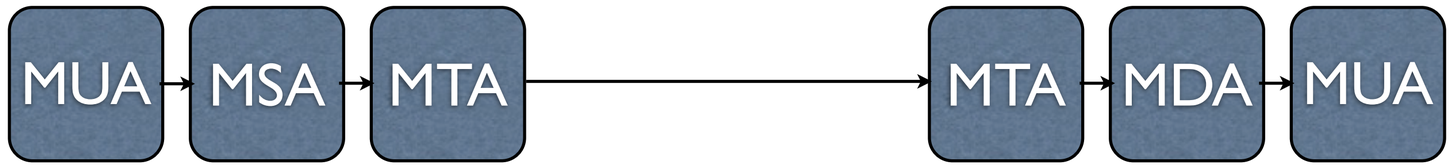
Nätverkssäkerhet
Mail

Marcus Wilhelmsson
marcus.wilhelmsson@lnu.se

Innehåll

- SMTP-protokollet
- MX-poster
- Open Relays
- DNS Blacklist
- Greylist
- SPF-poster
- Hashcash
- Statistisk filtrering
- Hybridfilter

SMTP



- MUA - Mail User Agent
- MSA - Mail Submission Agent
- MTA - Mail Transfer Agent
- MDA - Mail Delivery Agent

SMTP

- SMTP-kommandon
  - HELO och EHLO
  - MAIL
  - RCPT
  - DATA

SMTP

- Exempel

```
S: 220 lnu.se Ready
C: EHLO klient.se
S: 250-lnu.se greets klient.se
C: MAIL FROM:<nisse@klient.se>
S: 250 OK
C: RCPT TO:<kalle@lnu.se>
S: 250 OK
C: DATA
S: 354 Start mail input
C: Jag skickar ett mail.
C: .
S: 250 OK
C: QUIT
S: 221 lnu.se Service closing transmission channel
```

E-mailmeddelandet

- Header
  - To
  - From
  - Message-id
  - Recieved
- Body

Exempel på fake-header

```
Return-Path: [fake@fake.com]
Received: from smtp.real1.com (smtp.real1.com [145.5.33.4])
by smtp.real2.com with ESMTP id 73645544;
Fri, 3 Feb 2012 09:34:12 +0400 (MSK)
Received: from google.com (hhasdd.spammerz.ru [145.3.55.6])
by smtp.real1.com; Fri, 3 Feb 2012 10:41:31 +0100 (CET)
Date: Fri, 3 Feb 2012 10:41:31 +0100 (CET)
From: cheap viagra <viagra_boss@gmail.com>
To: ordinary@user.com
Subject: Cheap Viagra, you know you need it!
```

MX-poster

- Pekar ut SMTP-servrarna i en domän

Open Relays

- Innebär att servern kan användas av vem som helst att skicka mail till vem som helst

DNS Blacklist

- Svartlistade IP-adresser
- Spamtrap/honeypot
- Problem med blacklisting?

URI DNS Blacklist

- Liknar URL blacklist
- Letar efter blacklistade URLer

Greylisting

- Bygger på att man blockerar ALLA mail en gång
- Fungerar bra när legitima servrar följer SMTP-standarden men spammare inte gör det

SPF, Sender Policy Framework

```
kalmar.se. IN TXT ”v=spf1  mx a:backup-mail.kalmar.se mx:it.kalmar.se ip4:192.168.0.0/24
include:ekonomi.kalmar.se ~all”
```

Hashcash

- “Betala” för att skicka mail
- Valutan är CPU-tid istället för pengar

Statistisk filtrering

- Bygger på att spam innehåller vissa drag som gör att man kan särskilja dem
- Bayesisk filtrering är ett exempel på denna typ av filter

Hybridfilter

- Flera metoder är bättre än en
- Flera metoder används för att sätta en spampoäng
- SpamAssassin

SpamAssassin

- Används tillsammans med en MTA
- Licensierad under Apache License och utvecklas av Apache Software Foundation

- http://www.debuntu.org/postfix-and-pamassassin-how-to-filter-spam