Mail e Security

Incontri di GARR-B

Claudio Allocchio

Luca dell'Agnello

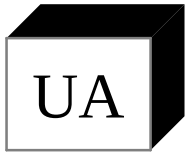
Claudio.Allocchio@garr.it

Luca.dellAgnello@garr.it

Sommario

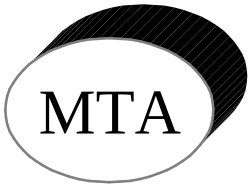
- Servizio Mail: concetti e servizi di base...
- ... e "ricevute" (DSN, MDN)
- La sicurezza: SPAM, Privacy, Virus, Hoaxes...
- Lo stato del software
- Come proteggersi: configurazioni, filtri, firewall
- Problemi? Come intervenire
- Prevenzione: come informare e educare l'utenza

User Agent (UA)



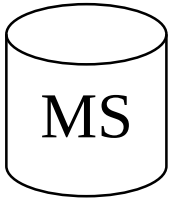
- Cosa fa in tramissione:
  - Interagisce con l'Utente (interfaccia testo o grafica)
  - Codifica il messaggio (con formato A)
  - Trasmette il messaggio (ad un MTA di solito predefinito)
- Cosa fa in ricezione:
  - Riceve il messaggio (da un MS di solito predefinito)
  - Decodifica il messaggio (con formato A)
  - Presenta il messaggio all'Utente (interfaccia testo o grafica)
  - Interagisce con l'Utente (risposta, archiviazione, ...)

Message Transport Agent (MTA)



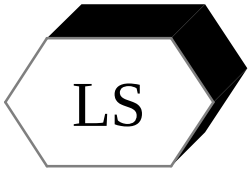
- Cosa fa:
  - Riceve il messaggio (da un UA o da un MTA)
  - Esamina le informazioni di Routing (da database locali o distribuiti)
  - Trasmette il messaggio (ad un altro MTA o da un mailbox server)

Mailbox Access Server (MS)



- Cosa fa:
  - Riceve il messaggio (da un MTA)
  - Trasmette il messaggio (ad uno UA)
  - Agisce sul database messaggi (su comandi di uno UA)

List Server (LS)



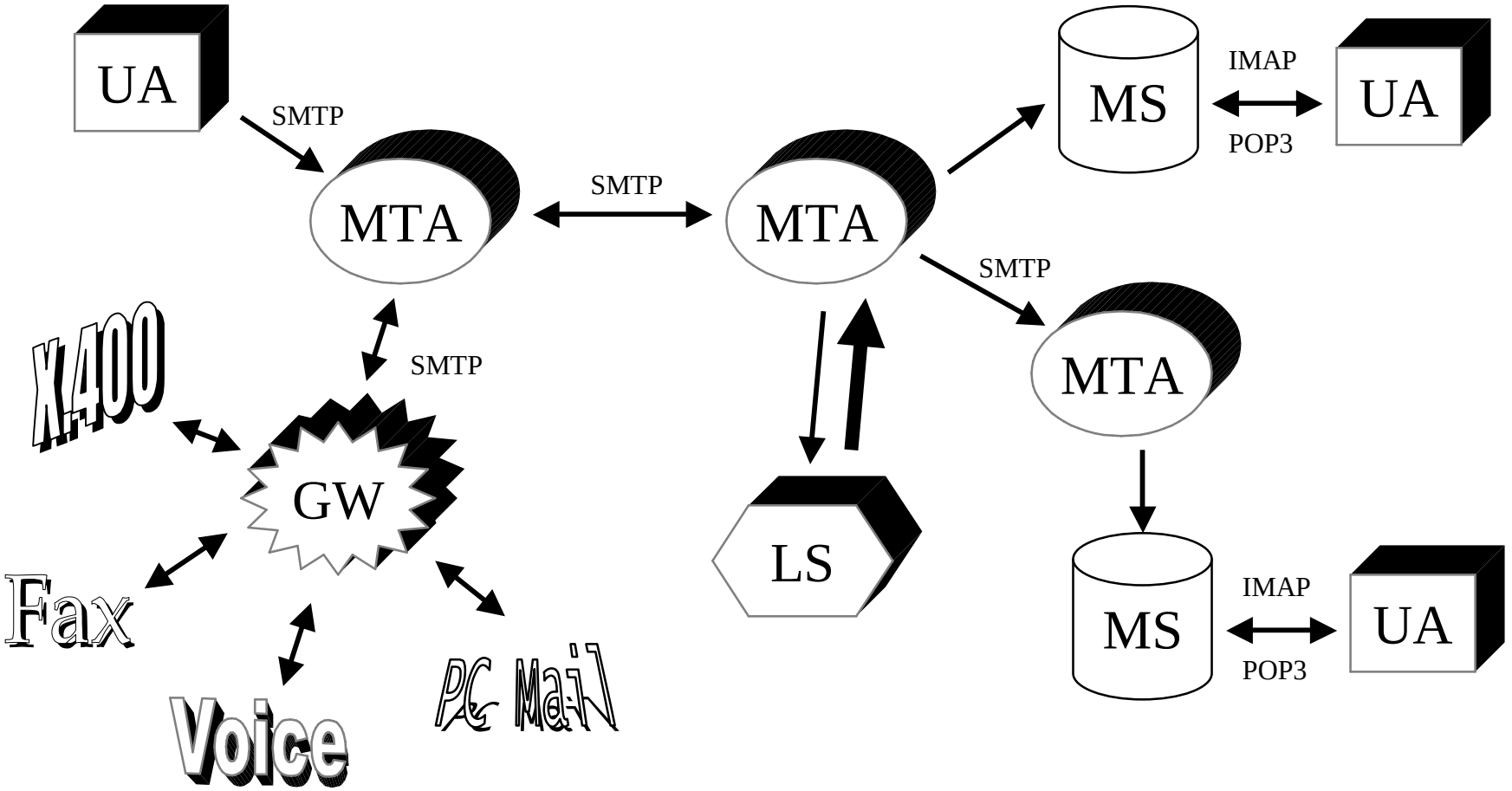
- Cosa fa:
  - Riceve il messaggio (da un MTA)
  - Decodifica il messaggio (come uno UA)
  - Esamina il database di distribuzione (iscritti alla lista)
  - Codifica il messaggio in N copie (come uno UA)
  - Trasmette il messaggio (al proprio MTA)

Mail Gateway (GW)

- Cosa fa:
  - Riceve il messaggio (da un MTA con mail protocol A)
  - Decodifica il contenuto (come uno UA con formato A)
  - Codifica il contenuto (come uno UA con formato B)
  - Trasmette il messaggio (ad un altro MTA con mail protocol B)

Mail Transport Service

MTS Globale Internet



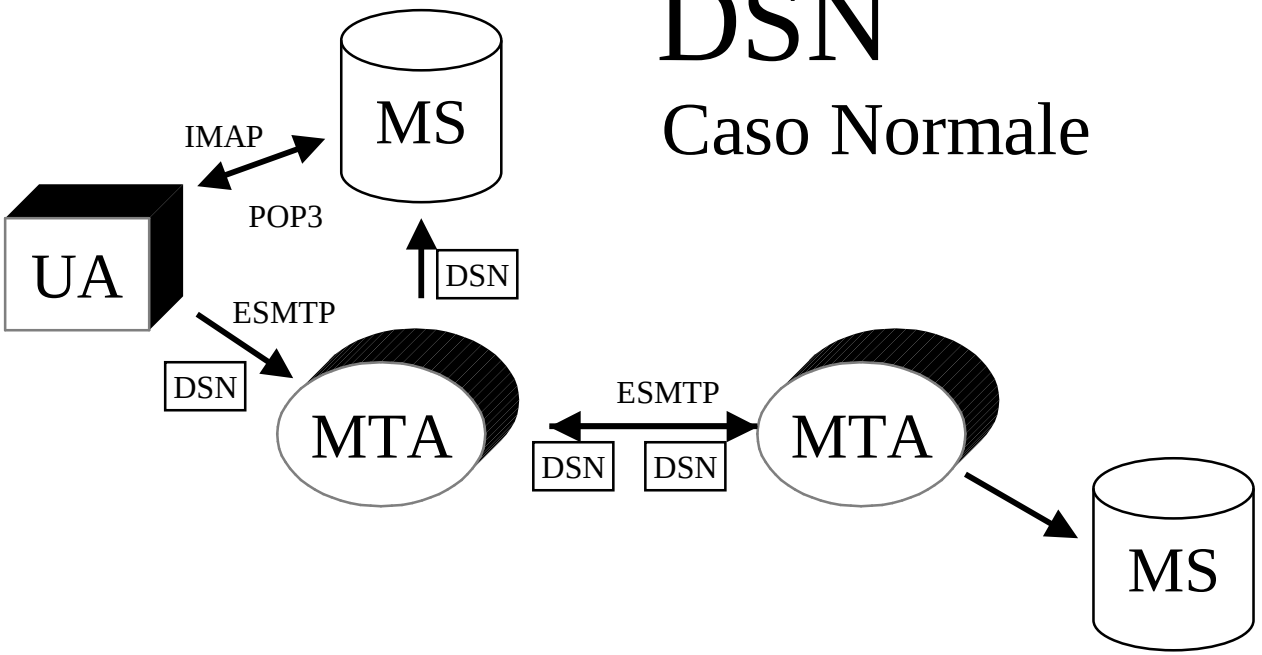
Delivery Status Notification (DSN)

DSN

- Ricevuta inviata al mittente quando viene scritto il messaggio nel MS del destinatario
- NON e' disabilitabile
- E' un formato STANDARD predefinito
- Non tutti gli UA ne permettono la richiesta
- Non tutti gli MTA, GW, LS la supportano

DSN

Caso Normale

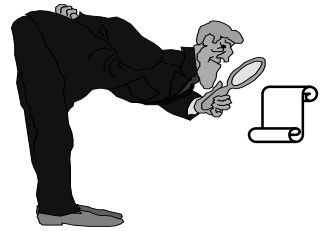


... Il Destinatario NON interviene!

Message Delivery Notification (MDN)

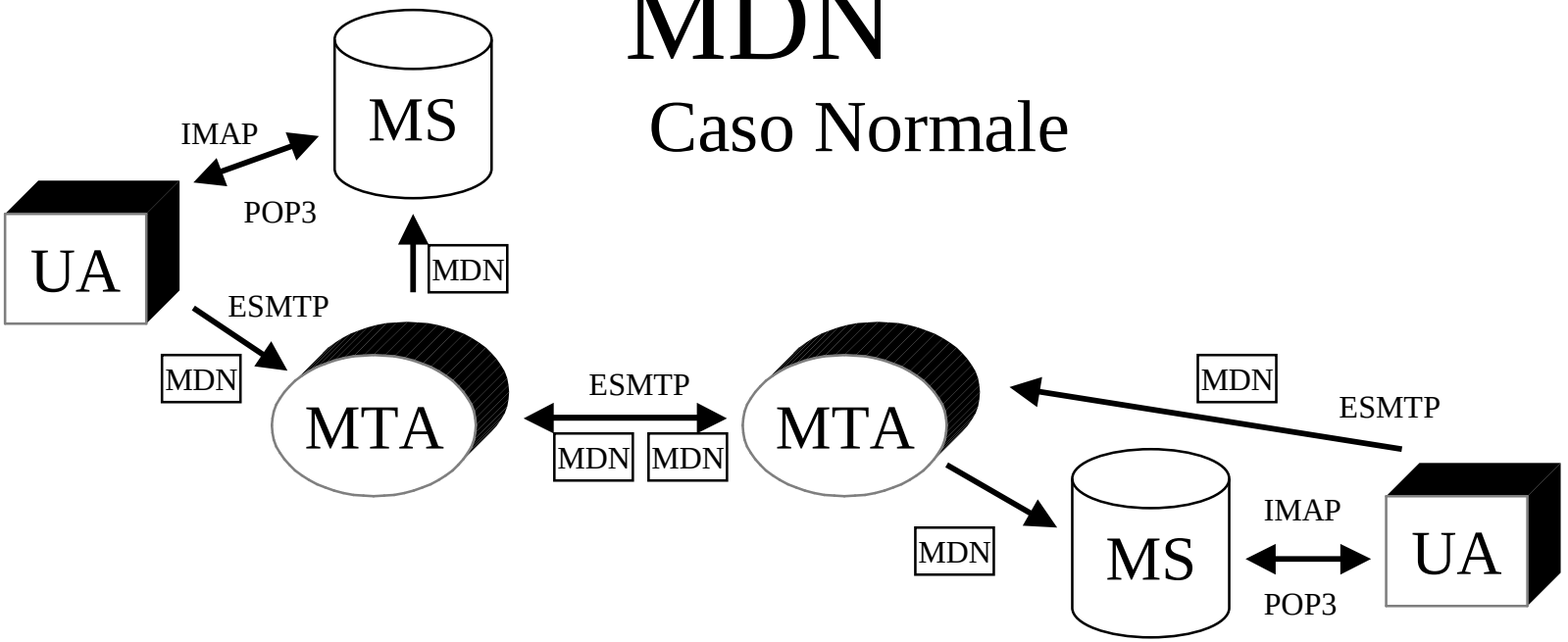
MDN

- Ricevuta al mittente che viene inviata su azione del "lettore" sul messaggio dentro il MS
- E' disabilitabile
- E' in formato STANDARD predefinito
- Non tutti gli UA ne permettono la richiesta
- Non tutti gli UA (e simili) e MTA la supportano



MDN

Caso Normale



...MDN generata dall'azione
del Destinatario (umano e/o software) !

Security: i Principi

- Impedire cattura delle password (peeking)
- Impedire lo SPAM
- Identificare sorgenti di attacco
- Proteggere le LAN dall'esterno
- Garantire autenticita' del mittente
- Garantire integrita' e/o riservatezza del messaggio

Password Peek

- Autenticazione Client-Server: password in chiaro
- Installare SSL, anche e soprattutto sulle LAN
- Utilizzare Client-Server con supporto SSL oppure utilizzare il tunnel SSL
- Proteggere il LOG files del Server (POP o IMAP)

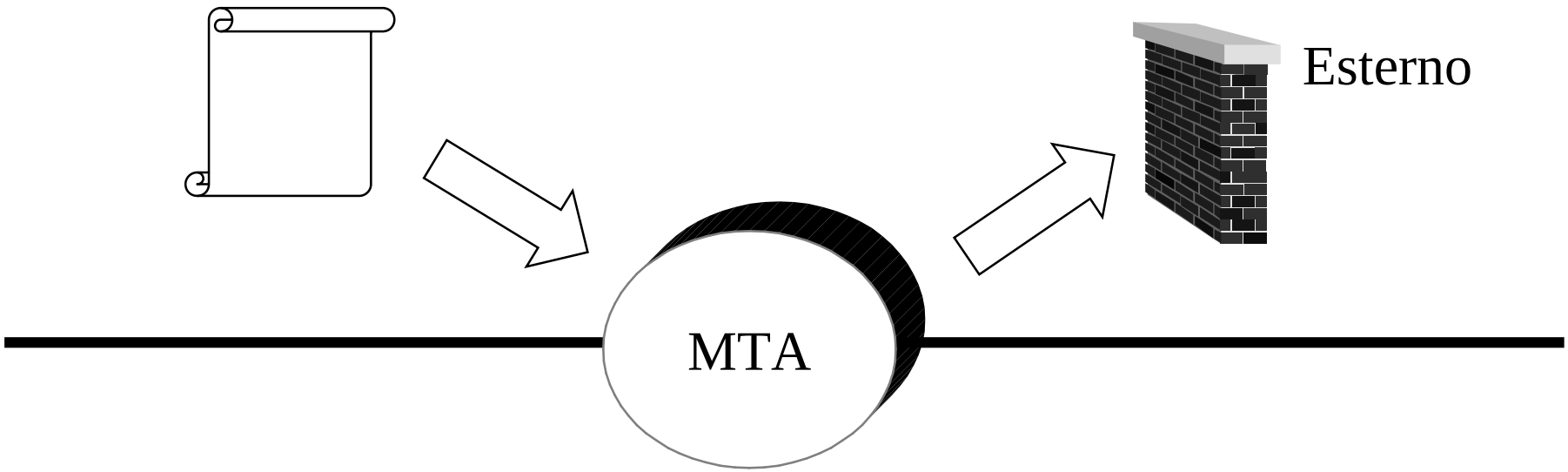
SPAM

- Invio di migliaia di messaggi a "spese altrui": MTA e risorse di rete (banda)
- Utilizzo di account gratuiti (AOL, Compuserve, msn, hotmail, tin, libero, tiscali,...)
- Utilizzo di software "per spamming"
- Spamming "ingenuo"
- La legge e lo SPAM: DL 185/99

Tipologie di mail spam

- Classico: "unauthorized mail relaying"
- Delitto Perfetto: "doppio non delivery"
- Attacco Diretto: "forged e-mail address"

Classico: Relay non autorizzato



Cosa e' "Interno" ?

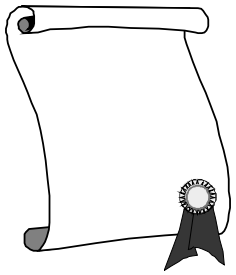
- il dominio e' uno dei propri domini
- l'indirizzo IP dell'host e' locale
- l'indirizzo IP e' un IP autorizzato
- LHS o mail address autorizzato
- IP --> nome corrisponde con PTR RR
- ...ma NON basta!

Mittente "Interno"

- Se indirizzo IP e' locale e dominio e' locale
- Se indirizzo IP e' locale e dominio e' remoto
- Se indirizzo IP e' locale e non c'e' dominio

e' piu' difficile falsificare l'indirizzo IP del mittente se non si appartiene alla LAN locale, quindi...

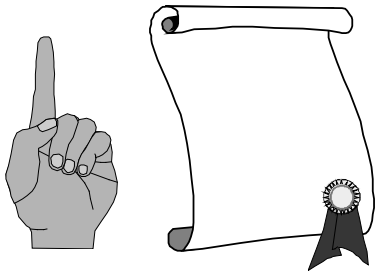
AMMESSO tutto il relay per tutte le destinazioni



Mittente "Esterno"

- Se indirizzo IP e' remoto e dominio e' remoto
- Se indirizzo IP e' remoto e non c'e' dominio

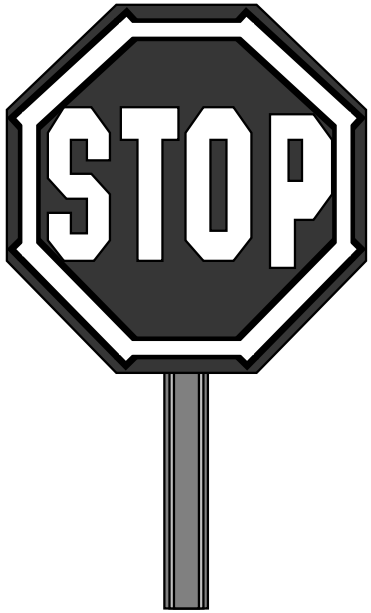
AMMESSO tutto il relay solo per le destinazioni LOCALI



Mittente "Falsificato"

- Se indirizzo IP e' remoto e dominio e' locale

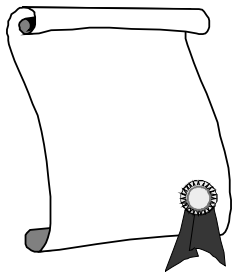
RIFIUTA QUALSIASI DESTINAZIONE !!



Destinatario "Interno"

- Se il dominio e' locale o tra i domini "MX"

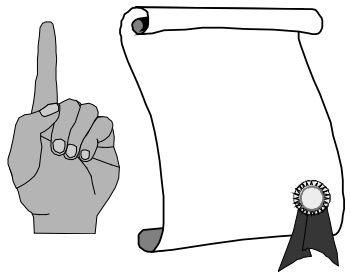
ACCETTA sempre il messaggio per la consegna.



Destinatario "Esterno"

- Se il dominio NON e' locale o NON e' tra i domini "MX"

ACCETTA il messaggio per la consegna SOLO se il mittente e' "interno".



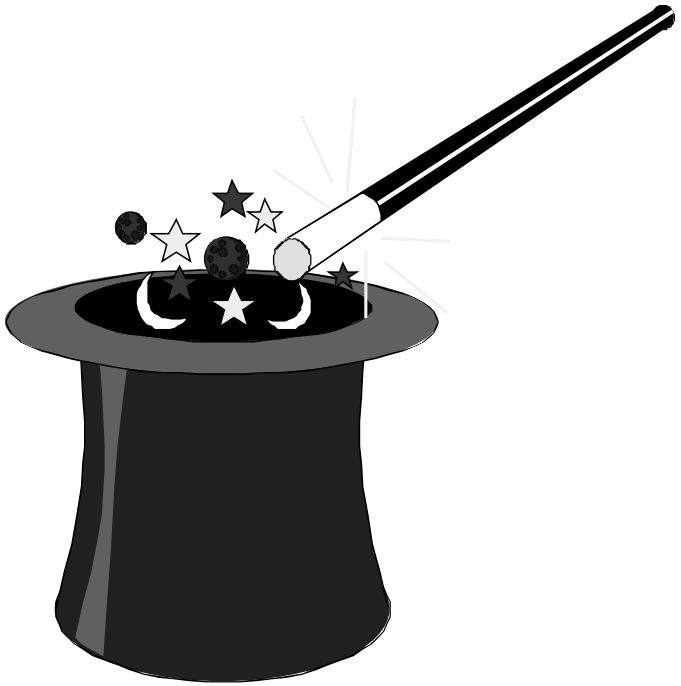
Esempio di Filtri - 1

Elenco domini "locali":

- trieste.infn.it
- ts.infn.it
- elettra.trieste.it

Elenco indirizzi IP "locali":

- 140.105.6.0



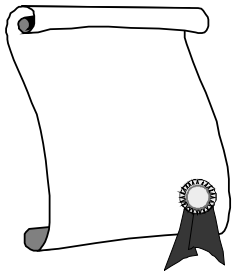
Esempio di Filtri - 2

indirizzo mittente:

Mario.Rossi@ts.infn.it

IP mittente:

140.105.6.93



Mittente "locale" OK, puo' spedire dovunque.

Esempio di Filtri - 3

indirizzo mittente:

Carlo.Bianchi@elettra.trieste.it

IP mittente:

140.104.4.3

Mittente NON "locale", puo' spedire solo a destinatari "locali".

Esempio di Filtri - 4

indirizzo mittente:

Jack.Spam@ts.infn.it

IP mittente:

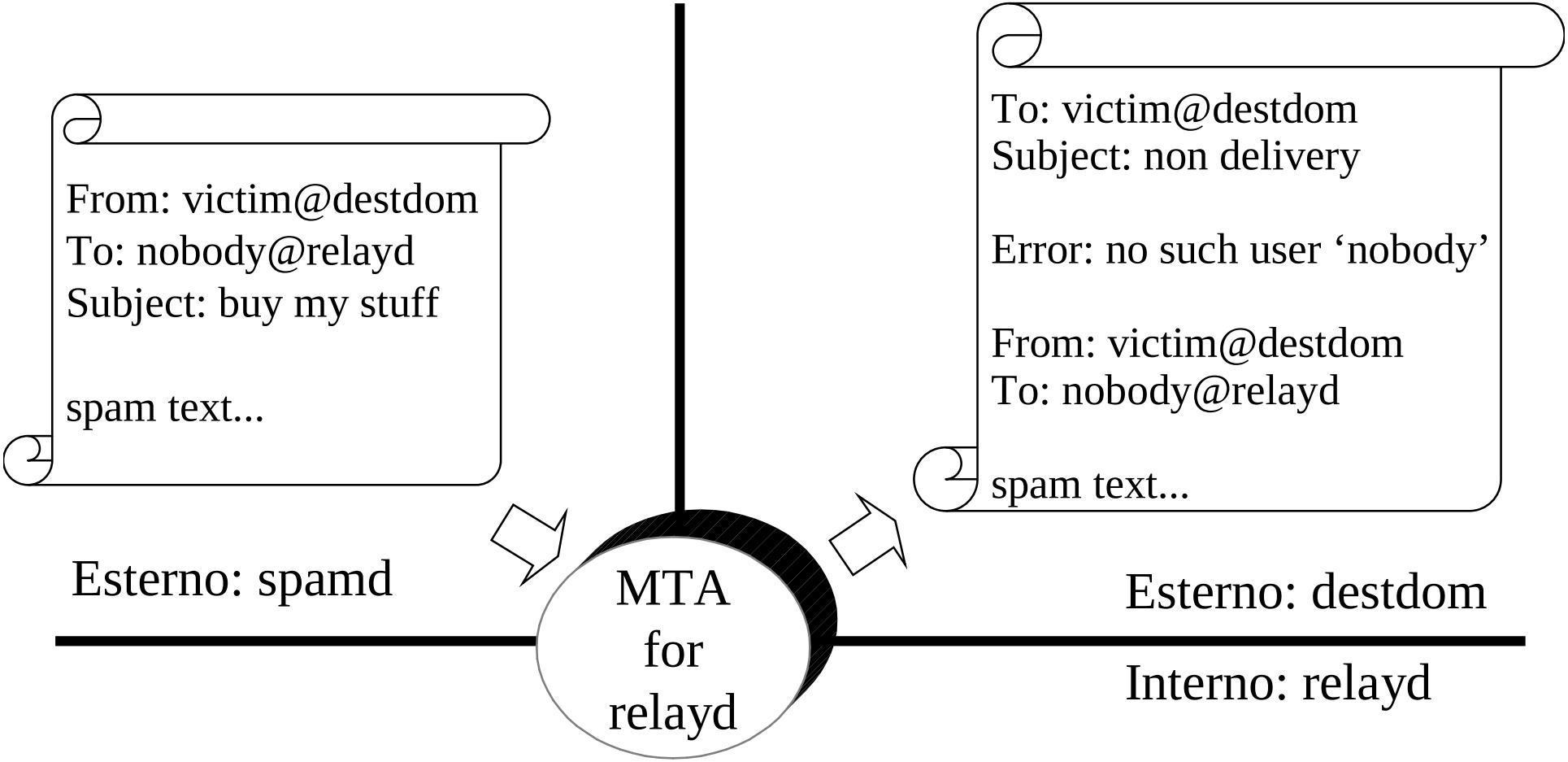
205.19.61.18

Mittente FALSIFICATO! non puo' spedire a nessuno

Caso Classico: considerazioni

- Il proprio MTA ha problemi:
  - potrebbe non essere la versione s/w corretta
  - potrebbe non avere i filtri corretti installati
  - potrebbe avere i filtri mal configurati
- E' un caso grave: segnalare al CERT e intervenire immediatamente!
- Quando si viene attaccati, si finisce subito nelle liste dei siti "vulnerabili": la situazione precipita !
- In caso di impossibilita' di intervento sul MTA, disabilitarlo o filtrarlo sui router!

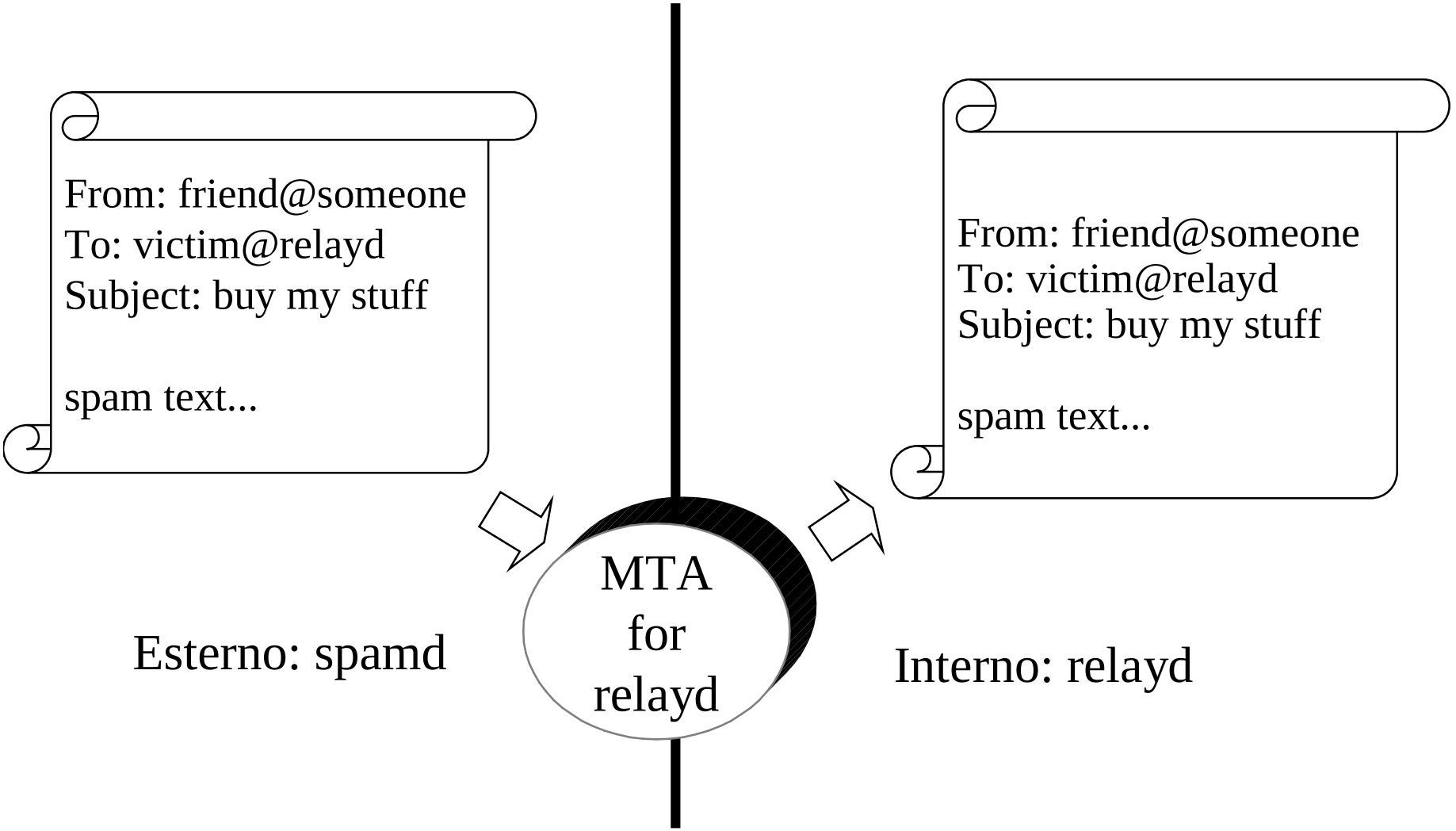
Delitto Perfetto: doppio non delivery



Delitto Perfetto: considerazioni

- I "filtri" non funzionano
- L'utente ha difficolta' a comprendere cosa succede
- Lascia "log files" apparentemente contraddittori
- Maschera meglio il mittente
- Spedisce un solo messaggio per volta
- Il proprio MTA e' innocente !
- Segnalare l'incidente al CERT

Attacco Diretto: forged sender



Attacco Diretto: considerazioni

- I "filtri" non funzionano
- Le vittime cercano di fare reply
- A volte il mittente e' un indirizzo esistente, ma del tutto estraneo allo spam
- Il proprio MTA e' innocente !
- Identificare quale MTA permette relay
- Segnalare l'incidente al CERT

SPAM "ingenuo"

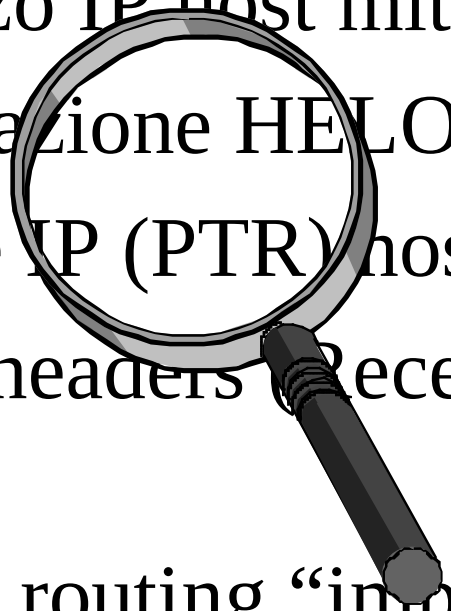
- Mittente "vero" !!
- Destinatario "vero" (la vittima)
- Il vostro MTA e' innocente !
- Messaggio "Unsolicited Commercial E-mail" (UCE)
- Messaggio "Chain Letter" (catena di S. Antonio)
- Segnalare l'attacco al CERT ed alla Naming Authority Italiana abuse@na.nic.it

La Legge e lo SPAM

- TUTTO lo SPAM e' vietato dalla Netiquette, obbligatoria per i domini del ccTLD "it"
- Le UCE sono vietate dalla legge: DL 185/99, articolo 10, con sanzione amministrativa da 1 a 10 Milioni di Lire

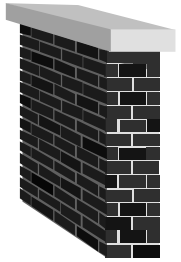
Identificare Sorgenti di Attacco

- registrare indirizzo IP host mittente
- registrare dichiarazione HELO / EHLO
- verificare reverse IP (PTR) host mittente
- conservare i full headers (Received, Message-id)
- depistaggio: mail routing "impossibili"

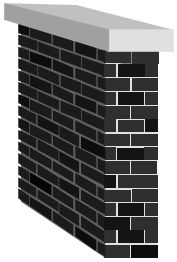


Protezione dagli Attacchi: MTA

- valutare filtraggio totale per indirizzo IP
- valutare filtraggio totale per dominio (vero)
- eventualmente inserimento in black list



Proteggere le LAN



- sui router permettere SOLO l'accesso verso i mailer interni protetti
- sui router eventualmente permettere l'accesso verso l'esterno SOLO ai mailer interni autorizzati e protetti

Firma Elettronica: autenticita'

- Firmare i messaggi spediti
- garanzia sull'identita' del mittente
- garanzia sull'integrita' del messaggio
- PGP: (uso "manuale", script o plug-in) - adatto a gruppi ristretti o ben organizzati di utenti
- S/MIME (integrato negli UA, standard) - richiede infrastruttura, scala molto bene

Firma Elettronica: riservatezza

- impedire la lettura dei propri messaggi a terzi
- coesistenza con "autenticita'"
- PGP
- S/MIME

Virus, Hoax e Leggende

- I virus via mail NON esistono (PenPal greetings... HOAX)
- solo casi estremamente particolari (bug in certi UA/MTA)
- esistono i virus nei FILES
- i files viaggiano come attachment...
- ... quindi via mail attachments POSSONO arrivare virus
- Comportarsi con gli attachments come con i floppy sconosciuti!!!

Virus, Hoax e Leggende - 2

- I sistemi antivirus a livello MTA hanno problemi!
- NON configurare gli UA per l'apertura automatica!
- NON eseguire MAI un attachment: Salvarlo, esaminarlo con antivirus, e poi aprirlo!
- Non mandare mai ad altri attachments ricevuti da sconosciuti!
- ... insomma usare solo un po' di buon senso vale molto piu' di molti filtri complessi!

Stato del Software: MTA

- BSD Sendmail
- Mailer Proprietari (Netscape SuiteSpot, Qmail,...)
- Altri sistemi operativi: WNT, MacOS, OpenVMS

Stato BSD Sendmail 8.9.3

- Filtri anti-spam via "FEATURE"
- controllo via access_db
- DSN e MDN supportate
- ESMTP
- controllo via aliases_db

Stato MTA Proprietari

- filtri anti-spam non sempre adeguati o efficienti
- controllo via access list (non tutti gli MTA)
- supporto DSN, MDN (non sempre corretti)
- ESMTP
- controllo via alias files

Stato VMS Sendmail 1.6d

- filtri anti-spam (equivalenti a 8.9.3)
- controllo via access_db
- supporto DSN, MDN (con estensioni)
- ESMTP
- controllo via smtp_aliases.db

Stato MTA per WNT, MacOS

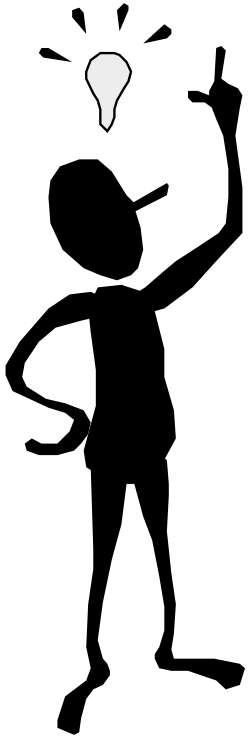
- alcuni basati su BSD sendmail, ma spesso versioni obsolete
- altri totalmente proprietari, ma non assicurano le protezioni/filtri necessarie
- il vero problema e' il supporto tecnico, spesso del tutto assente o inadeguato
- Se possibile NON usate questi sistemi operativi per MTA: meglio linux e BSD sendmail

Stato del software: UA

- PINE (dalla 3.91 in avanti, meglio 4.x)
- Netscape Comunicator 4.x
- Microsoft Outlook Express
- Eudora Pro
- Zmail Pro
- Pegasus Mail

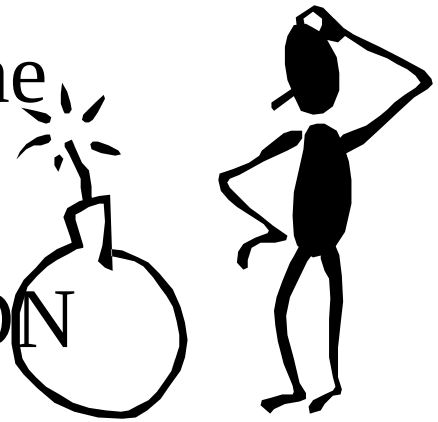
Stato di PINE, Eudora Pro, Zmail,...

- non supportano sessione off-line
- interfaccia e' spesso meno user friendly
- autenticazione dei mittente
- meno facilita' con gli attachment
- manca, a volte, richiesta DSN / MDN



Stato Netscape e Outlook

- stessa API --> stessi difetti !!
- problemi sincronizzazione on/off line
- spesso troppe finestre aperte insieme
- manca autenticazione dei mittenti
- manca, a volte, richiesta DSN / MDN
- molto user friendly per gli attachment
- configurazione default totalmente errata



Stato del software: MS

- IMAP4rev1 (public domain, commerciali)
- POP3 (commerciali)
- Message Store proprietari (commerciali)

Stato dei Mailbox Server

- Server IMAP4r1 (Unix, VMS Multinet 4.1b)
- Server POP3 (Unix, VMS Multinet 4.1b)

Stato dei Mailbox Server

- Servizi accesso POP3 e IMAP4 OK
- Servizi "disconnected" IMAP4 beta

Stato del software: GW

- Gateway con X.400 (Giveme2, PP)
- Gateway con FAX e Voice
- Gateway con PC Mail

Stato del software: LS

- Majordomo, ListServ, VLM
- Liste da "aliases"
- Liste da "files"

MTA: Sendmail

Requisiti

- server di posta centrale
- indirizzamento a dominio (RFC 822)
- raggiungibilita' utenti nome.cognome@dominio
- database utenti centralizzato
- spedizione consentita ai soli autorizzati

Componenti di Sendmail

- Sendmail - MTA
- mail.local - delivery locale
- makemap - utility per la costruzione dei database
- mailstats - statistiche di uso
- smrsh - shell sicura per sendmail

BSD Sendmail

Le istruzioni, esempi, macro, ed installation kit che seguono sono disponibili su

http://www.cert.garr.it/documenti/sendmail

Configurazione mailer generico: file domain.m4

divert(0)
VERSIONID('@(#)cnaf.infn.it.m4 8.2 (Berkeley) 4/21/95')

opzioni site-independent

define('confFORWARD_PATH', '$z/.forward.$w:$z/.forward')dnl
FEATURE(redirect)dnl
FEATURE(always_add_domain)
define('confPRIVACY_FLAGS', 'noexpn,needmailhelo,novrfy')
define('confMESSAGE_TIMEOUT', '5d/24h')

Configurazione mailer generico: file host.mc (1)

definizioni generali

divert(0)
include('../m4/cf.m4')
VERSIONID('@(#)relay.mc 8.2 (Berkeley) 8/6/95')

tipo di sistema operativo

OSTYPE(linux)dnl

Configurazione mailer generico: file host.mc (2)

definizione del dominio

DOMAIN(cnaf.infn.it)dnl
MASQUERADE_AS(cnaf.infn.it)
EXPOSED_USER(postmaster)
FEATURE(use_cw_file)dnl

definizione del file di alias

define('ALIAS_FILE', '/etc/aliases')

Configurazione mailer generico: file host.mc (3)

definizione del mail relay

define(`LUSER_RELAY', gandalf.cnaf.infn.it)dnl
define(`SMART_HOST', smtp:gandalf.cnaf.infn.it)dnl

shell sicura

FEATURE(smrsh)
define(`LOCAL_SHELL_PATH',`/usr/libexec/smrsh')

Configurazione mailer generico: file host.mc (4)

definizione dei mailer supportati

MAILER(local)dnl
MAILER(smtp)dnl

Configurazione mail server: file relay.mc (1)

definizioni generali

divert(0)
include('../m4/cf.m4')
VERSIONID('@(#)relay.mc 8.2 (Berkeley) 8/6/95')

tipo di sistema operativo

OSTYPE(linux)dnl

Configurazione mail server: file relay.mc (2)

definizione del dominio

DOMAIN(cnaf.infn.it)dnl
MASQUERADE_AS(cnaf.infn.it)
FEATURE(limited_masquerade)
EXPOSED_USER(postmaster)
FEATURE(use_cw_file)dnl

definizione del file di alias

define('ALIAS_FILE', '/etc/aliases')

Configurazione mail server: file relay.mc (3)

definizione del database utenti

define(‘confUSERDB_SPEC, ‘/etc/userdb.db’)dnl

definizione mail-hub

define(`MAIL_HUB', gandalf.cnaf.infn.it)dnl
FEATURE(relay_entire_domain)

shell sicura

FEATURE(smrsh)
define(`LOCAL_SHELL_PATH’,`/usr/libexec/smrsh’)

Configurazione mail server: file relay.mc (4)

regole per la riscrittura mittente

Kuserdb btree -o /etc/userdb.db

```
LOCAL_RULE_1
##########################################################
### Local Ruleset 1, rewrite sender header & envelope ##
##########################################################
#Thanks to Bjart Kvarme <bjart.kvarme@usit.uio.no>
S1
R$-                          $1 < @ $j . >                  user=>user@localhost
R$- < @ $=w . > $*           $: $1 < @ $2 . > $3 ?? $1      user@localhost ?
R$+ ?? $+                    $: $1 ?? $(userdb $2 : mailname $: @ $)
R$+ ?? @                     $@ $1                                  Not found
R$+ ?? $+                    $>3 $2                                 Found, rewrite
```

Configurazione mail server: file relay.mc (5)

definizione dei mailer supportati

MAILER(local)dnl
MAILER(smtp)dnl

Struttura del file di alias

Alias "obbligatori"

postmaster: root
abuse: root

Attenzione dopo ogni modifica dare il comando newaliases !

Per gestire piu' domini usare le virtusertable !

Struttura del file userdb

Vengono usate 2 keyword: maildrop, mailname

Le entry devono essere inserite nel file /etc/userdb.txt.

Es.:

luca:maildrop luca@myhost.cnaf.infn.it
luca.dellagnello:maildrop luca@myhost.cnaf.infn.it
luca:mailname: luca.dellagnello@cnaf.infn.it

Dopo ogni modifica ricostruire il database con il comando:

makemap btree /etc/userdb.db < /etc/userdb.txt

Struttura del file sendmail.cw

Le entry sono del tipo:

myhost.cnaf.infn.it

Equivalente ad inserire nel file di configurazione la riga:

Cw myhost.cnaf.infn.it

Dopo ogni modifica fare ripartire sendmail

Configurazione mail server: autorizzazione accessi

- /etc/mail/relay-domains (eq. a FEATURE(relay_entire_domain)
  lista domini riga per riga

- FEATURE(relay_hosts_only)
  scelta selettiva sugli host

- FEATURE(access_db)
  scelta selettiva sugli utenti

Struttura access db

cnaf.infn.it	**RELAY**
fi.infn.it	**RELAY**
roma1.infn.it	**REJECT**
205.188	**DISCARD**
amica@aol.com	**RELAY**
aol.com	**550 scio'!**

makemap hash /etc/mail/access.db < /etc/mail/access

Misure anti-spam

sendmail 8.9.3

+

configurazioni precedenti

=

relaying disabilitato

Filtri sul router

```
!
interface serial 0
......
ip access-group 103 in
.....
!
! definizione access-list (nell'esempio RETE e' una rete di "classe C")
!
access-list 103 permit tcp any host <MAIL SERVER 1>
access-list 103 permit tcp any host <MAIL SERVER 2>
access-list 103 deny   tcp any <RETE> 0.0.0.255 eq smtp log
access-list 103 permit ip any any
```

Problema

Con i filtri sul router gli indirizzi:

utente@macchina.dominio

non funzionano!

- Inserire record MX per l'host che punti al MS
- nello userd:
  mario.rossi:maildrop mario@[141.108.6.11]

In caso di problemi...

- Contattare immediatamente il CERT@GARR.IT
- Bloccare l'accesso al mailer compromesso
- Installare e configurare mailer protetti
- Conservare i LOG dell'attacco
- Informare gli utenti dell'attacco subito
- Controllare TUTTI i mailer della LAN
- Filtrare sui router i mailer non controllabili o sprotetti

L'utenza: informazioni

- Informare l'utenza sul mail SPAM
- invitarla a segnalarvi i casi di mail spam ricevuti
- invitarla a leggere le norme di Netiquette
- informarla su come agiscono i "virus" in attachment
- informarla sul Hoaxes e simili
- ... e molte altre cose!!