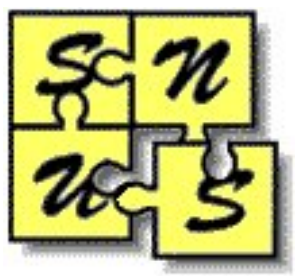
22 Oktober 2007

Stefan Görling, stefan@gorling.se



Låt oss börja positivt!

- *”The current period is characterized by the lack of any real new threats and an upswing in the commercialization of the virus writing environment.*
- *As I previously confirmed, the ball is now in our court - for the first time in many years, the antivirus companies have the upper hand.”*
- *- Kaspersky Labs*

Hur ser hoten ut?

- Trend: Parasiter skrivs av proffs
  - Maffiastrukturer
  - Företagsekonomisk logik
- Två typer av hot
  - Computer controlling
  - User controlling

Computer Controlling

- Parasiter som infekterar och tar kontroll över dator (BOTNets)
  - Affärsplattform för DDOS, Hemsidor, SPAM, Phishing, etc.
  - Fjärrstyrs via IRC eller P2P-nätverk
  - Konkurrens mellan olika "företag"
  - STORM anses störst idag mellan 1-10 miljoner datorer
  - Trots många datorer, fortfarande flaskhals.

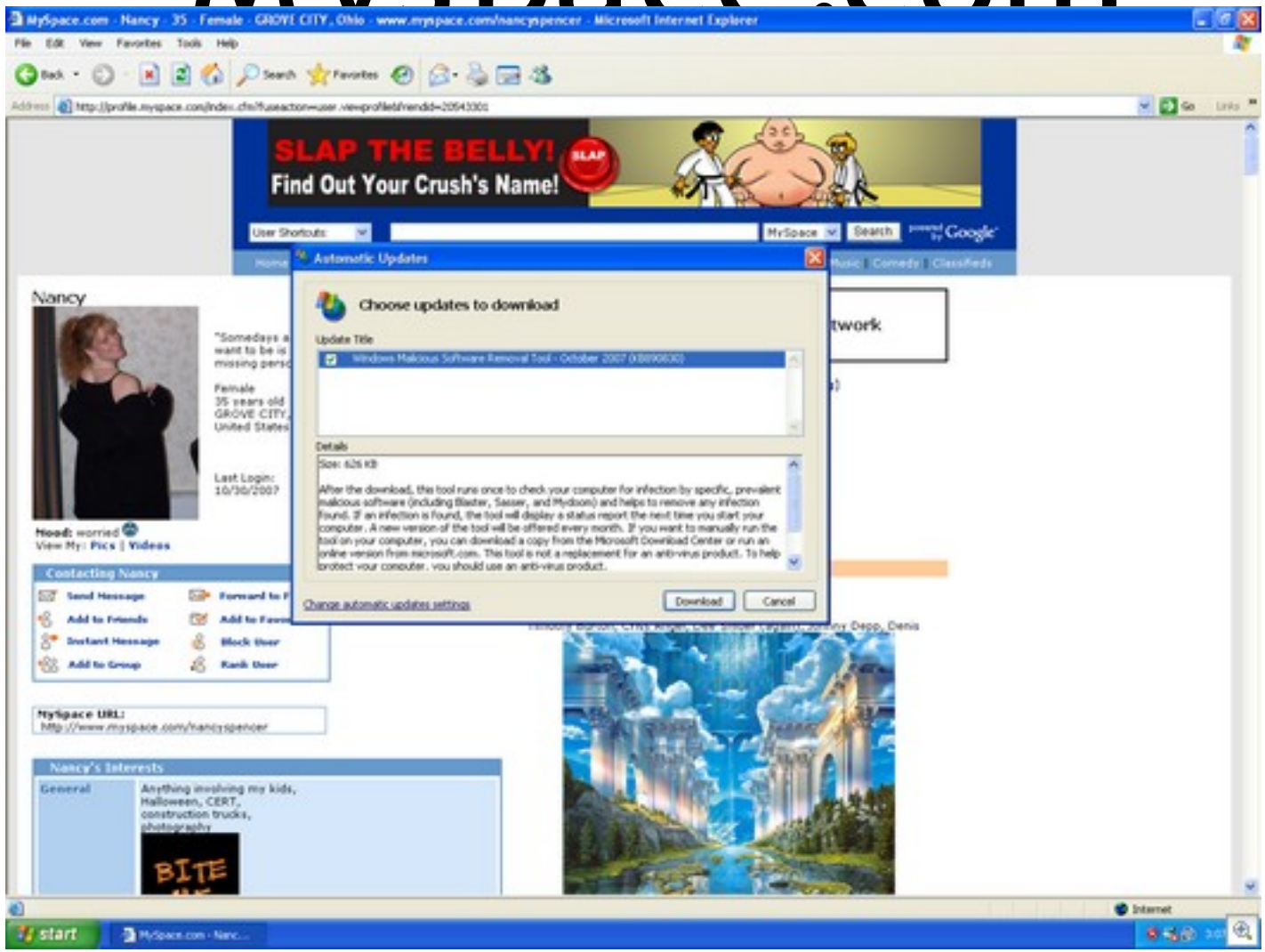
User Controlling

- Parasiter som försöker påverka användaren
  - Byter DNS-servrar för ökad kontroll
  - Skriver om Affiliate-programslänkar
  - Ser till att du går till Bokus istf. Adlibris

Två trender

- 1. Webbsmitta/attacker
  - Drive-by downloads
  - Siter hackas och inkluderar skadlig kod
  - Den skadliga koden genereras on-the-fly - Unika signaturer för varje användare.
- 2. Social-engineering istället för säkerhetshål
  - Lurar användaren att installera program (ex. VideoCodecs).
  - Eller lyssna på MP3:or... eller göra

Exempel: Myspace.com



Phishing

- Sverige 2007 - Nordeas år
- Negativt: Minskat förtroende för nättjänster
- Negativt: Kostnadsförluster och problem
- Positivt: Frågan på dagordningen, vi har (hade?) ett konkret problem att diskutera snarare än teoretiska vargar.

Angreppsätt

- Designa om SMTP
- Filtrering
- Öka transaktionskonstnaden
- Lagstiftning
- Blockera portar
- Avsändarautentisering

Avsändarautentisering

- Mål: Se till att
- Möjliggör verifikation av sändaren
- Minskar phishingproblematik
- Underlättar lokalisering av spammare

S tandarder

Standard/ Mechanism	Transparent to user	Standardized	Authentication	Content verification	Public/ Private key-based	Protects from phishing
OpenPGP	No	Yes, since 1996	Yes, to individual	Yes	Yes	No
S/MIME	No	Yes, since 1998	Yes, to individual	Yes	Yes	No
SPF	Yes	Yes, experimental 2006	Yes, to domain	No	No	Yes
DomainKeys /DKIM	Yes	No, working on draft	Yes, to domain	Yes	Yes	No

Utan SPF

GoodGuy.com

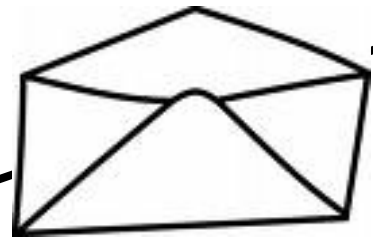
Utan SPF

Användare

GoodGuy.com

Utan SPF

Användare



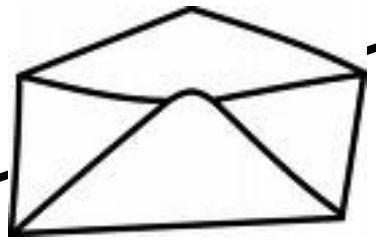
info@ goodguy.com

GoodGuy.com

Utan SPF

WOW! E-post från GoodGuy!

Användare



info@ goodguy.com

GoodGuy.com

Utan SPF

GoodGuy.com

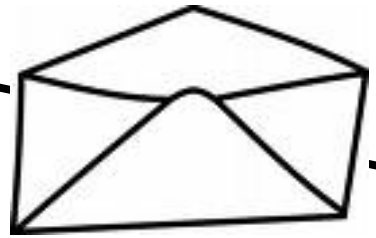
Utan SPF

GoodGuy.com

Användare

Utan SPF

GoodGuy.com

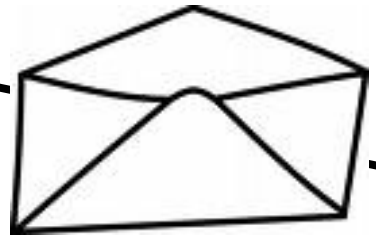


info@ goodguy.com

Användare

Utan SPF

GoodGuy.com



info@ goodguy.com

Användare

WOW! E-post från GoodGuy!

MedSPF

GoodGuy.com
10.10.10.1

Med SPF

GoodGuy.com
10.10.10.1

Användare

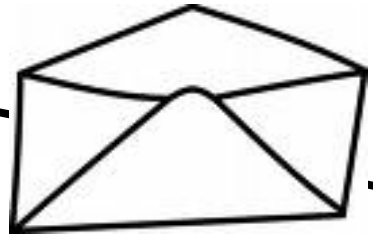
Med SPF

GoodGuy.com
10.10.10.1

Användare

Med SPF

GoodGuy.com
10.10.10.1

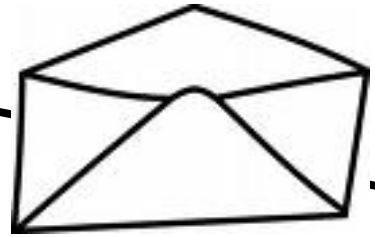


info@ goodguy.com

Användare

Med SPF

GoodGuy.com
10.10.10.1

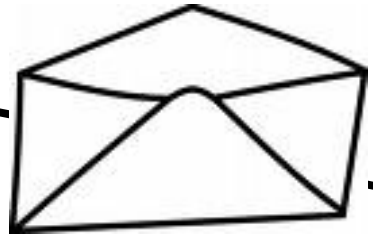


info@ goodguy.com

Användare

Med SPF

GoodGuy.com
10.10.10.1



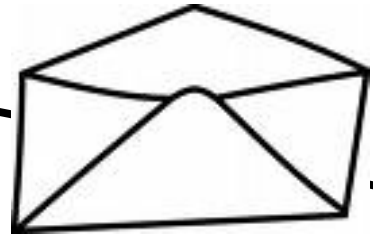
info@ goodguy.com

Användare

DNS -Server

Med SPF

GoodGuy.com
10.10.10.1



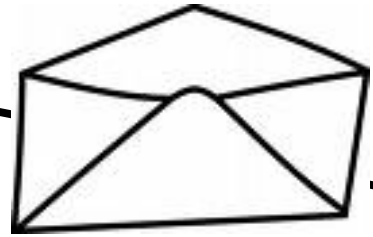
info@ goodguy.com

Användare

DNS -Server

Med SPF

GoodGuy.com
10.10.10.1



info@ goodguy.com

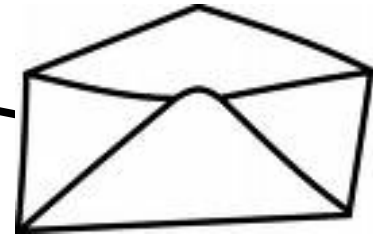
Användare

DNS -Server

- GoodGuy.com: IN TXT “v=spf1 ipv4: 50.50.50.1 -all"

Med SPF

GoodGuy.com
10.10.10.1



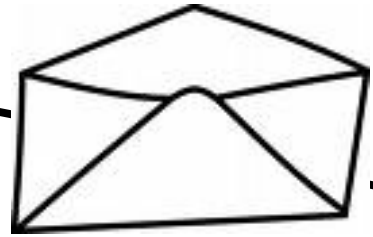
info@ goodguy.com

DNS -Server

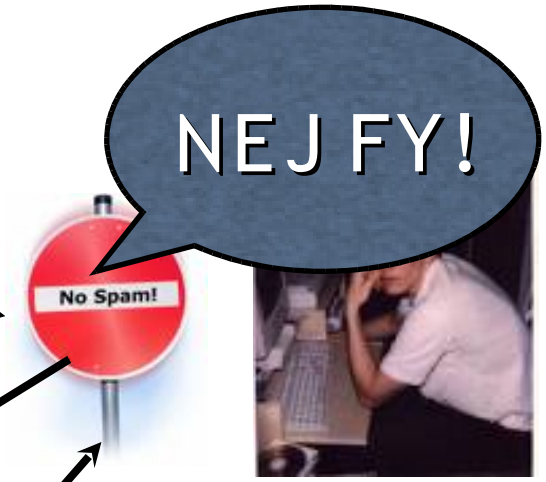
- GoodGuy.com: IN TXT “v=spf1 ipv4: 50.50.50.1 -all"

Med SPF

GoodGuy.com
10.10.10.1



info@ goodguy.com



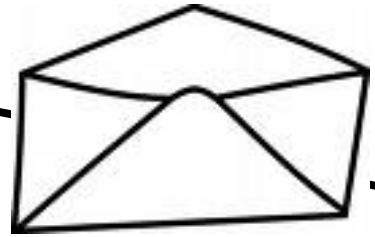
Användare

DNS -Server

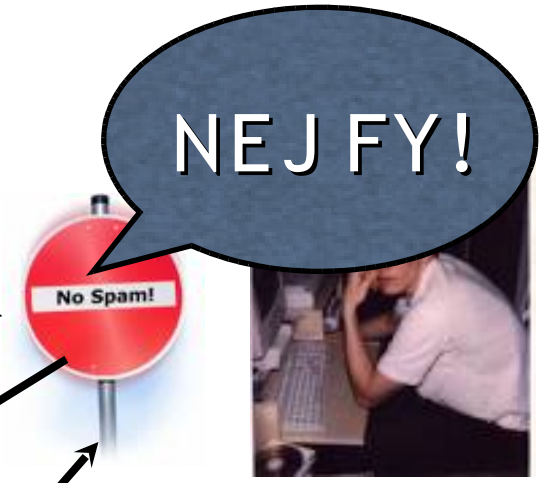
- GoodGuy.com: IN TXT “v=spf1 ipv4: 50.50.50.1 -all"

Med SPF

GoodGuy.com
10.10.10.1



info@ goodguy.com



Användare

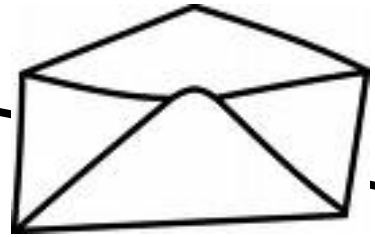
DNS -Server

- GoodGuy.com: IN TXT “v=spf1 ipv4: 50.50.50.1 -all"

Papperskorg

Med SPF

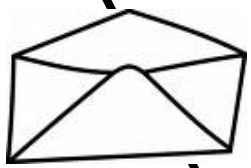
GoodGuy.com
10.10.10.1



info@ goodguy.com

Användare

DNS -Server

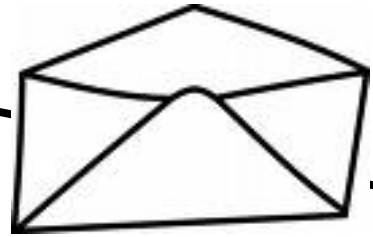


Papperskorg

- GoodGuy.com: IN TXT “v=spf1 ipv4: 50.50.50.1 -all"

Med SPF

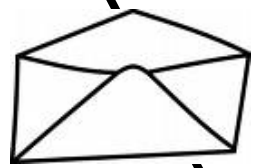
GoodGuy.com
10.10.10.1



info@ goodguy.com

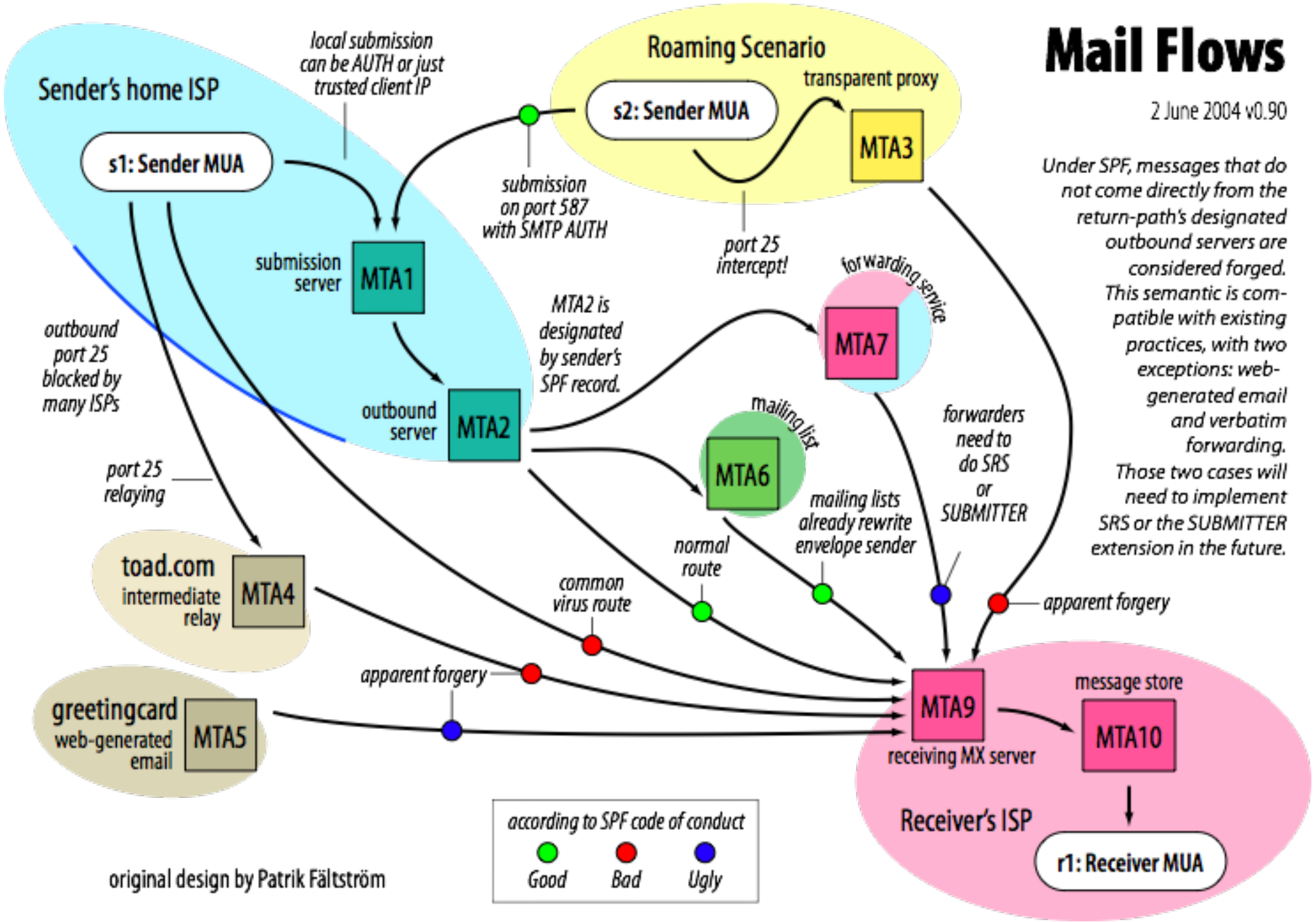
Användare

DNS -Server



Papperskorg

- GoodGuy.com: IN TXT “v=spf1 ipv4: 50.50.50.1 -all"


Mail Flows
2 June 2004 v0.90
Under SPF, messages that do not come directly from the return-path's designated outbound servers are considered forged. This semantic is compatible with existing practices, with two exceptions: web-generated email and verbatim forwarding. Those two cases will need to implement SRS or the SUBMITTER extension in the future.
Sender's home ISP
s1: Sender MUA
local submission can be AUTH or just trusted client IP
submission server
MTA1
outbound server
MTA2
outbound port 25 blocked by many ISPs
port 25 relaying
Roaming Scenario
s2: Sender MUA
transparent proxy
MTA3
submission on port 587 with SMTP AUTH
port 25 intercept!
MTA2 is designated by sender's SPF record.
forwarding service
MTA7
mailing list
MTA6
forwarders need to do SRS or SUBMITTER
mailing lists already rewrite envelope sender
normal route
common virus route
apparent forgery
toad.com
intermediate relay
MTA4
greetingcard
web-generated email
MTA5
apparent forgery
MTA9
receiving MX server
message store
MTA10
Receiver's ISP
r1: Receiver MUA
according to SPF code of conduct
Good
Bad
Ugly
original design by Patrik Fältström

Glossary

DNSBL: an IP-based blacklist.
RHSBL: a domain-name blacklist, conceptually superior to DNSBLs, but less used today due to sender forgery. *(see SPF)*
SPF: an anti-forgery mechanism

Envelope sender *vs* header From

The envelope of an SMTP transaction is the stuff that comes before DATA. After DATA you get the message headers and body.

This is the envelope sender, also known as the return-path. SPF tests the domain of the envelope sender. If a message has a blank sender (MAIL FROM: <>), it could be a legitimate mailer-daemon bounce, or it could be a spam trying to look like one. Then SPF falls back to the hostname given in the HELO command.

This is the "From:" header. SPF does not look at the header "From:". Most mailing lists preserve the original "From:" address, but change the envelope sender to the special owner address which handles bounces. It would be wrong for SPF to examine this "From:" address. Besides, SPF's authorized sender mechanisms operate well before the header is transmitted, so this would come too late anyway.

Anatomy of an SMTP+SPF transaction

The moment an SPF-enabled MTA receives MAIL FROM, it can perform anti-forgery tests. If the tests fail, the MTA can assume the payload is probably a worm, virus, or spam without even looking at the payload DATA. If SPF tests pass, other tests (eg. RHSBLs) can be used with greater confidence. SPF makes the RHSBL a more powerful antispam tool.

at each SMTP stage...	... an SPF-enabled MTA can perform certain actions
connection to port 25	the MTA knows the client IP and thus the PTR name.
HELO *hostname*	if the *sender* (below) is empty, SPF uses *hostname* instead.
MAIL FROM: <*sender*>	SPF runs. If the transaction looks forged, an MTA can reject it right away, or prepend a header for later processing. If the transaction is not forged, the MTA should still perform other tests, such as RHSBLs.
RCPT TO: <*recipient*>	If all tests pass, the transaction proceeds.
DATA	Most domains that publish SPF use it to describe the hosts permitted to send mail from that domain, so forgeries can be rejected at MAIL phase. But some domains may prefer to use S/MIME, PGP/GPG, Habeas, or some other authentication mechanism which puts credentials in the headers or message body. Those domains still need to declare that messages without those credentials should be rejected. SPF supports such declarations also, even though they are less common.
message header *Received-SPF: fail* *From: email@address*	Some SPF-enabled MTAs prepend a Received-SPF header indicating the result, for later filters to use.
message body *Maybe there's PGP or S/MIME here. Parsing bodies is slow and costly.*	

Exempelpolicy

- bigbank.com: IN TXT “v=spf1 mx
- a:office.bigbank.com/28 -all"

Vanliga motargument

- Löser inte spamproblemet
- Anses inte vara tekniskt vacker - TXT records i DNS
- Kräver DNS-SEC för att vara helt säker
- Kräver att mail ska skickas från vissa servrar - anses vara fel
- Fungerar inte bra för automatisk forwarding

Fördelar

- Adresserar phishingproblematik
- Enkel att implementera
- Finns redan implementerat i de vanligaste spamfilterprogramvarorna
- Fungerar, gör världen lite bättre
- Kanske inte lämpligt för alla organisationer, men mycket viktigt för många

Implementering i Sverige

- Hittills mycket lite intresse
- Nu inför storbankerna SPF
- 16 % av myndigheterna efter gårdagens rapport
- Nästa steg är att få mailoperatörer att aktivera filtreringen.

Tack!

- Kontakt: stefan@gorling.se
- http://www.gorling.se/