LITT OM SIKKERHETSARBEIDET

Hans Morten Kind
IT-Forum
Solstrand, 31. mars 2004

I dag snakker vi om alfabetet

A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z

En ny bokstav hver dag . . .!

Det handler selvsagt om virus

- 2003 var verre enn noe år tidligere
  - Sobig
  - Swen
  - Blaster
  - Slammer
- 2004 blir neppe bedre
  - Bagle
  - MyDoom
  - Netsky

Hvem lager virus – og hvorfor?

- Før var det iallefall bøller
  - PC-er har potensiale som filtjenere
- Sobig hadde kommersielle hensikter
  - Spam kommer fra hjemmemaskiner
- Kanskje er det nå bare en prestisjekamp mellom ulike gjenger?

Hvordan sprer virus seg?

- Noen har kanskje “forhåndsvisning” enda?
- Noen kan ha påskrudd ActiveX enda?
- Noen klikker på vedlegg . . .
- Folk dekoder ZIP-filer, skriver passord inn manuelt og klikker på resultatet!
- Folk leser epost fra eksterne servere

- Virusene sprer seg også utenfor epost
  - P2P (KaZaA etc)
  - shares

En sann plage – uansett

- Men de stoppes jo av serveren...
- ... og jeg har oppdatert antivirus fra CA

- De stjeler kapasitet på nett og server
- Det dukker stadig opp nye varianter
- De lager mye støy og utallige feilmeldinger

Hvordan kan vettuge unngå å forstå at avsender er forfalsket?

Hva kan vi gjøre

- Oppdaterte maskiner, selvsagt
- Oppdaterte virusprogram, selvsagt
- Trenger vi oppdaterte brukere også?

Og hva med:

- Hjemmemaskiner?
- Bærbare?
- Besøkende?

<u>Men vi har flere tiltak:</u>

Restriksjoner på utgående epost

- Epost bruker (nesten) bare port 25/TCP
- Ingen person har behov for egen server
- IT-avdelingen aksepterer “relay” internt
- IT-avdelingen støtter POP-before-RELAY
- Dispensasjon for servere kan gis
- Men eposttjenesten er vedtatt

sentralisert

Registrerte SMTP servere

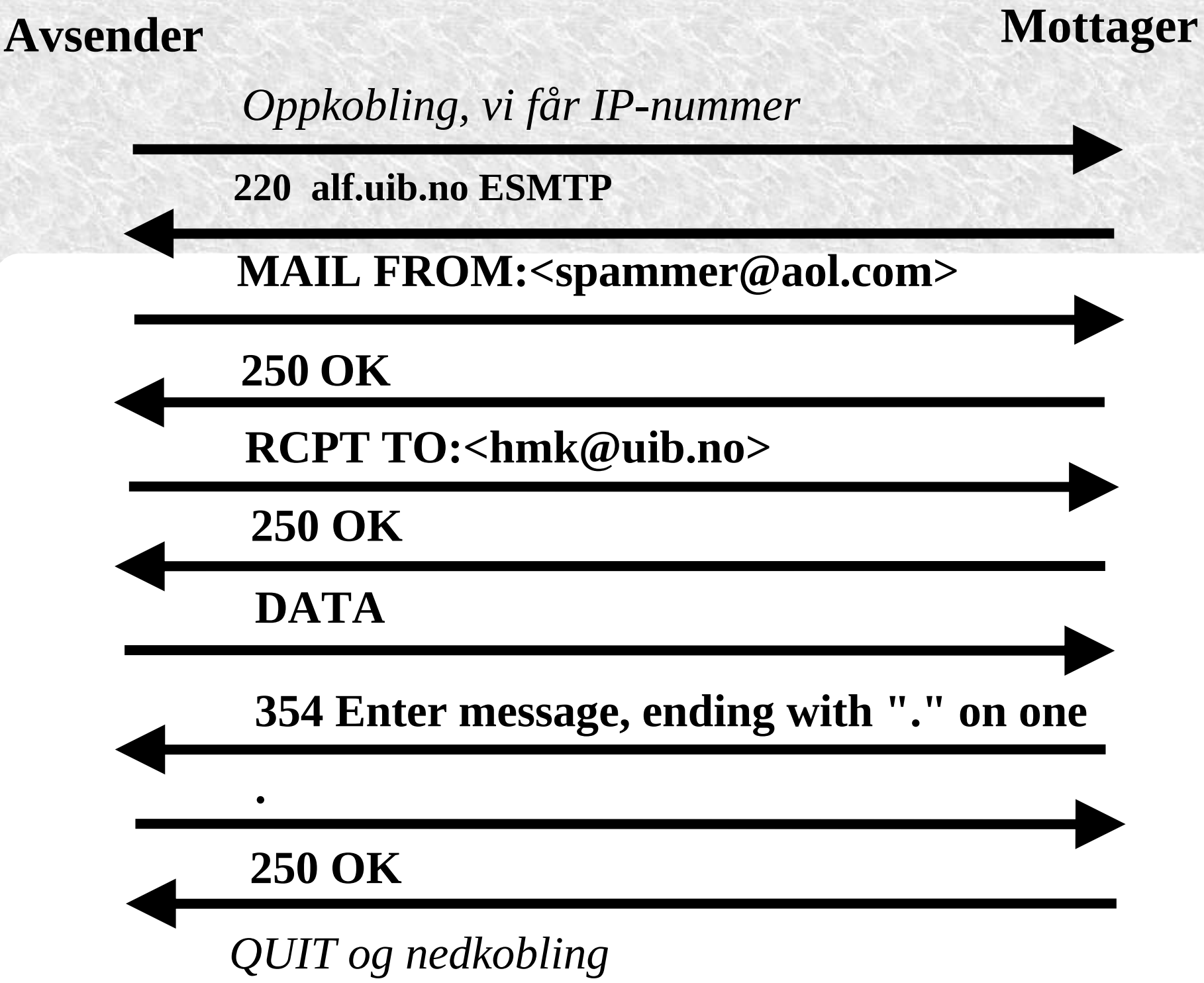
- alf rolf noralf rasmus (IT)
- eik.ii.uib.no mail.ii.uib.no (II)
- kj fi mi im gfi zoo geo (matnat)
- picasso helmer lingo ludo (HF)
- SIU SIB Haukeland Nansen (Andre)
- Kvarteret Fribyte Blug (studenter)

Totalt ca 30 IP-nummer

Grålisting

- BLACKlisting: NEI TAKK
- WHITElisting: OK, kom igjen uansett
- GREYlisting: Kanskje?

- http://tjinfo.uib.no/greylist.html
- http://projects.puremagic.com/greylisting/


Avsender
Mottager
Oppkobling, vi får IP-nummer
220 alf.uib.no ESMTP
MAIL FROM:<spammer@aol.com>
250 OK
RCPT TO:<hmk@uib.no>
250 OK
DATA
354 Enter message, ending with "." on one
.
250 OK
QUIT og nedkobling

Svarkoder

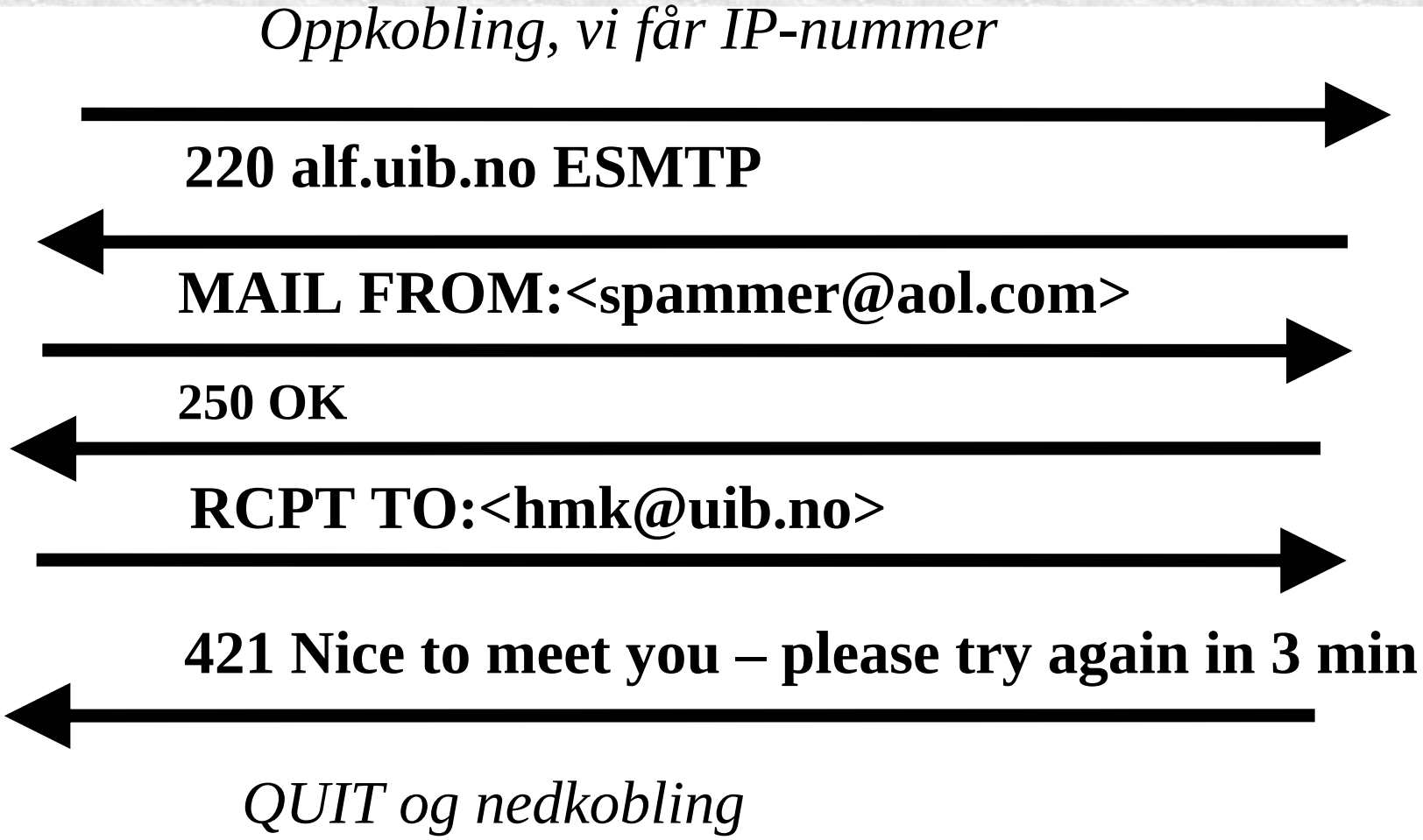
- 2XX OK
- 4XX Temporær feil, prøv igjen
- 5XX Permanent feil, lag feilmelding

En ekte eposttjener vil ved mottak av f.eks “421” køe meldingen og prøve å sende den senere.

UIB vil prøve etter 10 minutt, og med økende intervaller forsøke i inntil fem døgn før meldingen returneres. Melding til brukeren etter ett og tre døgn.

Avsender

Mottager



Greylist databasen

- Avsender (MAIL FROM)
- Mottager (RCPT TO)
- IP-nummer (/24 maske)

- **Ny triplet må være minst 3 minutter gammel**
- **Ny triplet må ikke være mer enn 25 timer gammel**
- **Triplet ugyldig etter 36 døgn**

- **Hvitelisting av mye brukte IP-nett, f.eks UNINETT**
- **Hvitelisting av tussete systemer**
- **Hvitelisting av lister med unik avsender pr melding**

Avsluttende ord

- Graphic programs stink
- Epost har mistet mye av sin praktiske nytteverdi
- Verden trenger nytt epostsystem
  men fortjener det neppe?
- Stillingskrigen på nettet vil aldri bli vunnet av noen
- Evig oppdatert forsvar

Takk for oppmerksomheten

- Spørsmål eller kommentarer?
- Baren er åpen!