FTC Presentation

Email Falsification
America Online, Inc.
April 2003

Intro to Email

- The Basics
  - TCP/IP, DNS and SMTP
- How Email Works
  - Transaction
  - Headers

The Basics: TCP/IP

- The Internet is a mesh of machines connected to each other by cables, wires, analog and digital lines, cells and satellites.
- TCP/IP (Transmission Control Protocol/Internet Protocol) is the language used by these machines, or servers, to communicate with one another.
- IP is responsible for moving packets of data between servers/nodes, whereas TCP is responsible for verifying data delivery from client to server.
- RFC: 791, 793 (http://www.rfc-editor.org)

The Basics: IP Addresses

- IP addresses are coordinates used to locate where servers on the Internet are with respect to each other. Every machine on the Internet has an IP address.
- The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. For example: 208.15.23.1. Each set of numbers is termed an “octet” or “netblock”, and each octet can be 0 to 255.
- RFC: 791

The Basics: DNS

- DNS (Domain Name System) is a distributed Internet directory which associates a domain name (like aol.com or ftc.gov) and the IP addresses of the servers which belong to that domain name.
- Most Internet services rely on DNS to work, and if DNS fails, web sites cannot be located and email delivery stalls.
- Tools: **nslookup** and **traceroute** from a networked unix host will tell you which domain is responsible for certain IP addresses, and vice versa, and what types of functions servers with those IP addresses perform
- http://samspade.org/
- http://nitrous.digex.net/mae/sn-lg.html (otherwise known as Mae East)
- RFC: 1034

The Basics: SMTP and Email

- SMTP (Simple Mail Transfer Protocol) is the procedure (generally on port 25) by which email data packets are transferred from one networked machine to another.
- There are thousands of different types of software which speak SMTP. Some software packages are free, others are not. Sendmail is the most widely used email software (it's virtually free and very reliable). Other well-known software packages are NTMail, Post.Office, Microsoft Exchange, SMI, and Eudora.
- RFC: 821, 822

Here's an SMTP example:

telnet mx1.mail.yahoo.com 25
Trying...
Connected to mx1.mail.yahoo.com.
Escape character is '^]'.
220 YSmtp mta121.mail.scd.yahoo.com ESMTP service ready
helo aol.com
250 mta121.mail.scd.yahoo.com
mail from:<XXXX@aol.net>
250 sender <XXXX@aol.net> ok
rcpt to:<testforftc@yahoo.com>
250 recipient <testforftc@yahoo.com> ok
data
354 go ahead
Date: April 28, 2003
From: Margot (XXXX@aol.net)
Subject: Test for FTC
This is a test...
.
250 ok dirdel
quit
221 mta121.mail.scd.yahoo.com
221 mta121.mail.scd.yahoo.com
Connection closed by foreign host.

How Email Works: Logging and Headers

- Headers are the mess of “received from” lines at the top/bottom of an email message.
- Headers are a recorded log of the specific route a particular email took from its destination to its arrival point.
- Theoretically, headers are stamped by every machine an email packet hits, in order, from bottom to top. The top most “Received:” line in a header is the last machine an email touched before it arrived in your mailbox.
- All header information, with the exception of the most recent (top-most) transaction, is forgeable.
- Lets take a look at the headers of the SMTP transaction I did.

Headers…

X-Apparently-To: testforftc@yahoo.com via 216.136.226.145; 28 Apr 2003 11:14:02 -0700 (PDT)
Return-Path: XXXX@aol.net
Received: from 152.163.224.70 (HELO aol.com) (152.163.224.70) by mta121.mail.scd.yahoo.com with SMTP; 28 Apr 2003 11:13:27 -0700 (PDT)**Date:** April 28, 2003
From: "XXXX@aol.net" <Margot@> | This is spam | **Add to Address BookSubject:** Test for FTCThis is a test…

Here's how easy it is to "forge" an email...

Side-effects of email forgery…

- Forged <return-path> fields cause bounce bombs injuring unrelated/innocent parties
- Fake “from” addresses damage the misrepresented organizations’ goodwill
  - the junkmail recipients’ anger is directed at the wrong organization/sender
  - dilution of “forged” organizations’ intellectual property rights
  - copycatting of an organizations’ legitimate products for nefarious reasons
- Fake/fraudulent headers aim to outwit filtering and law enforcement efforts
- Bogus domain registration information has a similar effect
  - New issue: “borrowing” zombie netblocks

Tools to detect forgery…

- Tools to help you determine the origin of an email
  - http://www.samspade.org
  - http://www.networksolutions.com/cgi-bin/whois/whois
  - http://www.arin.net/whois/index.html
  - http://www.ripe.net/db/whois/whois.html
  - http://www.apnic.net/apnic-bin/whois.pl
  - http://resellers.tucows.com/opensrs/
  - http://groups.google.com “news.admin.net-abuse.email” (N.A.N.A.E.)