Trivial Internet weaknesses with solutions proposal

("A global initiative" Part 1: Focusing on e-mail)

Ram Narula
ram@pluslab.com
For presentation at APNIC 20 in Hanoi

Simple Mail Transfer Protocol (SMTP)

- "THE PROTOCOL" for email communication
- Generally performs everything in plain-text (no data encryption) for server to server communication
  - Open to sniffing and Man-in-the-middle attacks
- Generally perform no authentication of sending server/receiving server

What did it all mean?

- When you send email to your SMTP server and your servers sends it to the designated SMTP server (of the recipient), the email is not encrypted. This allows anyone/router between them to view your message and alter your message (session hijack).
- Wanna see how many routers your message passes through? Try doing a “traceroute” from your SMTP server to recipient’s SMTP server (hidden router/firewall will not even show up!)

Sample 'traceroute' result from Bangkok to APNIC's SMTP server

```
$ traceroute kombu.apnic.net -q 1
traceroute to kombu.apnic.net (202.12.29.57) from 203.xxx.xxx.xxx, 30 hops max, 38 byte packets
 1  203.xxx.xxx.xxx (203.xxx.xxx.xxx)  248.598 ms
 2  203.xxx.xxx.xxx (203.xxx.xxx.xxx)  61.918 ms
 3  202.47.xxx.xxx (202.47.xxx.xxx)  89.270 ms
 4  202.47.253.134 (202.47.253.134)  46.515 ms
 5  global.hgc.com.hk (218.189.12.241)  127.309 ms
 6  global.hgc.com.hk (218.189.8.161)  96.762 ms
 7  210.0.247.34 (210.0.247.34)  97.296 ms
 8  210.0.247.42 (210.0.247.42)  115.330 ms
 9  peer.hgc.com.hk (218.189.96.54)  137.293 ms
10  i-3-4.wwh-dist02.net.reach.com (202.84.155.74)  81.425 ms
11  i-5-1.wwh-core01.net.reach.com (202.84.155.125)  80.450 ms
12  i-7-1.syd-core01.net.reach.com (202.84.249.186)  245.951 ms
13  10GigabitEthernet5-0.pad-core4.Sydney.telstra.net (203.50.13.37)  320.919 ms
14  10GigabitEthernet9-0.chw-core2.Sydney.telstra.net (203.50.6.89)  335.737 ms
15  Pos2-0.cha-core4.Brisbane.telstra.net (203.50.6.226)  264.211 ms
16  GigabitEthernet5-1.cha23.Brisbane.telstra.net (203.50.51.33)  258.429 ms
17  apnic1-new.lnk.telstra.net (139.130.97.62)  262.345 ms !X
```

17 hops!!

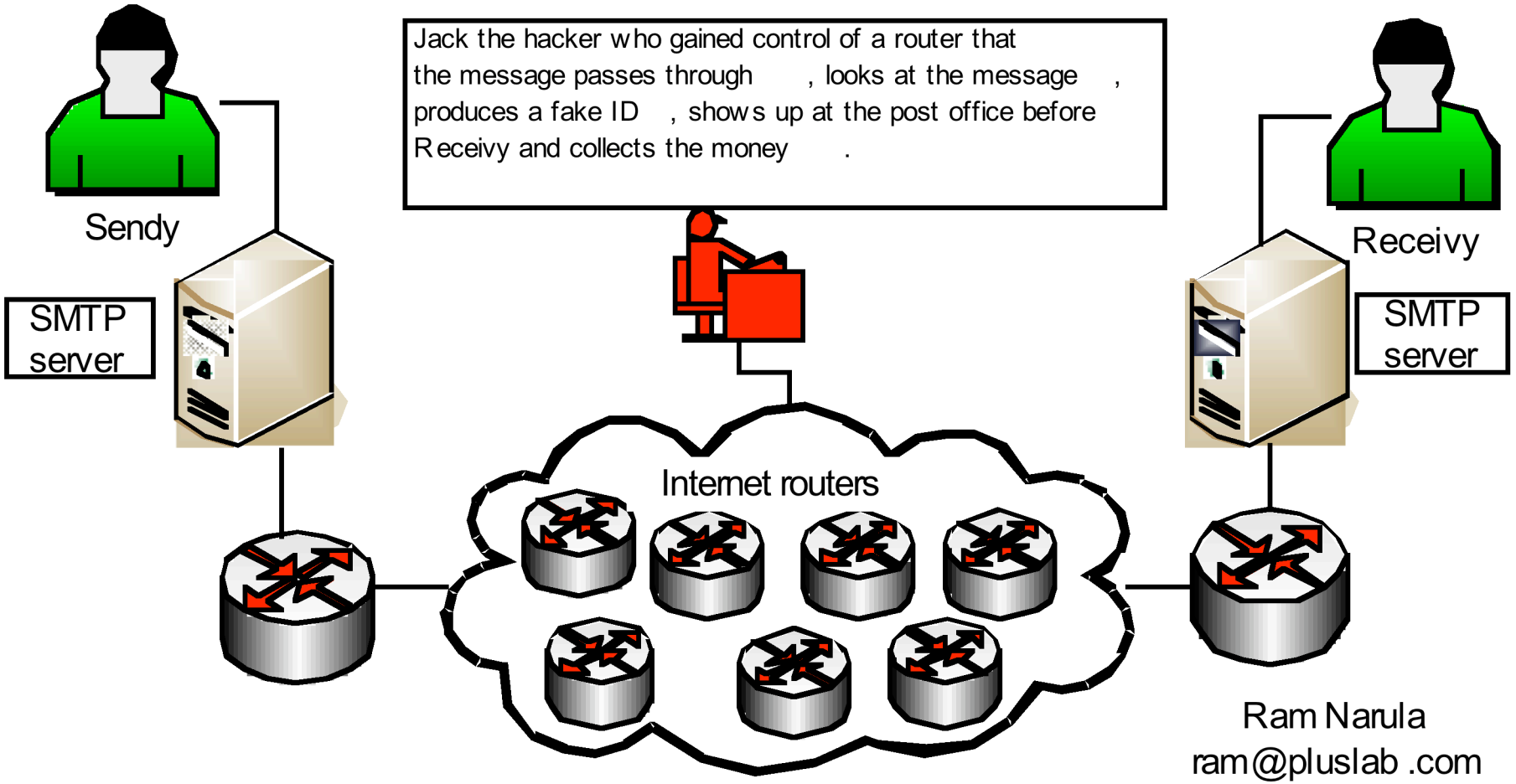
by Ram Narula ram@pluslab.com

Example of an attack

From Sendy to Receivy "Dear Receivy , I have send $100 to you via Post , just bring your ID to the post office and show them this number 21482172."

Receives the correct message from Sendy "Dear Receivy , I have send $100 to you via Post , just bring your ID to the post office and show them this number 21482172."

Jack the hacker who gained control of a router that the message passes through , looks at the message , produces a fake ID , shows up at the post office before Receivy and collects the money .



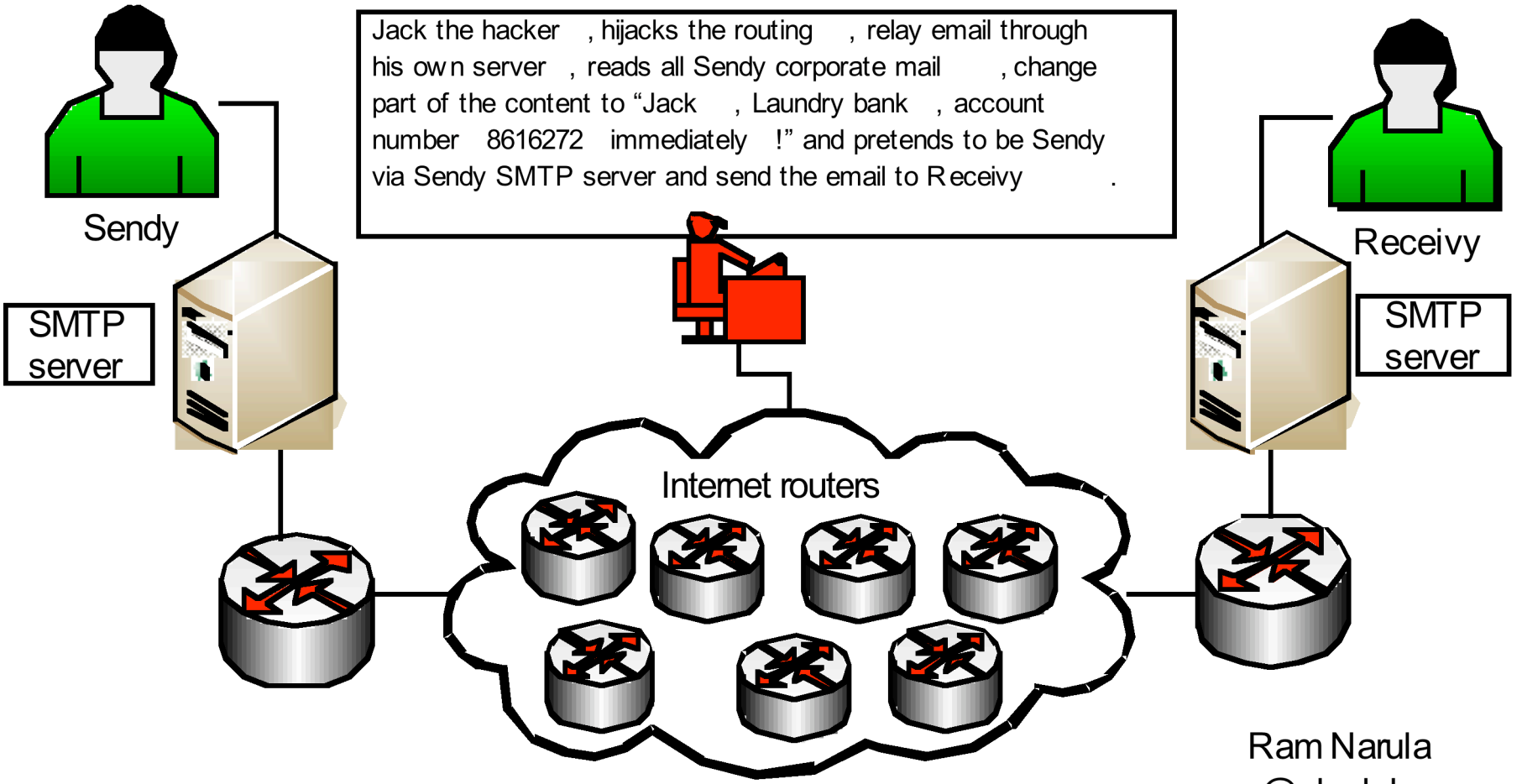
Ram Narula
ram@pluslab .com

Another example of an attack

From Sendy to Receivy "Dear Receivy , I have looked at your corporate proposal , and we are willing to take your investment of two million dollar , please transfer the amount to "Sendy , Reliable bank, account number 2712648".

From Sendy to Receivy "Dear Receivy , I have looked at your corporate proposal , and we are willing to take your investment of two million dollar , please transfer the amount to "Jack , Laundry bank , account number 8616272 immediately !".

Jack the hacker , hijacks the routing , relay email through his own server , reads all Sendy corporate mail , change part of the content to "Jack , Laundry bank , account number 8616272 immediately !" and pretends to be Sendy via Sendy SMTP server and send the email to Receivy .



Ram Narula
ram@pluslab .com

Not a new problem

- This is not a new problem, it is just being overlooked
- It needs more attention
- Solutions exists
- People will not understand or want to understand the problem until something bad happens
- SMIME, PGP and TLS (Transport Layer Security) implementation are not new

Solution for end-to-end encryption

- Use SMIME or PGP for encrypting email
  - Problems
    - Both sender and receiver must be ready to use SMIME or PGP (could be a problem for general use)
    - Man in the middle issues: Jack the hacker will still be able to gather email headers including subject, time of email, internal corporate network information including software name and version information, etc.

Another Approach – TLS is not new

- Implement TLS (Transport Layer Security) in all SMTP servers (both sending and receiving sides)
  - With TLS all SMTP communication between SMTP servers will be encrypted
  - With proper digital certificates, SMTP servers will also be able to authenticate their identities. This will also help in reduction of spam as unregistered/unsigned SMTP servers will not be able to operate.
  - SMIME and PGP users will not be affected
  - Problem: New SMTP servers will be required to wait for certificate signing

Implementation

- An entity that will be responsible for registration and signing of SMTP server certificates will have to be established (could be similar to RIRs/NIRs/LIRs structure)
- *(Small)* Payment must be collected from SMTP server owners for registration and signing (to ensure seriousness in operating the SMTP server)
- A cut off date will have to be established, no fall-back to non-TLS should take place after a set date (e.g. Dec 1st 2006)

Technical implementation for UNIX/Linux platform

- Sendmail
  - "STARTTLS" – by Claus Assmann *http://www.sendmail.org/m4/starttls.html*
- Postfix
  - "Postfix TLS Support" - Lutz Janicke and Wietse Venema *http://www.postfix.org/TLS_README.html*
- Exim
  - "Including TLS/SSL encryption support" by Exim team *http://www.exim.org/exim-html-4.50/doc/html/spec_4.html#SECT4.6*

Technical implementation for Windows platform

- Microsoft Exchange
  - "How to Help Protect SMTP Communication by Using the Transport Layer Security Protocol in Exchange Server" – Microsoft corporation *http://support.microsoft.com/default.aspx?scid=kb;en-us;829721*

...:-).....

$ telnet maila.microsoft.com smtp
Trying 131.107.3.125...
Connected to maila.microsoft.com.
Escape character is '^]'.
220 IGR-IMC-01.redmond.corp.microsoft.com <Inbound SMTP Virtual Server> Thu, 11 Aug 2005 00:xx:xx -0700
EHLO x
250-IGR-IMC-01.redmond.corp.microsoft.com Hello [203.xxx.xxx.xxx]
250-TURN
250-SIZE 10485760
250-ETRN
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-8bitmime
250-BINARYMIME
250-CHUNKING
250-VRFY
250-X-LINK2STATE
250-XEXCH50
250 OK
STARTTLS
554 5.7.3 Unable to initialize security subsystem

by Ram Narula ram@pluslab.com

Issues with TLS?

- The entity that signs the certificate must be trusted by all SMTP servers
- It does not provide end-to-end encryption (like SMIME or PGP) as it only secures SMTP communication
- Certificate revocation mechanism will have to exist & short lived certificate will have to be considered
- Additional cost for setting up and maintenance
- Requires additional processing power and bandwidth
- Could be illegal where encryption is prohibited

Cost vs. Benefit

- Similar view for cost vs. benefit for implementation of Web-based SSL(?)
  - Security and privacy to the next level
  - SMTP servers will have legal owners
- How much spam would admin of registered server be kind to tolerate?
  - Comments?
- What do you think?

SMTP-TLS Summary

- Advantages/plus side for implementation
  - Authenticity of SMTP servers could be confirmed
  - Increased privacy and security for email users
  - Spam reduction as all SMTP servers will have to be registered and will need a signed certificate
- Disadvantages/hurdles
  - Entity that will take care of each region's registration will have to be formed for every regions (creating more jobs :-)
  - More admin work to maintain the SMTP servers and certificates
  - All SMTP servers will have to trust the signer
  - Higher processing and bandwidth requirements
  - SMTP server registration and certificate associated costs

Why should TLS be implemented on a global scale?

- Makes emailing a safer thing to do with more privacy without end-user involvement
- Makes email communication become traceable and more reliable
- Help in reducing spam

...:-).....

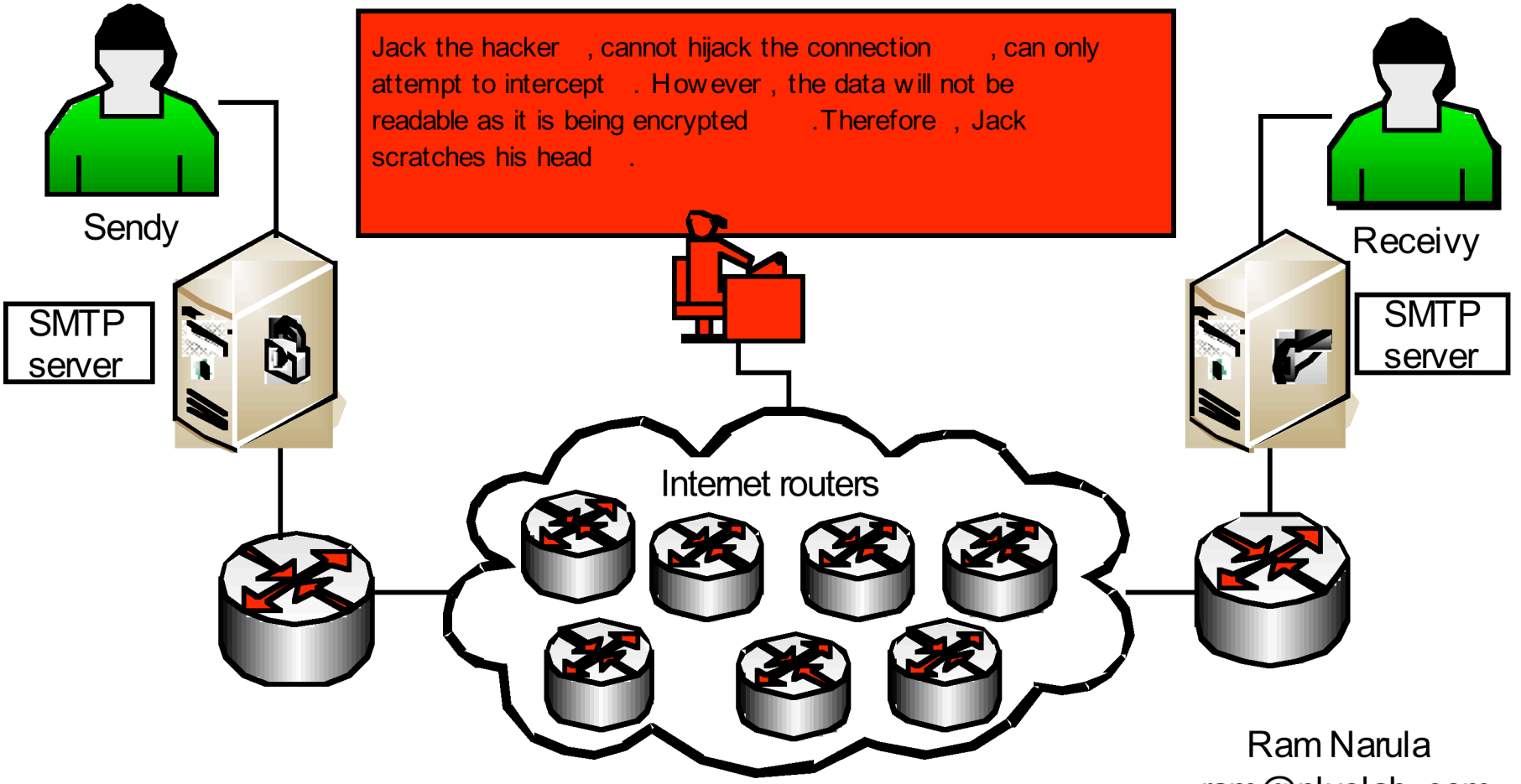
```
$ telnet kombu.apnic.net smtp
Trying 202.12.29.57...
Connected to kombu.apnic.net.
Escape character is '^]'.
220 kombu.apnic.net ESMTP Postfix
EHLO x
250-kombu.apnic.net
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250 8BITMIME
STARTTLS
502 Error: command not implemented
```

Sample of TLS implementation

From Sendy to Receivy "Dear Receivy , As we both have implemented TLS on our SMTP servers , let's see if it works" .

From Sendy to Receivy "Dear Receivy , As we both have implemented TLS on our SMTP servers , let's see if it works" .

Jack the hacker , cannot hijack the connection , can only attempt to intercept . However , the data will not be readable as it is being encrypted .Therefore , Jack scratches his head .



Ram Narula
ram@pluslab .com

End of SMTP part

by Ram Narula ram@pluslab.com

File Transfer Protocol (FTP)

- Widely used, implemented in web browsers
- Communicates in plain-text (no encryption) for everything including username, password, and files
- Vulnerable to sniffing and Man-in-the-middle attacks (session hijack)

(Not as popular as email and web)

FTP Solution

- 2 major approaches
  - FTP over TLS/SSL
    - Secure but not popular yet
  - SFTP (File transfer using SSH based protocol)
    - Secure but not widely used except for SSH users (seems to be more popular than FTP over TLS/SSL)

Internet Explorer support for FTP

- Internet Explorer 6 (world's most popular browser) accepts ftps:// and sftp:// type URLs but will just revert to ftp:// and shows *"FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use Web Folders (WebDAV) instead"*

Technical implementation

- General implementation with list of supported SSL/TLS FTP server/client
  - *http://www.ford-hutchinson.com/~fh-1-pfh/ftps-ext.html*
- SFTP (SSH based)
  - *http://www.openssh.org*
  - *http://www.ssh.com/support/documentation/online/ssh/winadminguide/32/SFTP_Server.html*
- Microsoft IIS implementation
  - There seem to be no direct support for this. Instead of SSL/TLS for FTP, WebDAV (World Wide Web Distributed Authoring and Versioning) seems to be preferred.

References

- "RFC2487 - SMTP Service Extension for Secure SMTP over TLS" http://ftp.apnic.net/ietf/ietf-mirror/rfc2487.txt
- "S/MIME and OpenPGP" Internet Mail Consortium http://www.imc.org/smime-pgpmime.html
- "Filling SMTP gaps -- The secrets to using e-mail standards" by Joel Snyder http://searchsecurity.techtarget.com/general/0,295582,sid14_gci1067499,00.html
- "SSL versus TLS versus STARTTLS" by Jeremy Mates http://sial.org/howto/openssl/tls-name/
- "Browsers Statistics" by Refsnes Data http://www.w3schools.com/browsers/browsers_stats.asp

Supporter/Sponsorship

- This presentation has been created independently.

- Any supporter?
  - Please email me at ram@pluslab.com