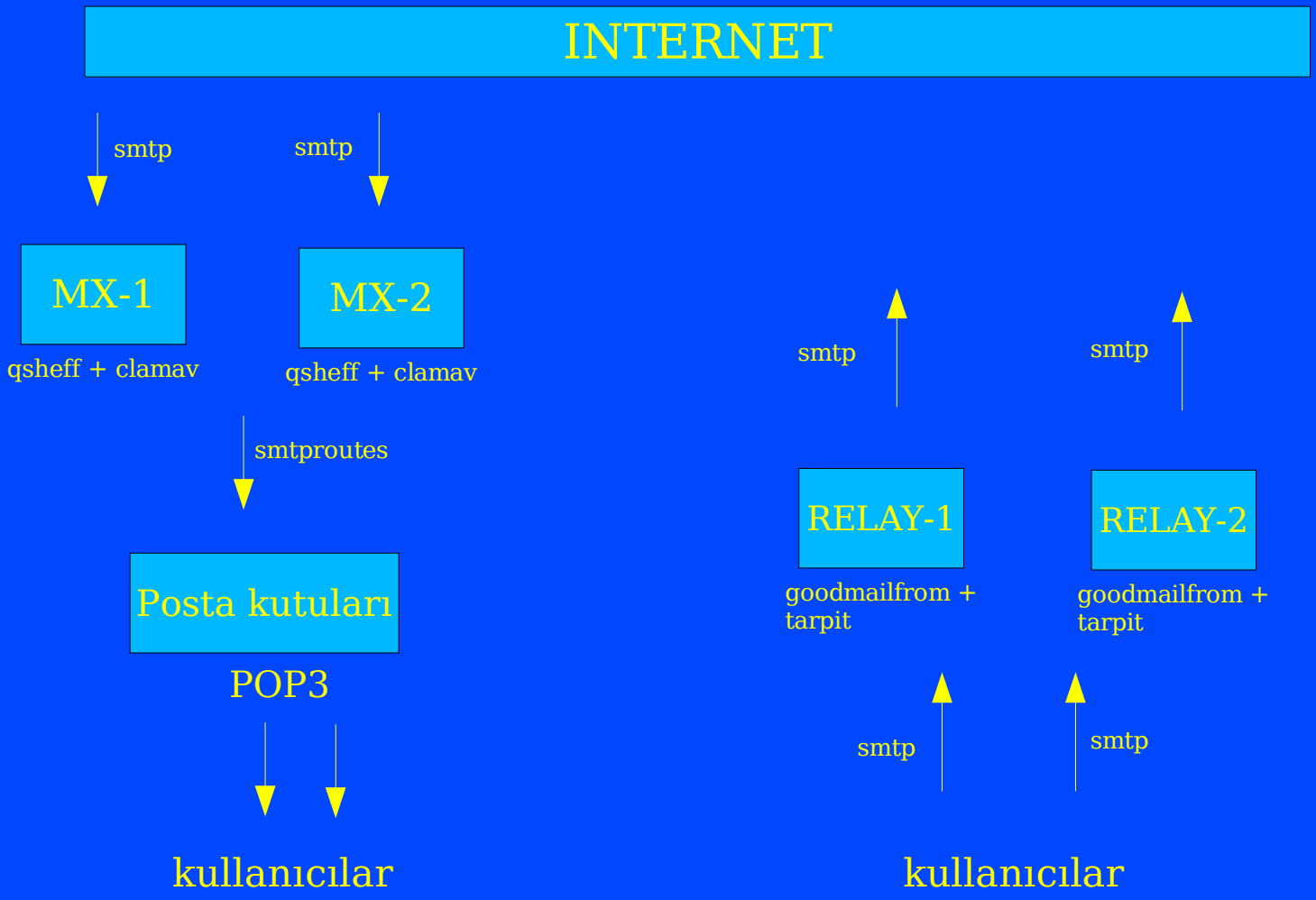
qmail ile SPAM engelleme

Devrim Sipahi
Dokuz Eylül Üniversitesi
devrim.sipahi@deu.edu.tr

Üniversitelerde kullanılan mail sisteminin iki belirgin özelliği vardır.

1. Çok sayıda kullanıcı (örneğin 10000)
2. Yoğun kullanım
    a. Normal kullanım (Toplu mail gönderimi)
    b. İstenmeyen trafik (spam virüs)

Sistem yapısı



Sistem yapısı

POSTA KUTULARI

Solaris 10
qmail-vpopmail-mysql
Sanal kullanıcılar
(vpopmail:vchkpw)
posta kutusu türü: maildir

Ekli dosya tipi kontrolü
Log analizi (isoqlog)
Alıcı sayısı kısıtlaması
Uzunluk kısıtlaması

DİĞER SUNUCULAR

MX sunucular FreeBSD

qmail
qsheff
clamav

RELAY sunucular FreeBSD

qmail
tarpit: Alıcı sayısı kısıtlaması
goodmailfrom: Gönderen kısıtlaması

Dışarıya SPAM Gönderilmesini engellemeye yönelik çözüm

1. Yetkili makineler dışında hiçbir pc dışarıyla smtp bağlantısı kurmamalıdır. Örnek pf.conf satırı:

```
table <SMTP> persist file "/etc/smtp"
block  in quick  on $int_if  proto tcp from ! <SMTP> to any port 25 flags S/SA
```

2. RELAY sunuculardan toplu gönderimi engellemek için **tarpit** yaması uygulanmalıdır.

3. Başka domainler adına posta gönderilmesini engellemek için **goodmailfrom** yaması uygulanmalıdır.

Tarpit yamasının uygulanması

http://www.palomine.net/qmail/tarpit.patch

adresindeki yama qmail-smtpd.c dosyasına uygulanır.
Bu yama programın akışını değiştirmez.
İki kontrol dosyasında yazılı iki değişken kullanılır.
Tarpit sayısı ---> control/tarpitcount
Tarpit süresi ---> control/tarpitdelay

Bir mesajdaki alıcı sayısı (To,Cc, Bcc toplanmı) tarpit sayısına ulaştığında tarpit süresi kadar bekletilir.
Böylelikle toplu maillerde istemci program zaman aşımına uğrar.

Goodmailfrom yaması

RELAY hakkı verdiğiniz kullanıcıların,
size ait olmayan alan isimlerini (domain) kullanmasını engellemek için
"goodmailfrom" yaması uygulanır.

Bu yama badmailfrom mantığı ile aynıdır.
/var/qmail/control/goodmailfrom isimli dosya oluşturulur.
İstenen alan isimleri, başlarına "@" işareti ekleyerek yazılır
Örnek:
@deu.edu.tr
@deu.net.tr

İstisnalar için GMFCHECK değişkeni kullanılır.
Bu değişkenin değeri 0 ise bu kural uygulanmaz.
etc/tcp.smtp dosyasına

192.168.0.2:allow,RELAYCLIENT="",GMFCHECK="0"
:allow,GMFCHECK="0"

İkinci satır olmazsa dışardan mail alamazsınız.

Gelen postalarda spam engelleme

Gelen spamların çoğu (%80) yetkisiz adreslerden gönderilmiştir.
Yetkili / Yetkisiz adres tanımı smtp protokolünde yoktur.

SPF (Sender Policy Framework): Bir domain adına posta gönderebilecek IP adreslerini belirleyen bir standarttır. RFC 4408 de tanımlanmıştır. Ters MX kaydı olarak da gösterilebilir.

DNS protokolünün pek kullanılmayan TXT kaydını kullanır. Örnek TXT kaydı:

v=spf1 ip4:193.140.151.0/24 a mx ptr -all

Gönderen adresin SPF kaydı yok ise

Çoğu alan isimlerinin SPF kayıtları yoktur.
Ancak bu alan isimleri için SPF tahmini yapabiliriz.

IP adresleri kurumlara büyüklüklerine göre B veya C sınıfı olarak dağıtılmaktadır.

Dolayısıyla posta gönderdiği IP adresi ile MX veya A kayıtlarının aynı C veya B sınıfı içinde olma olasılığı çok yüksektir.

Bu nedenle karşılaştırmayı B sınıfı adresleri dikkate alarak yapabiliriz.

Programın çalışma mantığı

Program kişiye özel çalıştığından kişinin postakutusu dizinindeki (~vpopmail/domains/alan_ismi/kisi_ismi) “.qmail” dosyası düzenlenir.

Programda olabilecek hatalara karşı gelen posta önceden güvenli bir yere alınır. “./Maildir2/”

Sonra gelen posta program tarafından işlenir. Eğer “spamdır” sonucu çıkarsa 99 çıkışı; “doğrudur” sunucu çıkarsa 0 çıkışı ile sonlanır.

Son satırda da normal postakutusu dizini yer alır. “./Maildir/”

.qmail dosyası içeriği

```
##########
./Maildir2/
|/vpop/prog/spf/ds91
#|/usr/local/bin/spamcheck4
./Maildir/
##########
```

Maildir2: karantina dizinidir. Belli aralıklarla eski postalar silinmelidir.
ds91: C ile yazılmış programın derlenmiş hali.
spamcheck4: bash betiği ile yazılmış program
Maildir: Normal posta kutusu

Alıcının bilgilendirilmesi

Spam engelleme programlarının en büyük sorunu “yanlış alarm” olarak da isimlendirebileceğimiz gibi spam olmayan bir postanın spam olarak belirlenmesidir.

Program spam olarak belirlediği postaların gönderildiği adresleri, tarihi ve gönderdiği IP adresini bir dosyada biriktirir: SPAM_POSTA
Gün sonunda bu dosyada biriken adresler bir posta ile alıcıya iletilir.

Alıcı, bu adresler içinde spam olmadığını düşündüğü adresi bildirerek bir gün gecikmeyle ilgili postaya ulaşabilir.

Spam bilgisi

Aşağıdaki adreslerden gönderilen postalar SPAM olarak değerlendirilip size ulaştırılmamıştır.

2007-1-25 7:11 220.172.224.156 caracasjeo@holbrookelectric.com
2007-1-25 7:24 217.128.129.80 ccb@airaction-northampton.co.uk
2007-1-25 11:14 189.139.19.231 miriamtricia@frueherziehungsdienst.ch
2007-1-25 11:38 24.154.50.21 uent@chlazenivlk.cz
2007-1-25 12:1 81.183.168.250 scripturaljo@eris.qinetiq.com
2007-1-25 12:12 70.110.91.131 piynyfun@verizon.net
2007-1-25 12:13 202.155.149.154 bjfsatoe@jfsato.com
2007-1-25 13:46 58.88.115.17 cclp@0733.com
2007-1-25 14:56 82.101.137.6 bcontinentalpapere@continentalpaper.com
2007-1-25 15:5 211.9.167.152 rlmuqxhkhqid@eva.ro
2007-1-25 15:7 84.47.191.219 tkcatwi@mortgagerefi.com
2007-1-25 15:8 125.235.37.222 daniel@trader.com
2007-1-25 15:32 82.144.64.36 qmg20kwe@pentaphise.com
2007-1-25 17:56 212.195.240.61 cmjzpi@masonnationalbank.com

Programın yapısı

Program gelen postanın sadece başlık kısmına bakar.
Başlık kısmında gönderen adres, gönderen IP ve gönderen makine ismi bilgilerini alır.
Örnek başlık:

Return-Path: <uthe1rimvt@mac.com>
Delivered-To:
Received: (qmail 25059 invoked by uid 60010); 29 Jan 2007 12:16:40 -0000
Delivered-To: deu.edu.tr-root@deu.edu.tr
Received: (qmail 25039 invoked from network); 29 Jan 2007 12:16:40 -0000
Received: from unknown (HELO altay.adm.deu.edu.tr) (193.140.151.84)
  by kordon.adm.deu.edu.tr with SMTP; 29 Jan 2007 12:16:40 -0000
Received: (qmail 57150 invoked from network); 29 Jan 2007 12:18:24 -0000
X-Mail-Scanner: Scanned by qSheff 1.0 (http://www.enderunix.org/qsheff/)
Received: from unknown (HELO zyzytnoji) (82.149.3.75)
  by gelen.posta.deu.edu.tr with SMTP; 29 Jan 2007 12:18:22 -0000
To: <riti@deu.edu.tr>
Bcc: <riye.okumus@deu.edu.tr>, <rkabidin.ozturk@deu.edu.tr>, <rmaz@deu.ed
u.tr>, <rmizi@deu.edu.tr>, <rona@deu.edu.tr>, <root@deu.edu.tr>
Date: Mon, 29 Jan 2007 13:17:15 +0100
From: "Margurite Caren" <uthe1rimvt@mac.com>

Başlık bilgileri

Return-Path: <uthe1rimvt@mac.com>

Bu satırda gönderen adres yeralmaktadır. Qmail bu adresi SENDER çevre değişkeninde tutar.

gelen.posta.deu.edu.tr : Dışardan gönderilen postayı ilk karşılayan makinedir.
Bunun konuştuğu IP ve makine ismi gönderen IP ve makine ismidir.

Received: from unknown (HELO zyzytnoji) (82.149.3.75)
Makine ismi (hostname): zyzytnoji
IP: 82.149.3.75

Yetkili IP tespiti

Gönderen IP adresinin yetkili olup olmadığına djbdns araçları ile bakılır.
dnstxt: TXT kayıtlarını getirir.
dnsmx: MX kayıtlarını getirir.
dnsip: A kayıtlarını getirir.

Bulunan IP adreslerinin ilk iki hanesi alınır ve gönderen IP adresinin ilk iki hanesi ile karşılaştırılır.
Aynı ise doğru postadır.
Farklı ise spam postadır.

DNS sorgularını hızlandırmak

Tekrar tekar aynı DNS sorgularını yapmak yerine, bulunan DNS kayıtlarını dosyalarda veya veritabanında tutulabilir.

Çünkü DNS kayıtları B sınıfı açısından bakıldığında nadiren değişmektedir.

Yetkili IP için önce dosya veya veritabanına bakılır. Kayıt yoksa DNS sorgularına bakılır.

Programın derlenmesi

Program veritabanı olarak mysql kullanmakta, dns sorgularını da djbdns kütüphanesi ile yapmaktadır. Djbdns kütüphanesinin adresi
http://smarden.org/pape/djb/manpages/djbdns-pd-1.05.tar.gz

Solaris 10 için:
#gcc -L/lib -ldjbdns -lmysqlclient -lresolv -I/ usr/local/include/libdjbdns/ -o ds91 ds91.c

FreeBSD için:
gcc -L/lib -ldjbdns -lmysqlclient -I/usr/local/include/libdjbdns/ -o ds91 ds91.c

Kaynaklar

1. Bash betiğinin adresi
http://web.deu.edu.tr/~devrim/spamcheck4

2. C programının adresi
http://web.deu.edu.tr/~devrim/ds91.c

3. Bu belgenin adresi:
http://web.deu.edu.tr/izmirunix/seminer/qspam.sxi