Driftsättning av DKIM med DNSSEC

Examensarbete

Rickard Bondesson

ricbo974@student.liu.se
0730 – 23 95 16

Agenda

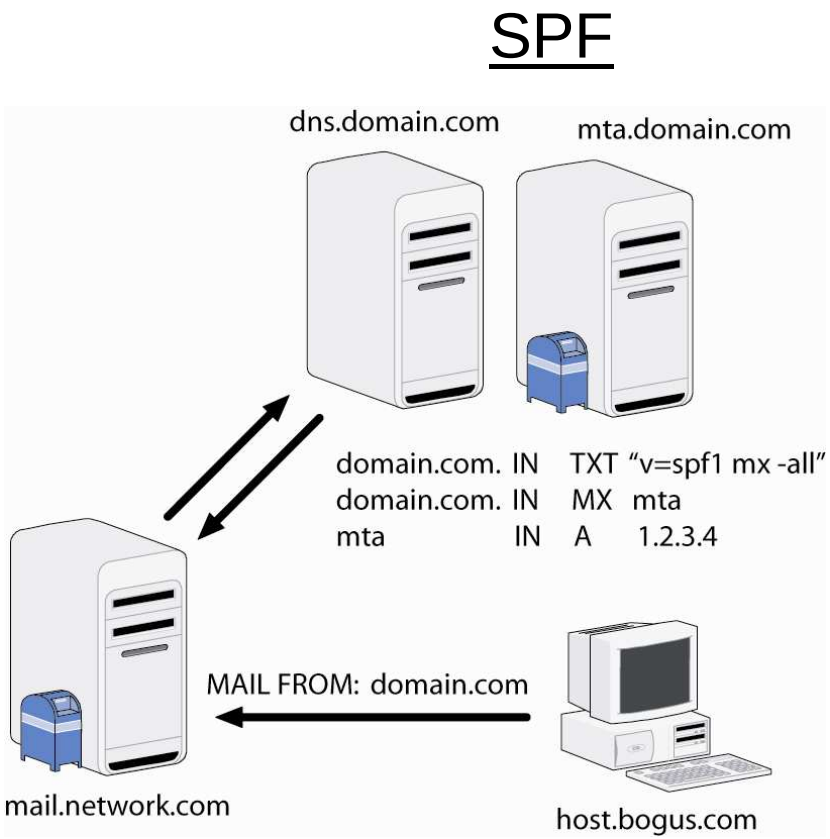
- Förfalskning av epost
- Åtgärder
- DKIM
- Pålitligheten inom DNS
- Driftsättning
- Tester
- Statistik
- Lärdomar

Förfalskning av epost

- Falska eposthuvuden
- Spam
- Phishing

Åtgärder

- Autentisering av avsändare
  - SPF
  - ADSP
  - SenderID
  - Black-/grey/whitelisting
- Autentisering av innehåll
  - S/MIME
  - PGP
- DKIM och DomainKeys



DKIM

- Fördelar
  - Genomskinligt för användarna
  - Alla behöver inte införa samtidigt
  - Anonymitet för användarna
  - Ingen ny public-key infrastructure behövs
  - Trasig signatur är som ingen signatur alls (ADSP?)
  - Löser inte spamproblematiken, men skyddar mot missbruk av epost domännamnet
- Nackdelar
  - Kräver extra hantering hos mailservern
  - Mer nackdelar kommer under hotanalysen

.se

DKIM - Canocalization

- Epost modifieras under leveransen
- Förbereder meddelandet innan signering
- Påverkar inte själva meddelandet
- Undviker vissa typer av modifikationer
- Två typer: simple och relaxed
  - Simple header canocalization
  - Relaxed header canocalization
  - Simple body canocalization
  - Relaxed body canocalization

.se

DKIM - Signering

- Checksumma av innehållet
- Signerar utvalda huvuden
  - Måste signera From: och delar av DKIM-huvudet
  - Rekommenderat att inte signera huvuden som troligtvis kommer att ändras under transporten
  - Denial-of-existence

.se

DKIM - Signatur

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
   d=exempel1.tset.se; s=ex1; t=1216375318;
   bh=F49+TW8nMriWgjHxXsVGiPa+xLNWevC3bGAT+Zl8Qag=;
   h=Reply-To:From:To:Subject:Date:Message-ID:MIME-Version:
   Content-Type:Content-Transfer-Encoding; b=AsmD11IU0TwqQwK
   9fGWIlV7TPtBRgEzcFwuhgbvaoipwcI9hA8M1TzE025rPzbLlJbEJKz8T
   2WSfmg7BbmSQ4rklSaq5ou1BrwxGTQWn/I37sOPhzg+pRfAjq7IWo6Zys
   OOgDkbCcOjL46kECDFQBWSvgKD3oOID4FOj5huSdzw=
```

Finns fler taggar än dessa. Se RFC4871

.se

DKIM – Publik nyckel

- Publicerar den publika nyckeln i DNS
  - Under *selector._domainkey.domain TXT*
  - Nyckelhantering med olika selektorer
  - Nyckelåterkallning

- Exempel:

```
ex1._domainkey.exempel1.tset.se. IN TXT "v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC6oekzH849jUK1EYJnfUM72
OlhpaTxqBhvNu3UTGsbRywFWBHCPfoeHAZKnYhN+pLAXuJ49oUNO1kybAqUfxPM
OpTbupY0zVdaJCtcMHi7j7rFgSrRi8nH55Frhq4aiS00ocdw1po0p72c7TkTNm5
E1Q2jZ4pGpjEXJtjzb9YckwIDAQAB"
```

.se

DKIM - Verifiering

- Återkonstruerar signaturen och jämför
- Resultatet kan exempelvis läggas i:

```
Authentication-Results: exempel2.tset.se; dkim=pass
    (1024-bit key) header.i=@exempel1.tset.se;
    dkim-adsp=none
```

.se

DKIM – Pålitligheten inom DNS

- Behöver tillförlitlighet för publika nycklar
- Sårbarheter hos DNS-systemet
  - Packet Interception
  - ID Guessing and Query Prediction
  - Name Chaining
  - Betrayal By Trusted Server
  - Denial of Service
- Attackerare publicerar egna DKIM nycklar

.se

DKIM - DNSSEC

- Digitala signaturer
- Upptäcker modifiering av tredjepart
- Säkrar källan av den publika DKIM-nyckeln
- Trust anchor till varje island-of-trust
- Signera hela vägen upp till rooten
- Skyddar ej mot Denial of Service

DKIM - Hotanalys

- Återspelning av tidigare skickad epost
- Riktiga användare som skickar dålig epost
- Använda liknande domännamn
- Använda samma namn som en pålitlig användare
- Lägga till information om längdparametern används
- Modifiera eller lägga till osignerade huvuden
- Utnyttja canocalization-algoritmen

.se

DKIM - Driftsättning

- Använder DKIM Milter
- Patchad för att hantera DNSSEC
- Kör två mailservrar
  - Sendmail
  - Postfix

.se

DKIM Milter - Tester

- Patchen
  - Funktionstester
  - Domäntester
- DKIM
  - Grundläggande epostfunktionaliteter
  - Samexistens med SPF, PGP, S/MIME och SpamAssassin
  - Interoperabilitet

.se

DKIM Milter - Resultat

- Funktionstester
  - OK
- Domäntester
  - OK
- Maskering
  - Nej, om det sker efter signering

DKIM Milter - Resultat

- Aliasing
  - OK
- Forwarding
  - OK
- Epostlistor (Mailman)
  - Ja, om epostlistan signerar
  - Nej, om epostlistan inte signerar
    Även om Mailman är konfigurerad att inte ändra något, så tar den bort vinkelparanteser i returadressen och bryter därmed signaturen.

.se

DKIM Milter - Resultat

- S/MIME
  - OK
- PGP
  - OK
- SMF-SPF
  - SPF OK
  - Programmet bryter signaturen då de ibland blandar resultatutskrifterna
- SpamAssassin
  - SPF och DKIM validering OK
  - Bryter signaturen om tidigare resultat är signerad

.se

DKIM Milter - Resultat

- Testa mot andra implementationer av DKIM
  - OK
- Epostlista hos GoogleGroups
  - OK, de signerar om meddelandet.
- Epostkonto hos GMail
  - OK
- Autoforward av ett epostkonto hos LiU
  - Nej, de gör en form av sanering i eposthuvudena innan eposten skickas vidare till tredje part. Bryter signaturen.

.se

DKIM - LiU

- Exempel på vad som bryter signaturen

  Skickades som:
  `From: ”Rickard B” <test@exempel.se>`

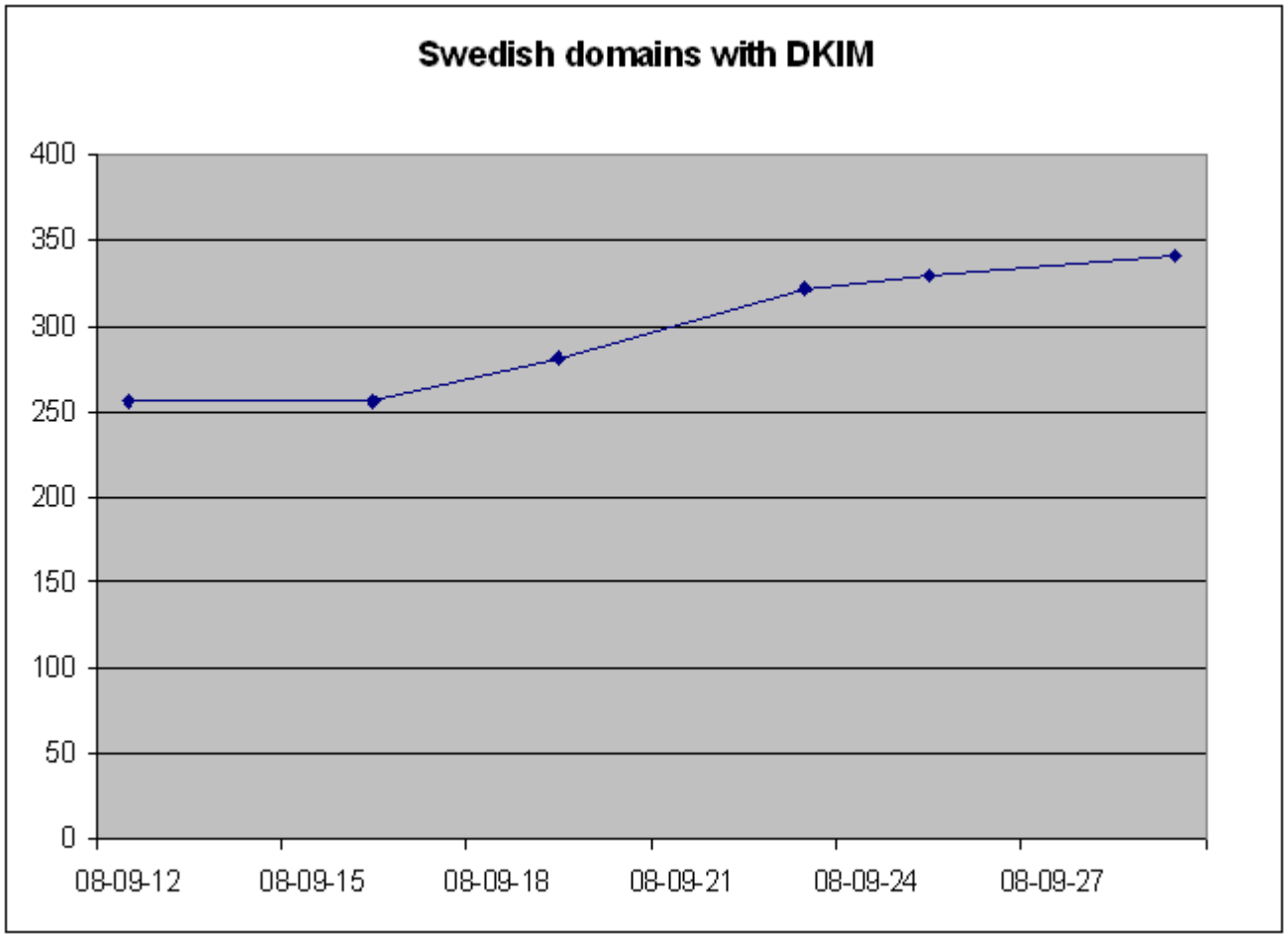
  Ändrades till:
  `From: Rickard B <test@exempel.se>`

.se

DKIM - Statistik

- Antalet publika DKIM-nycklar bland de svenska domänerna
- Mäta vid en epostserver
  - Antalet signerade samt signerade och verifierbara i relation mot antalet spam och antalet ham.

DKIM - Statistik



Defence.se
Fabege.se
Handelsbanken.se
Kirei.se
Spray.se
UU.se
Yahoo.se

.se

DKIM - Statistik

- Metoden är framtagen
- Söker större flöden för att säkerställa statistiken bland de epost som rör sig på Internet

DKIM - Lärdomar

- Modifiering under transport
- Epostlistor förstör ofta signaturen
- Finns vissa säkerhetshot
- Vad ska signeras?
- Policy? Kasta eller behålla?
- Använda ADSP
- DNSSEC skyddar DKIM nycklarna
- DKIM kompletteras gärna med andra teknologier så som SPF

.se

Tack för ert intresse!

- DNSSEC-patch till DKIM Milter
  http://opensource.iis.se/dkim/
- Rapport i slutet på november
  http://www.ep.liu.se

.se