augustus hebben in verband met de definitieve oplevering van het rapport.

1 Werkwijze

Aangezien de beschikbare tijd voor mij erg kort was, heb ik mij beperkt tot de volgende acties.

1. Het bestuderen van hoofdstuk 5.
2. Het bestuderen van de programmacode.
3. Het uitvoeren van testen.
4. Het beschrijven van de resultaten.

2 Het rapport van Fox-IT

Hoofdstuk 5 valt uiteen in drie delen: het probleem met het stemgeheim in 2030, de snelle aanval om een geldige `Kp` te berekenen en een aantal algemene bevindingen.

2.1 Achterhalen van `Kgenvoterkey`

De verhandeling over de kracht of juist de zwakte van de 2TDES-sleutel `Kgenvoterkey` lijkt mij correct. Het is helaas een intrinsiek probleem als het gaat over gegevens die voor lange tijd geheim moeten blijven. Als men maar lang genoeg de tijd heeft zal een brute-force attack uiteindelijk slagen. Maar men kan natuurlijk wel proberen de termijn zolang mogelijk te maken, door een krachtiger algoritme te gebruiken. Verder merkt Fox-IT terecht op dat naast de relatief zwakke 2TDES encryptie vooral de directe koppeling met het BSN ervoor zorgt dat het stemgeheim in 2030 niet meer gewaarborgd is.

Als de sleutel eenmaal is ingesteld wordt er met de call DES_cbc_cksum een DESmac berekend op dezelfde manier als in RIES wordt gedaan: encrypt de invoer via CBC en neem de laatste 8 bytes als resultaat. Op dit moment is er dus een kandidaat VnPID berekend.

En uiteindelijk wordt een kandidaat RnPID berekend door MDC2 (VnPID) uit te rekenen.

Allemaal precies zoals het binnen RIES ook gebeurt. In het bijzonder heb ik gecontroleerd dat als er een echte VnPID uit de referentietabel van RIESKOA als invoer wordt gebruikt, er ook daadwerkelijk dezelfde RnPID uitkomt als in die referentietabel staat.

4 Testen

Na overtuigd te zijn van het feit dat de berekeningen in het programma overeenkomen met de berekeningen in RIES, heb ik het programma aan het werk gezet op een reeds enkele jaren oude Pentium 4 waarop Fedora 9 draait.

```
 cat /proc/cpuinfo
processor : 0
vendor_id : GenuineIntel
cpu family : 15
model : 2
model name : Intel(R) Pentium(R) 4 CPU 2.80GHz
stepping : 9
cpu MHz : 2793.059
cache size : 512 KB
fdiv_bug : no
hlt_bug : no
f00f_bug : no
coma_bug : no
fpu : yes
fpu_exception : yes
cpuid level : 2
wp : yes
flags : fpu vme de pse tsc msr pae mce cx8 apic mtrr pge mca cmov
                  pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe
                  up pebs bts cid xtpr
bogomips : 5589.25
clflush size : 64
```

De machine heeft 1 gigabyte aan geheugen. Verder is het nog een gewone 'single core' machine. In het bijzonder is het duidelijk dat deze machine geen 'state of the art' is en dus zeer geschikt voor deze test.

Helaas heb ik geen echt 'profile' programma beschikbaar en heb ik de timing dus op een wat onnauwkeurige manier moeten doen via de time.h module en clock() functie.

Het standaardprogramma dat 1 miljoen opeenvolgende RnPID's uitrekent (waarbij opeenvolgend slechts slaat op de gebruikte sleutel aangezien de MDC2 en zo er natuurlijk voor zorgt dat er geen volgorde meer in te herkennen is) gaf een waarde van 1.7 seconden. Dat is niet zo snel als Fox-IT claimt, maar deze machine is dan ook iets langzamer dan de 3GHz die zij als maat nemen.

Vervolgens heb ik het programma een beetje aangepast zodat het geschikt is om tijdens een run in een file wat trace-informatie weg te schrijven. Uiteraard maakt dit het programma wat langzamer, maar dit is verwaarloosbaar. Om bijvoorbeeld 2^{32} RnPID's uit te rekenen laat ik na elk blok van 2^{26} RnPID's één entry in de log file wegschrijven. Daarbij bleek overigens een duidelijke regelmaat op te treden: elk blok van 2^{26} RnPID's kostte ongeveer 143 seconden, met als theoretisch gevolg dat de totale berekening van 2^{32} ongeveer 2.5 uur zou moeten duren. Dat bleek inderdaad te kloppen. In het bijzonder betekent dat dat het uitrekenen van de gewenste 2^{36} RnPID's op