Institutet for Matematik og Datalogi
Syddansk Universitetet, Odense

Spam - verifying the sender

DM71 Forår 2006

Bo Simonsen, 01-02-1983

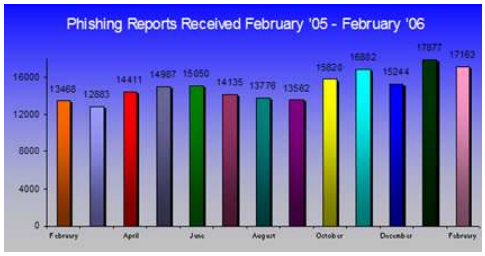
Indhold

1 Forord

Denne rapport beskriver metoder til bekæmpelse af SPAM, dvs. nuværende metoder der bliver benyttet til formålet, men primært metoder hvor en verifikation af afsender serveren foretages.

2 Spam - problemet

SPAM (formelt UCE - Unsolicited commercial e-mail) er kendt af de fleste som værende et voksende problem. Hvis vi betrakter figur 1 ses antallet af rapporterede phishing forsøg til APWG (Anti-phishing working group), disse tal er dog ikke realistiske da det formentlig kun er en meget lille procent (formentlig promille) af spam mails der bliver rapporteret til denne gruppe.



Figur 1: Antallet af rapporteringer vedr. phishing til APWG [1]

Langt de fleste brugere af e-mail modtager SPAM, hvis der ikke er en foranstaltning der kan filtrere spam. De åbentlyse ulemper ved SPAM er overfyldte mailbokse (mange udbydere af mails sætter en kvota på hver brugers mail konto), hvilket gør at måske vigtige mails ikke kan modtages, samt nogle virksomheder betaler for den trafik der bliver brugt på deres internet forbindelse, derved kommer de til at betale for SPAM.

3 Nuværende metoder

På nuværende tidspunkt er de mest brugte metoder til bekæmpelse af SPAM:

- Bayesian filters [4], som er baseret på et matematisk grundlag, netop Bayes theorem vi kender fra sandsyneligheds teori.

$$Pr(spam|words) = \frac{Pr(words|spam)Pr(spam)}{Pr(words)}$$

  Som det ses er sandsyneligheden for spam givet nogle ord lig med sandsyneligheden for at finde disse ord i en spam mail multipliceret med sandsyneligheden for hvilken somhelst e-mail er spam divideret

med sandsyneligheden for at finde disse ord i en hvilken somhelst e-mail. Selve filteringen foretages ved at brugeren først "træner" filteret, dvs. klassificere nogle mails som spam, herved stiger sandsynligheden for $Pr(words|spam)$ samt $Pr(spam)$ derimod stiger $Pr(words)$ alt efter antallet af e-mails der modtages. Denne type filter benyttes bl.a. i Mozilla thunderbird, hvilket er en meget brugt e-mail client. Men benyttes også på server siden i bl.a. spam filterings programmet SpamAssassin.

- Realtime Black List (RBL) - Denne metode benyttes på server siden, vha DNS opslag. Afsender mail serverens ip slås op vha følgende DNS opslag

  $$62.242.216.110 \Rightarrow 110.216.242.62.relays.ordb.org$$

  Hvis DNS opslaget lykkedes er den omtalte IP blacklistet, da det er blevet rapporteret der bliver afsendt spam fra denne ip. I ovenstående eksempel er der benyttet ORDB som kun lister mailservere der er "åbne relays", hvilket vil sige alle kan sende gennem disse mailservers, som spammere naturligvis udnytter.

- Graylisting - Denne metode udnytter at man i SMTP protokollen, som benyttes til post overførsel, kan afvise en mail midlertidigt. Dvs. første gang mailen sendes, vil den blive afvist, herefter vil afsenderen prøve igen (dette er beskrevet i RFC 821 [2]. Essensen er at spammere ikke har plads til at sætte mails i kø, hvilket en "rigtig" mailserver har, da den ellers ikke vil overholde RFC'en.

I ovenstående metoder bliver afsender serveren ikke verificeret på nogen måder, hvilket gør at disse metoder ikke bekæmper spam 100%. Med en verifisering opnår man nemlig at man nemt kan spore en spammer, hvilket ovenstående metoder ikke gør muligt.

4 DKIM

DKIM (Domain Key Identified Mail) er en teknik udviklet af Cisco/Yahoo til at verificere afsender serveren vha privat/offentlig nøgle kryptering.

Princippet i Domain key er følgende:

- Afsender serveren offentliggør hans offentlige nøgle i DNS.

- Før der afsendes en mail indsættes der en DKIM signatur i mailens header. I denne signatur indgår en signeret (med afsenderens private nøgle) sum (fx. SHA-1) over nogle udvalgte headers (som afsender serveren selv vælger, i henhold til IETFs specifikation [3] skal From headeren være inkluderet. Efter signeringen encodes summen i base64.

- Når mailen modtages hos modtager serveren slås afsenderens offentlige nøgle op i DNS, modtager serveren udregner summen over de udvalgte headers, decoder den modtagede sum, og herefter verificere den sum der er modtaget fra afsender serveren.
- Hvis summen kan verificeres leveres mailen, ellers ikke.

Der ses et rutediagram over modtagelsen af mailen i sektion A i appendix.

4.1 Tekniske detaljer

Syntaksen for en minimal domainkey signatur ser således ud (i Appendix C forefindes et eksempel):

```
DomainKey-Signature: a=..; q=..; c=..; s=..; d=..;
h=..;b=..
```

De enkelte værdier i denne signatur betyder følgende (alle tænkelige værdier for en DKIM signatur er beskrevet i [3]):

- **a**= Algoritme - Fx. rsa-sha1, hvilket betyder der benyttes RSA til signering og SHA1 til udregning af sum. Herved ligger standarden sig ikke fast på nogen specielt signering/kryptering.
- **q**= Query method - Fx. DNS, dvs. den offentlige nøgle hentes vha DNS.
- **h**= De headers fra mailen der udvælges til at udregne summen med.
- **b**= Den signerede sum encodet i base64.
- **c**= "Canonification" - angiver hvilken algoritme der benyttes til at fortolke headers. Disse kan blive ændret under overførselen **simple** tillader ingen modifikationer, derimod **nofws** er i stand til at verificere summen alligevel selvom der bliver *wrappet* linjer i headeren.

For at foretage DNS opslaget benyttes **s**= (selector) samt **d**= (domainet), samt det er TXT recorden der skal slås op. Dette foretages på følgende måde.

```
host -t txt <selector>._domainkey.<domain>
```

Resultatet af opslaget vil have følgende syntaks:

```
$ host -t txt beta._domainkey.gmail.com
beta._domainkey.gmail.com descriptive text "t=..\; k=..\; p=.."
```

Hvor **t**= angiver diverse flags, pt. benyttes kun y for "testing", hvilket i henhold til IETF specifikation [3] betyder at verificeret mail og ikke verificeret mail skal behandles på samme måde. **k**= angiver nøgle typen (i eksempelet i appendix D er denne RSA). **p**= er selve nøglen.

5 Sender ID

Sender ID / SPF [5] er Microsofts metode til bekæmpelse af SPAM, denne metode er mere simpel end DKIM, da der verificeres på IP niveau fremfor der benyttes kryptografi. Det overordnede princip i Sender ID er:

- Afsender server offentliggøre SPF record i DNS.
- Når en mail sendes, slår modtager serveren SPF recorden for det domain afsender påstår at må sende fra i DNS.
- Hvis afsenderens IP er listet i SPF recorden, accepteres mailen, ellers afvises den.

Der ses et rutediagram over modtagelsen af mail ved brug af SenderID i appendix B

5.1 Tekniske detaljer

Som det ses i ovenstående forklaring, er SPF (Sender policy framework) recorden essensen i Sender ID. Dette er ganske almindelig DNS TXT record, som ser sådan ud

```
bo % host -t txt geekworld.dk
geekworld.dk descriptive text "v=spf1 a mx ptr ~all"
```

Ovenstående record vil være en af de mest gængse, da denne record fortæller de IP adresser, som A og MX recorden peger på må sende fra den omtalte domain. Samt hvis IP's reverse record peger på domainet (dvs. en ip slås op til at være <hostname>.domain). Man kan også angive særskilte ip ranges vha **ip4:<ip range>**, ip ranget angives vha CIDR [6] notationen fx. 192.168.0.0/24 hvilket betyder alle IP adresser i intervallet 192.168.0.0-255.

~ all betyder at hvis afsender serveren ikke er en af ovenstående, vil Sender ID rapportere en soft fail, dvs. at det er op til mail systemet at afgøre om den enkelte skal accepteres. Hvis **-all** var angivet.

Man kan også benytte **include** hvis der fx. er mange IP adresser der må sende for et domain som fx. hotmail.com der råder over mange mail servere. Deres SPF record ser således ud:

```
hotmail.com descriptive text "v=spf1 include:spf-a.hotmail.com
.. ~all"
```

Ovenstående betyder der er en henvisning til `spf-a.hotmail.com` hvor der er angivet en SPF record, der skal benyttes. Årsagen til dette er at TXT records har en maximal længde (512 bytes i henhold til [3]).

6 Nuværende status

De to omtalte metoder er på nuværende tidspunkt implementeret hos:

- Gmail.com benytter både DKIM og Sender ID.
- Yahoo.com benytter DKIM.
- Hotmail.com benytter Sender ID.

Ovenstående er nogle af de største udbydere af Gratis E-Mail adresser.

7 Konklusion

DKIM er en meget avanceret metode til at verificere afsenderen med. Dette har ulemper i form af kompleksitet (i forhold til almindelig e-mail overførsel har signering/verificering en højere tidskompleksitet), men omvendt er spammere nemme at spore hvis de benytter DKIM, da alle der besidder et domain kan spores. Hvis man skal lave et angreb, kræver det man fremskaffer den private nøgle, som skal holdes hemmelig af den enkelte server.

Sender ID er en mere simpel metode, men metoden verificere afsender serveren da det kun er domæne ejeren der kan offentliggøre SPF recorden. Sender ID er mere sårbar over for DNS poisoning da der ikke indgår kryptografi, men blot kontrol på IP niveau.

En ulempe ved begge metoder er, at brugere skal benytte en anden port (port 587 er på nuværende tidspunkt foreslået), for hvis brugerne benytter port 25 til afsendelse af mail vil der opstå komplikationer, i det SPF rekorden ikke kan verificeres, samt der er ikke er angivet en Domainkey signatur.

Begge metoder vil være bedre end de nuværende, da der fortiden bliver filteret SPAM på grundlag af sandsynelighed, samt lister man ikke har nogen garanti for er korrekte.

Dog kan det sagtens tænkes, at man benytter Bayesian filters sammen med Domainkey/Sender ID. En hensigtsmæssig måde ville være, at hvis en mail er verificeret enten vha Domainkey eller Sender ID vil den forbigå Bayesian filter, ellers vil mailen blive undersøgt af Bayesian filter.

Bo Simonsen

Litteratur

[1] Anti-Phishing Working Group - `http://www.antiphishing.org/`

[2] RFC 821 - SMTP protocolen - `http://rfc.sunsite.dk/rfc/rfc821.html`

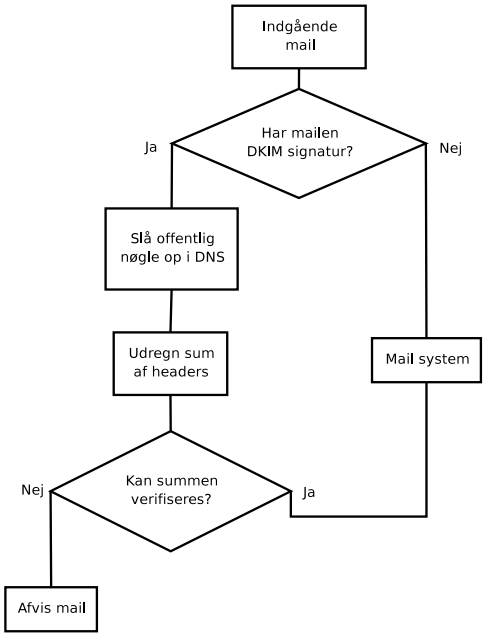
[3] IETF (The Internet Engineering Task Force) specifikation om domainkey - `http://www.ietf.org/internet-drafts/draft-delany-domainkeys-base-04.txt`

[4] Bayesian filter - `http://en.wikipedia.org/wiki/Bayesian_filter`

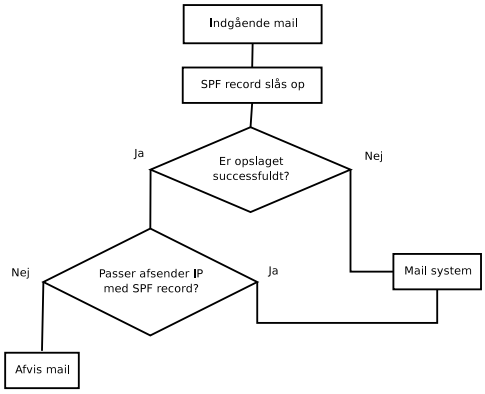
[5] IETF specifikation om SPF - `http://www.ietf.org/internet-drafts/draft-schlitt-spf-classic-02.txt`

[6] CIDR - `http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing`

A Rute diagram for modtagelse af mail med DKIM



B Rute diagram for modtagelse af mail med Sender ID



C Domainkey signatur

DomainKey-Signature: a=rsa-sha1; q=dns; c=nofws; s=beta; d=gmail.com; h=received:message-id:date:from:to:subject:mime-version:content-type; b=tHX1w3JH8T/INYEBNqeHXK1YkGaILaK8RbAAc7rT5Uqaga3P9su9I6vm/IMbyAfiCbbG4 xWdq1BJWuJffMRZjam617v6W9k2Zz6dfg3U4NMpPRI9PxXyn5bcqIrfRCnuf5ZInXXAOe0l euLbv+bwZ/nbZeun3Ze+us+NKmiC4Xg=

D Domainkey DNS record

```
$ host -t txt beta._domainkey.gmail.com
beta._domainkey.gmail.com descriptive text "t=y\; k=rsa\; p=MIGfMA0GCSq
GSIb3DQEBAQUAA4GNADCBiQKBgQC69TURXN3oNfz+G/m3g5rt4P6nsKmVgU1D6cw2X6Bnx
KJNlQKm1Of8tMx6P6bN7juTR1BeD8ubaGqtzm2rWK4LiMJqhoQcwQziGbK1zp/MkdXZEWM
CflLY6oUITrivK7JNOLXtZbdxJG2y/RAHGswKKyVhSP9niRsZF/IBr5p8uQIDAQAB"
```