

# TÖLVUPÓSTUR

Sjálfstætt verkefni í Tölvuöryggi

Háskólinn í Reykjavík, Tölvunarfræðideild, Haustönn 2004.

Leiðbeinendur: Dr. Gísli Hjálmtýsson og Björn Brynjúlfsson.

Nemandi: Sigurjón Sveinsson.

## 1 Inngangur

Rafrænn póstur, oftast kallaður tölvupóstur, er einn vinsælasti samskiptamátinn á Internetinu í dag. Milljónir skeyta berast milli manna dag hvern og nytsemi tölvupósts er mikil. En þegar kemur að öryggi gagnanna og góðri notkun þá er mörgu ábótavant og nokkrir gallar hafa komið í ljós. Má þar nefna öryggisgalla í auðkenningu, óumbeðin dreifipóst og tölvuvírusa.

Þessi greinargerð mun útskýra hvernig tölvupóstur er uppbyggður, hvernig hann virkar, hverjir öryggisgallarnir eru, hvernig brugðist hefur verið við þeim og hvað má betur fara.

Vegna tæknilegrar umfjöllunar verður gert ráð fyrir að lesendur þessarar greinargerðar hafi þekkingu á tölvusamskiptum og lagskiptingu þeirra, sérstaklega TCP/IP staðlinum.

## 2 Tölvupóstur

Rafrænn póstur (e. electronic mail, e-mail eða email), oftast kallaður tölvupóstur kom fram áður en tölvusamskipti hófust með nettengingum. Þá var tölvupósturinn útfærður á stórtölvum (e. mainframe) sem margir notendur höfðu aðgang að. Tölvupóstur var sendur á milli þeirra notenda sem höfðu aðgang að sömu vélinni og fór ekki út fyrir hana.

En síðar meir komu nettengingar og tölvupóstur var sendur með þeim miðli. Nettengingar urðu afkastameiri og algengari og með því jókst notkun tölvupósts. Í dag er notkun tölvupósts gífurleg á heimsvísu. Og samfara þeirri þróun hafa vankantar tölvupósts komið betur og betur í ljós.

### 2.1 Lagskipting tölvupósts

Tölvupóstssamskipti skiptast í þrjá megin hluta þ.e. **biðlari** (e. user agents), **póstþjónar** (e. mail servers) og **samskiptareglur** (SMTP, e. Simple Mail Transfer Protocol).

#### 2.1.1. Biðlari

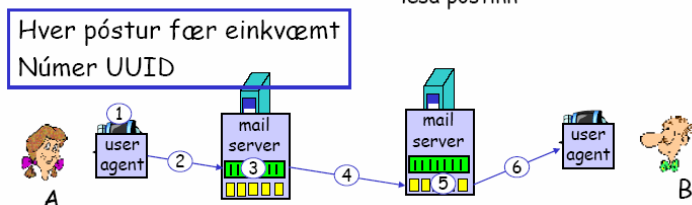
Biðlari er forrit á borð við t.d. Eudora, Outlook eða önnur póstforrit sem útfæra grafískt viðmót til að semja, senda, lesa og halda utanum tölvupóst. Þessi forrit geta verið einföld forrit sem gera lítið annað er að sýsla með tölvupóst. Þau geta einnig verið flókin og viðamikil eins og Microsoft Office Outlook sem ekki einungis sér um tölvupóst. Outlook heldur einnig utan um dagbækur og verklista og getur deilt ýmsum gögnum með tengingu við pósthjón á borð við Exchange Server frá Microsoft.

#### 2.1.2. Póstþjónar

Póstþjónar eru t.d. SendMail <http://www.sendmail.org/> og Exchange frá Microsoft þar sem hver notandi hefur sitt mailbox. Til að fá póstinn sinn þangað verður notandinn að tengjast póstþjóni ISP aðila eða innanhús í fyrirtækjum/skólum með biðlaraforriti sínu, auðkenna sig með notandanafni og lykilorði og sækja póstinn af póstþjónum í póstforritið. Ef notandi A sendir póst á notanda B þá tala póstþjónarnir saman. Ef t.d. póstþjónn B getur ekki tekið á móti sendingu frá A þá geymir A póstinn í biðröð (message queue) og reynir að senda póstinn aftur á fyrirfram ákveðnum fresti (skilgreindur tími af kerfisstjóra) þangað til pósturinn kemst til skila.

## Að senda póst

- 1) A býr til tölvupóst til B í sínum biðlara
- 2) A sendir póstinn á sinn póstþjón
- 3) Póstþjóninn kannar hvort móttakandi sé hjá sér
- 4) Póstþjónn A sendir tölvupóstinn áfram á Póstþjón B með TCP tengingu á port 25
- 5) Póstþjónn B setur póstinn í pósthólf B
- 6) B notar sinn biðlara til að lesa póstinn



Mynd af póstsendingu, © Ágúst Valgeirsson.

### 2.1.3. Ósamstillt samskipti

Tölvupóstur er ósamstilltur, þ.e. það þarf ekki að vera bein tenging milli sendanda og móttakanda til að hægt sé að senda póstinn á milli aðila. Sendandinn sendir póstinn úr sínu póstforriti og þarf hann að vera nettengdur þegar sendingin fer fram. Þegar sendandinn sendir póstinn af stað fer hann úr því forriti sem notað er yfir á póstþjón þess sendanda. Póstþjónn sendandans sendir póstinn á póstþjón móttakandans og þar liggur pósturinn þar til að móttakandi nær í hann á þeim þjóni.

## 3 Samskiptastaðlar tölvupósts

Fyrstu staðlarnir fyrir tölvupóst komu fram á dögum ARPA netsins. Fyrsti staðallinn sem lýsti rafrænum póst var RFC 196 (Richard W. Watson, 20. júlí 1971) [3]. Í september 1980 kom fram RFC 772 sem lýsti staðli sem kallaður var Mail Transfer Protocol, skammstafað MTP, og var það forveri þess tölvupóstsstaðals sem við þekkjum í dag þó að hann hafi notað telnet og FTP (e. File Transfer Protocol) sem burðarlag en ekki TCP/IP sem tölvupóstur notar í dag.

### 3.1 Simple Mail Transfer Protocol

Í ágúst 1982 kom fram fyrsta útgáfa af SMTP (e. Simple Mail Transfer Protocol) í RFC 821. Þessi RFC lýsti því tölvupóstkerfi sem við notum í dag, þ.e. tölvupóstur sem notar TCP/IP samskiptastaðalinn sem burðarlag. Síðar meir var SMTP staðallinn uppfærður og endurbættur í RFC 974, 1869, 2487,

2821, 2822, 2920, 3030 sem einnig lýstu viðbótum við staðalinn á borð við MIME (e. Multipurpose Internet Mail Extensions) og notkun SSL (e. Secure Sockets Layer) til að auka gagnaöryggi.

SMTP var barn síns tíma þegar afköst á tölvunetum og tölvum voru langt undir þeirri getu sem við búum við í dag. Eitt besta merki þessa er að allt skeytið verður að vera á 7 bita ASCII formi. Ástæðan fyrir því að þetta er til trafala í dag er sú að samkvæmt SMTP staðlinum þarf að breyta öllum viðhengjum, t.d. margmiðlunargögnum á stafrænu formi, sem fara með póstinum sem viðhengi, yfir í ASCII áður en þau eru send með tölvupósti með SMTP. Svo þarf að þýða viðhengið aftur yfir í stafrænt form eftir SMTP sendinguna. Einnig takmarkar þetta þann fjölda tákna sem hægt er að senda á hefðbundinn hátt í tölvupósti, því einungis er hægt að tákna 128 tákn með 7 bitum og það útilokar t.d. séríslensk tákn og langflest tákn sem ekki eru í enska stafrófinu.

SMTP notar TCP/IP til að senda tölvupóst frá biðlara til miðlara á porti 25. SMTP er svokallaður push samskiptastaðall. Þetta þýðir að öllum skeytum er ýtt (e. push) af sendanda til móttakanda. Það er ekki móttakandi sem sækir (e. pull) póstinn með SMTP.

### 3.1.1. Sendingaferli SMTP

Sendingaferlið er þrjúþætt:

- "Handshaking" þar sem þjónarnir kynna sig hvor fyrir öðrum áður en skilaboðasending fer fram.
- Senda skilaboð frá þjóni sendanda til þjóns móttakanda.
- Loka samskiptum þjónanna.

Þessi samskipti fara fram með því að senda skipanir milli þjónanna á 7 bita ASCII formi ásamt stöðugildum og skýringum

Eftirfarandi er dæmi um þau samskipti milli tveggja póstpjóna, sendanda (S) og móttakanda (M), eftir að TCP tengingu hefur verið komið á [3].

```
M: 220 hamburger.edu
S: HELO crepes.frS: 250 Hello crepes.fr, pleased to meet you
S: MAIL FROM: <alice@crepes.fr>
M: 250 alice@crepes.fr... Sender ok
S: RCPT TO: <bob@hamburger.edu>
M: 250 bob@hamburger.edu... Recipient ok
S: DATA S: 354 Enter mail, end with "." on a line by itself
S: Do you like ketchup?
S: How about pickles?
S: .
M: 250 Message accepted for delivery
S: QUIT
M: 221 hamburger.edu closing connection
```

Hér sendir sendandinn skilaboðin "Do you like ketchup? How about pickles?" frá póstpjóninum hamburger.edu.

## 3.2 Sækja póst af pósthjónum

Að senda póst með SMTP er "push" aðgerð. En að sækja póst frá biðlara á pósthjón er "pull" aðgerð. Það eru til nokkrar aðferðir við þessa aðgerð "Access Protocol" eins og POP3, IMAP og HTTP.

### 3.2.1. POP3

POP3 staðallinn er skilgreindur í RFC 1939, þetta er mjög einfaldur staðall [1]. POP3 sækir póst með því þegar biðlari opnar TCP tengingu við pósthjón á porti 110. Með TCP tengingunni fer POP3 í gegnum þrjú skref: Auðkenning, færsla og uppfæra. Auðkenning er til að auðkenna notandann með notandanafni og lykilorði. Í færslunni fær biðlarinn skilaboðin frá hjóninum og í uppfærslan hefst þegar biðlarinn hefur skilgreint "quit" skipunina. Þá endar POP3 tengingin. Hægt er að velja í POP3 að geyma skilaboð á pósthjóni eftir að náð hefur verið í póst þannig að hægt sé að nálgast þau á fleiri en einni tölvu. Einnig er hægt að skilgreina að eyða póstinum af hjóni eftir ákveðinn tíma eftir að POP3 hefur náð í póst og að eyða pósti af hjóni þegar biðlarinn hefur eytt póstinum hjá sér.

### 3.2.2. IMAP

Notendur vilja oft geyma mismunandi skilaboð í möppum í pósthólfinu sínu, færa á milli mappa, búa til nýjar möppur, flokka póst o.s.frv. Með POP3 getur notandinn ekki flokkað svona í möppur og komið síðan að annarri tölvu og fengið sömu flokkun. Þetta er hinsvegar mögulegt með IMAP (Internet Mail Access Protocol) sem skilgreindur í RFC 2060. IMAP er með marga möguleika umfram POP3 en er aftur á móti mun flóknari.

### 3.2.3. Vef viðmót

Fleiri og fleiri notendur í dag senda og skoða allan sinn tölvupóst í gegnum vafra á borð við Internet Explorer, Firefox og Opera. Þessir notendur eru þá að sýsla með sinn póst á pósthjónum sem birta póstinn með vefviðmóti sbr. Hotmail og margar aðrar vefpósthjónustur. Einnig eru margir pósthjónar, sem eru í raun að þjóna biðlurum, með vefviðmót. Dæmi um þetta eru pósthjónar á borð við Exchange Server frá Microsoft og Lotus Notes frá IBM.

Það sem gerist er að þegar notandinn vill sýsla með póstinn sinn í pósthólfinu sínu, sem staðsett er á pósthjóninum. þá er pósturinn sendur af pósthjóninum í vafra í gegnum HTTP í stað POP3 eða IMAP.

## 4 Öryggisvandamál í pósthöðlum

Eins og fram hefur komið eru staðlarnir fyrir tölvupóst orðnir nokkuð gamlir og að vissu leyti úreltir. Má þar nefna formun skeyta í 7 bita ASCII. En það eru einnig öryggisgallar í þeim höðlum sem notaður er í tölvupósti.

### 4.1 Auðkenning

Þegar POP3 tengist pósthjóni til að ná í póst þarf biðlarinn að auðkenna sig gagnvart pósthjóninum. Það gerir hann með því að senda hjóninum notandanafn, sem tilgreinir póst hvers er verið að ná í, og lykilorð, sem sannreynir að notandinn sé sá sem hann segist vera, sé lykilorðið rétt.

Þessar upplýsingar fara milli biðlara og miðlara óbrenslaðar. Þetta þýðir að hægt er að fylgjast með TCP samskiptum milli biðlara og pósthjóns með einföldum hugbúnaði og sía út úr þeim samskiptum notendanafn og lykilorð. Þessi galli er stór öryggisgalli. Það að óviðkomandi aðilar geta með auðveldum hætti komist yfir tölvupóst annarra er ekki það eina við þetta. Við þetta bætist að fólk notar oft sama notendanafn og/eða lykilorð að mörgum kerfum, hvort heldur sem það er tölvupóstur, aðgangur að sinni einkatölvu eða aðgangur að tölvukerfum og staðarnetum. Því má segja að komist tölvuprótar yfir aðgangsupplýsingar fólks með þessum hætti er hætt við að aðgangur að fleiri kerfum sé opinn. Sem dæmi má nefna að í Háskólanum í Reykjavík eru það sömu upplýsingar sem notaðar eru til að auðkenna notendur gagnvart tölvupóstinum og innranetinu.

Það er hægt að stemma stigu við þessum öryggisgalla með því að útfæra tengingu milli biðlara og miðlara með tengingum á borð við SSL sem auka gagnaöryggi. Einnig er hægt að útfæra auðkenningu með dulritun eins og SPA (e. Secure Password Authentication).

## 4.2 Open Relay

Þegar sendandi sendir póst tiltekur hann hvaða pósthjón sendingin á að fara í gegnum. Sem dæmi má nefna að ef nemandi í Háskólanum í Reykjavík ætlar að senda póst í gegnum pósthólf sitt á pósthjóni háskólans, sem heitir mail.ru.is, þá þarf að tilgreina hann sem svokallaðan "outgoing" hjón. "Outgoing" þýðir að allur póstur sem senda á með SMTP á að fara í gegnum hann.

Einn öryggisgalli í útfærslu pósthjóna var sá að það var hægt að senda póst í gegnum pósthjóna og tilgreina sendanda sem hafði ekkert með tiltekinn pósthjón að gera. Til dæmis gæti hver sem er sent póst til hvers sem er og tilgreint mail.ru.is sem "outgoing" hjón, þ.e. ef sá hjónn gerði ekkert til að koma í veg fyrir þetta. T.d. gæti Michael Moore sent póst sem George Bush og tilgreint netfang sendanda president@whitehouse.gov (raunverulegt netfang) og notað mail.ru.is til að senda póstin.

Þessi galli hefur verið kallaður Open Relay eða opin endurvörpun.

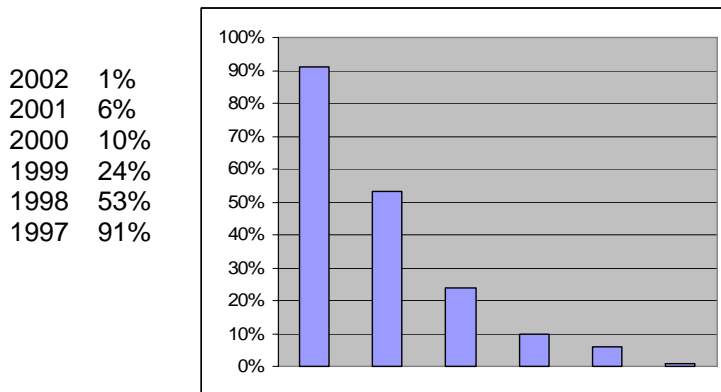
### 4.2.1. Álag á pósthjónum vegna opinna endurvörpunna

Ef pósthjón er með opna endurvörpun getur hver sem er sent hverjum sem er tölvupóst, óháð léni póstsins eða því hvort sendandi hafi pósthólf á þeim hjóni. Þetta þýðir að þessir pósthjónar eru vinsælir hjá þeim aðilum sem senda út óumbeðinn fjöldapóst, stundum kallaður SPAM póstur eða ruslpóstur. Þegar þessar sendingar fara í gegnum pósthjóna orsakar það að álagið á pósthjóninum eykst ásamt því að þessar sendingar taka upp þá bandvidd sem sá pósthjónn hefur til umráða.

Til að sporna við þessu fóru margir aðilar af stað með hjónustur sem söfnuðu saman lista af þeim pósthjónum sem voru með opna endurvörpun og seldu aðgang að þeim listum. Þessir listar voru, og eru enn, notaðir af pósthjónum sem keyrðu á hjónum. Með þessum listum geta pósthjónar hafnað pósti frá þeim sem eru á listanum til að sporna við ruslpósti.

En þörfin fyrir þessa lista er að minnka. Framleiðendur hugbúnaðar fyrir pósthjóna eru orðnir mjög meðvitaðir um þennan galla og útfæra í dag þann möguleika að slökkva á opna endurvörpunna [1].

Öryggisfyrirtækið NTA, sem er með fremstu fyrirtækjum Evrópu í öryggisprófunum, hefur fylgst með opnum endurvörpunum síðan 1997 og samkvæmt þeim hefur hlutfall þeirra í Bretlandi verið eftirfarandi ár hvert [5]:



Minnkun opinna endurvarpanna frá 1997-2002.

Samkvæmt þessum tölum hefur stórlega dregið úr opnum endurvörpunum og þar af leiðandi er þessi galli ekki jafn alvarlegur í dag og hann var.

### 4.3 Óskalistinn

Það væri gaman að búa í fullkominni veröld, og ef tölvupóstur í þeirri fullkomnu veröld ætti að vera öruggur þá mætti ætla að útfæra þyrfti nokkur eigindi. Eftirfarandi eru nokkur atriði sem gaman væri að sjá sem hluta af tölvupóstsstaðli þessa fullkomna heims.

- Friðhelgi: Að einungis móttakandi og sendandi tölvupósts geti lesið innihald póstsins og enginn annar. Að ekki fari fyrir netið óbrenslaðar upplýsingar um notandann á borð við notandanafn og lykilorð.
- Auðkenning: Að móttakandi sé fullviss um hver sendandinn er.
- Auðkenning sendanda: Að ekki sé hægt að senda tölvupóst á netfangi sem ekki er til og að ekki sé hægt að senda tölvupóst með virkt netfang sem sendanda án þess að vera eigandi þess netfangs.
- Heilindi: Að móttakandi geti fullvissað sig um að tölvupósti hafi ekki verið breytt frá því að sendandinn sendi póstinn.
- Óumdeilanleiki: Að móttakandi geti sannað það fyrir þriðja aðila að sendandi tölvupósts sé raunverulega sá/sú sem hann/hún sagðist vera. Þetta þýðir að sendandi getur ekki neitað því seinna meir að hafa sent ákveðinn tölvupóst.
- Sannreyning á móttöku: Staðfesting á því að móttakandi hafi tekið á móti tölvupósti.
- Leynd á flæði tölvupósts: Að óviðkomandi aðilar geti ekki séð hverjir eru að senda hverjum tölvupóst. Það þýðir að ekki sé hægt, fyrir óviðkomandi aðila, að fylgjast með flæði tölvupósts til og frá fólki.

- Nafnleynd: Að móttakandi geti ekki komist að því hver sendandinn er.
- Inilokunarstefna: Hægt verði að halda ákveðnum upplýsingum frá því að komast út fyrir ákveðið net.
- Skráning á atburðum: Netþjónar geta skráð hjá sér viðburði er varða tölvupóst sem hafa þýðingu fyrir tölvuöryggi.
- Tölfræði: Að þau kerfi sem sjá um tölvupóst geti fylgst með flæði tölvupósts og skráð hjá sér upplýsingar um eðli þess flæðis. Sem dæmi mætti nefna að geta fylgst með notkun einstakra aðila á bandvidd (stór skeyti), fylgjast með pósti sem gæti verið óumbeðinn fjöldapóstur og margt annað.
- Sjálfseyðing: Tölvupóstur eyðist hjá móttakanda eftir ákveðinn tíma. Þannig mætti koma í veg fyrir að móttakandi geti áframsent póst eða vistað hann.
- Heilindi sendingarraðar: Fullvissa um að tölvupóstur hafi komist til skila í þeirri röð sem hann var sendur, án taps.

SMTP útfærir engin af ofangreindum atriðum og færst tölvupóstskerfi í dag útfæra nokkuð af þeim. Jafnvel kerfi sem skilgreina sig með hátt öryggisstig útfæra ekki nema hluta þessara atriða.

## 5 Dulritun í tölvupósti

Dulritun er oftast lýst sem brenglun á texta eða gögnum þannig að þau verða óskiljanleg nema fyrir þá aðila sem hafa svokallaða lykla til að afbrensla gögnin aftur í sitt upprunalega horf. Flest atriðin á óskalistanum er ekki hægt að útfæra nema með notkun dulritunar.

### 5.1 PEM

PEM dulritun (e. Privacy Enhanced Mail) var sett fram í RFC 1421-1424 sem komu fram í febrúar 1993. PEM útfærir nokkrar þjónustur til auka öryggi tölvupósts. Friðhelgi (e. confidentiality), auðkenning (e. authentication), heilindi (e. integrity) og óumdeilanleika (e. non-repudiation of origin).

Þó svo að PEM hafi verið hannað í upphafi með það í huga að vera óháð hvaða algrímum væri beitt varðandi dulritunina þá hefur DES, sem er leynilykill, ráðið ríkjum í að dulrita skeytin [2] sjálf. Til að skiptast á lykllum notar PEM RSA algrímið, sem er dreifilykill. Við auðkenningu og heilindi er oftast notast við MD2 og MD5 algrímin til að reikna prófsummu [2].

PEM er útfært á endastöðvum, þ.e. hjá sendanda tölvupósts og móttakanda hans. Allir þeir nethnútar sem áframsenda tölvupóst milli endastöðva koma ekki við sögu í dulrituninni. En það eru vissir hlutar tölvupóstsins sem ekki er hreyft við, hvorki þegar allt skeytið er dulritað né þegar verið er að reikna prófsummur. Þessir hlutar tölvupóstsins eru í haus tölvupóstsins eða svokölluðum header. Þau svæði sem eru látin vera eru svæði merkt TO, FROM, SUBJECT og TIMESTAMP. Ástæðan fyrir þessu er að þessar upplýsingar þurfa að vera lesanlegar fyrir alla þá nethnúta sem meðhöndla tölvupóstinn á leið sinni að endastöð svo að þeir viti hvað á að gera við hann.

## 5.2 PGP

Árið 1991 kom Philip Zimmermann fram með hugbúnað sem dulritaði tölvupóst og kallaði Zimmermann forritið Pretty Good Privacy eða PGP. Zimmermann hvatti almenning til að dreifa þessum hugbúnaði en það stangaðist á við bann bandarísku ríkisstjórnarinnar við útflutningi á viðkvæmum varningi á borð við kjarnorkuleyndarmál og dulritun. Einnig stangaðist PGP á við réttthafa RSA einkaleyfisins, en PGP notar RSA dulritun, því réttthöfunum var illa við að hugbúnaðinum væri dreift ókeypis. Hægt er að nálgast forritið á vef PGP Corporation, [www.pgp.com](http://www.pgp.com), bæði forritið sjálft og kóða þess.

PGP virkar í grófum dráttum eins og PEM og veitir sömu þjónustur. Meginmunur á PGP og PEM er vottun á lykllum. PEM notar mjög ósveigjanlegt erfðatré á vottun lykla en í PGP er nokkurs konar stjórnleysi, þ.e. ekki er hægt að reikna með að vottaðir aðilar gefi út þá lykla sem notaðir eru. Þetta þýðir að það er ekki PEM sem ákveður hverjum er treystandi varðandi útgáfu lykla og samþykki heldur er það notendanna sjálfra að samþykkja [2].

## 6 Vírusar

Vírus er forrit eða hluti forrits sem dreifir sér sjálf milli tölva án vitunar eigenda tölvanna. Þessir vírusar eru mismunandi í eðli sínu og virka á mismunandi hátt, allt frá því að valda miklum óafturkræfum skaða á sýktri tölvu niður í það að senda frá sér meinlausan áróðurstexta. En það sem vírusar eiga sameiginlegt er að þeir nota önnur forrit til að dreifa sér og er tölvupóstur, og þau forrit sem hann senda, lang algengust.

Dæmigerð virkni fyrir vírus er að virkjast þegar notandi fær vírusinn í tölvupósti sem viðhengi. Notandinn keyrir vírusinn þegar hann opnar viðhengið. Það sem vírusinn gerir þá er að skoða hvaða notendur viðkomandi notandi hefur í netfangalistanum og senda sjálfan sig áfram sem tölvupóst á alla þá aðila og með sjálfan sig sem viðhengi.

Fyrsta vírusinn má rekja til 1987 þegar óþekktur aðili laumaði forriti inn í ARPA netið sem bandaríski herinn, bandarískir háskólar og þarlend hermálafirvöld ráku. Síðan þá hafa margir vírusar komið fram og orðið mis frægir. Skæðasti vírusinn sem komið hefur er, að mati MessageLabs, hin svokallaði Mydoom vírus. Hann gerði ekki mikinn skaða á þeim vélum sem hann sýkti en dreifing hans var svo ör, mikil og skæð að álag á pósthjónum jókst mikið. Auk þess gat vírusinn opnað bakdyr að þeim tölum sem hann sýkti svo að hægt væri að stýra henni annars staðar frá. Vírusleit á pósthjónunum minnkaði afköst þeirra ásamt því að fjöldi skeyta með vírusnum varð það mikill að um tíma var tólfta hvert skeyti sýkt með vírusnum.

Mydoom notar ekki netfang þess sem á sýktu tölvuna sem netfang sendanda heldur eitthvað annað tilviljunarkennt netfang. Þannig að sá galli að geta sent tölvupóst með netfangi sem þarf ekki einu sinni að vera til, án allrar auðkenningar sendanda, spilar hér stórt hlutverk.

## 7 Óumbeðinn fjöldapóstur

Óumbeðinn fjöldapóstur, stundum kallaður ruslpóstur eða spam póstur, er tölvupóstur sem endur er á marga móttakendur eða póstlista. Þessi póstur er yfirleitt sendur til fólks án þess að það hafi beðið um að fá hann og er þar af leiðandi yfirleitt óumbeðinn. Þessi póstur getur innihaldið margvíslegt efni á borð við auglýsingar eða kynningar á vöru sem oft er vafasöm, kynningu á auðfengnum leiðum til ríkidæmis og margar vafasamar þjónustur.

### 7.1 Hver er afleiðing fjöldapóstsins?

Óumbeðinn fjöldapóstur er oftast sendur í miklu magni í einu, þ.e. á marga móttakendur. Þá er ekki verið að tala um einhverja tugi móttakenda heldur tugi eða hundruð þúsunda móttakenda. Það sem svona stórar sendingar gera er að hægja mikið á afköstum þeirra póstpjóna sem taka við póstinum, sérstaklega póstpjónum hjá stórum internetveitum á borð við AOL. Einnig minnka afköst þeirrar bandviddar sem internetveiturnar hafa við svo mikla netumferð. AOL gaf eitt sinn út að þeir fengju 1.8 milljón skeyti af óumbeðnum fjöldapósti frá einum aðila, Cyber Promotions, á dag þar til AOL fékk dómsúrskurð til að stöðva hann. Samkvæmt John Leyden hjá The Register var 67,6% af öllum tölvupósti fjöldapóstur í apríl síðastliðnum. Þetta er mjög hátt hlutfall og fer vaxandi.

Internetveitur þurfa að greiða pening fyrir allan þennan fjöldapóst. Við það að senda allan þennan fjöldapóst lendir kostnaður sendinganna því á þeim sem tekur á móti póstinum. Þar af leiðandi lendir þessi kostnaður á endanum á viðskiptavinum internetveitanna.

Þeir aðilar sem senda þennan fjöldapóst beita ýmsum ráðum til að verða sér úti um netföng til að senda á. Þessir aðilar stela listum hjá lögmætum fyrirtækjum, leita að netföngum á vefsíðum, kaupa listanna hjá óprúttum internetþjónustuaðilum og nota leitarvélur til að leita að netföngum svo eitthvað sé nefnt.

Það getur verið erfitt að rekja þessar sendingar. Sá galli í SMTP að krefjast ekki auðkenningar sendanda og opin endurvörpun gera þeim, sem vilja hylja slóð sína sem sendandi, mjög auðvelt að torvela leit að uppruna fjöldapósts. Einnig geta tölvuprjótur brotist inn í tölvur sem tengdar eru internetinu og notað þær til að senda fjöldapóst. Þannig er engan veginn hægt að finna sendandann nema með því að komast að því hver braust inn.

Það er erfitt að berjast gegn óumbeðnum fjöldapósti. Það hafa verið sett lög í ýmsum ríkjum gegn þessum ófögnuði en mislangt er gengið í þeim efnum. Í Bandaríkjunum hafa verið sett lög (CAN-SPAM Act) sem leyfa fjöldapóst ef hann hylur ekki uppruna póstsins. Evrópsk lög banna óumbeðin fjöldapóst en þó fylgja engin viðurlög því að brjóta þessi lög. Aðeins Ítalía og Ástralía banna óumbeðinn fjöldapóst og refsa fyrir brot á því banni [4].

## 8 Lokaorð

Tölvupóstur er mjög gagnlegur og hentugur við að koma gögnum og upplýsingum milli aðila á tölvutæku formi. En þeir staðlar sem notaðir eru við þessi samskipti eru óöryggir og sýna barnalegt traust þeirra sem sömdu þá á heiðarleika mannanna. Þessir öryggisgallar hafa valdið því að

tölvupóstur er mjög misnotaður þegar kemur að því að dreifa ófögnuði á borð við óumbeðinn fjöldapóst og vírusa. Vegna þessa trausts er einnig nokkuð auðvelt fyrir kunnáttumenn að “hlera” samskipti og lesa tölvupóst annarra. Þar að auki eru tæknilegar útfærslur, sem voru takmarkaðar vegna takmarkanna vélbúnaðar á sínum tíma, orðnar úreltar því þær takmarkanir eru ekki fyrir hendi í dag. Má þar nefna kröfu um 7 bita ASCII texta í SMTP staðlinum sem takmarkar mjög möguleg tákni sem hægt er að senda í tölvupósti án þess að grípa til umritunar.

Það væri því “alþjóðþrifaverk” að endurskoða alla þá staðla sem tölvupóstur byggir á, með það sem markmið að nýta nútímatækni í hugbúnaði, netsamskiptum og vélbúnaði til að gera tölvupóst öruggari, afkastameiri og til að binda endi á dreifingu ruslpósts og vírusa með tölvupósti.

## 9 Heimildaskrá

- [1] James F. Kurose, Keith W. Ross, 2003. *Computer Networking, A Top-Down Approach Featuring the Internet*. Pearson Education, Inc
- [2] Charlie Kaufman, Radia Perlman og Mike Speciner, 1995. *Network Security: Private Communication in a Public World*
- [3] Charles M. Kozierok, 7. júní 2004. *The TCP/IP Guide, TCP/IP Electronic Mail System Overview and History*.  
[http://www.tcpipguide.com/free/t\\_TCPIPElectronicMailSystemOverviewandHistory-2.htm](http://www.tcpipguide.com/free/t_TCPIPElectronicMailSystemOverviewandHistory-2.htm)
- [4] John Leyden, The Register 25. maí 2004. *Two thirds of emails now spam: official*.  
<http://www.securityfocus.com/news/8766>
- [5] NTA *NTA Monitor says 'open relay' spam is a minimal problem*.  
<http://www.nta-monitor.com/news/press-releases/03-spamcomment.htm>