Practical Traceability (101)

31st October 2000

by Richard Clayton
Reading List

http://www.linx.net/noncore/bcp/traceability-bcp.html

written by UK ISP industry;
edited by Richard Clayton
Outline

• TCP/IP refresher
• When IP addresses don’t work
• When IP addresses work
• Finding the source
• Dealing with dialup
• Hiding on a LAN
All you need to know about TCP/IP (almost)
Are addresses valid?

- Destination address is always valid
- Source address is valid for 2-way traffic
- Can do denial of service with 1-way traffic
- Can spoof addresses if stack poorly written
- Filters can be useful in providing validity; but beware of source routing
DoS: smurf attack

???.???.??.

194.70.55.255

128.232.15.208
Smurf protection

• Ingress filtering (RFC2267)
• Change directed broadcast rules (RFC2644)
• “Name and shame” lists for amplifiers
  http://www.netscan.org
• Low probability responses for tracking
• Detection of flows on border routers and at exchange points
Spoofing

• 3-way handshake
  --> SYN client offset
  <-- SYN-ACK server offset
  --> ACK

• If offset (and other info) is predictable don’t need to see the return traffic to have a successful conversation

• Described by Morris (85) and CERT (95)
Who owns an address?

- Regional registries issues numbers ARIN, APNIC & RIPE
- ISPs reallocate within their blocks
- Hence “whois” will yield owner
- Reverse DNS should also yield name
  eg: for 100.101.102.103:
    103.102.101.100.in-addr.arpa
If the owner is unclear?

• Traceroute may give a clue

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>59 ms</td>
<td>61 ms</td>
<td>64 ms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tele-border-12-168.router.demon.net</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>65 ms</td>
<td>66 ms</td>
<td>63 ms</td>
</tr>
<tr>
<td>7</td>
<td>64 ms</td>
<td>61 ms</td>
<td>63 ms</td>
</tr>
<tr>
<td>8</td>
<td>179 ms</td>
<td>66 ms</td>
<td>62 ms</td>
</tr>
<tr>
<td>9</td>
<td>62 ms</td>
<td>61 ms</td>
<td>63 ms</td>
</tr>
<tr>
<td>10</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>

Request timed out.

• ie: try to identify upstream providers
Traceability of email

Received: from pop3.demon.co.uk by rnc-portable.turnpike.com with POP3
   id "happyday.972662921:20:06557:0".happyday@pop3.demon.co.uk>
   for <happyday@pop3.demon.co.uk> ; Fri, 27 Oct 2000 17:09:15 +0100
Return-Path: <chris@cjt.co.uk>
Received: from punt-2.mail.demon.net by mailstore for richard@highwayman.com
   id 972662921:20:06557:0; Fri, 27 Oct 2000 16:08:41 GMT
Received: from finch-post-12.mail.demon.net ([194.217.242.41])
   by punt-2.mail.demon.net id aa2110410; 27 Oct 2000 16:08 GMT
Received: from cjt.demon.co.uk ([193.237.160.201])
   by finch-post-12.mail.demon.net with esmtp (Exim 2.12 #1)
   id 13pC3U-000CZt-0C
   for richard@highwayman.com; Fri, 27 Oct 2000 16:08:39 +0000
Traceability on USENET

Xref: news.demon.co.uk demon.ip.support.turnpike:53979
Path: news.demon.co.uk!demon!happyday.demon.co.uk!turnpike.com!richard
From: Richard Clayton <richard@turnpike.com>
Newsgroups: demon.ip.support.turnpike
Subject: Re: Can’t seem to set a global for email
Date: Sat, 28 Oct 2000 12:06:26 +0100
Message-ID: <ZtZltlCyMr+5EAty@turnpike.com>
References: <jsH65KAiZK+5EwqI@btinternet.com>
NNTP-Posting-Host: happyday.demon.co.uk
X-NNTP-Posting-Host: happyday.demon.co.uk:158.152.30.53
X-Trace: news.demon.co.uk 972731811 nnrp-12:7455 NO-IDENT
happyday.demon.co.uk:158.152.30.53
X-Complaints-To: abuse@demon.net
Traceability on IRC

• Need to map nickname to server to IP address
• May be intentionally untraceable

• Different policy aims may be present
  children should be anonymous
  dirty old men should not be anonymous
Identifying dialup users

- Dynamic IP is commonplace
- RADIUS logs connect and disconnect
- Hence from time + IP can deduce account

- Various “gotchas”
  - UDP means logs incomplete
  - Time may be inaccurate
  - Logs are large and only kept short-term
More practical problems

- RADIUS and IP allocation may be done by different organisations
- Account may be generic (sales promotion)
- Remote machine may only have DNS record (and hence IP address is deduced)
Identifying the user

- Ask them for name and address
- Credit card info
- Telephone callback
- Other relationship (store card, account no)
- Caller Line Identification (CLI)
CLI

• Engineering CLI travels to switches, user (or presentation) CLI can be withheld (141)
• ISPs will get engineering CLI “soon”
• CLI tends to fail:
  on international calls
  at telco boundaries
  when using bulk carriers
Passwords

• Passwords are poor identifiers
  ISP staff
  household
  post-it notes
  Usenet
  social engineering

• Accounts may be legitimately used by many people; so spotting extra use can be hard
Traceability on LANs

- A LAN is a broadcast medium
- Naïve to think MAC addresses are fixed
- Possible to steal MAC & IP addresses
- Hard to locate senders
  - big practical problem for DHCP
  - bridges know direction
  - can fingerprint the NICs
More complications

- Network Address Translation
  used to preserve IP address space
  used to hide network architecture
  unlikely to be logged

- DHCP
  dynamic allocation of addresses
  logging can be problematic
Authenticity

- Logs need to be authentic & correctly timed
- DNS needs to be trustworthy
- IP Allocations need to be documented
- Machines need to be secure
- Staff need to be trustworthy

nightmare scenarios:
chasing a sysadmin or ISP staff
Retention & Preservation

• Data Retention is a matter for Data Protection legislation; have to show a business need

• Data Preservation is at the request of Law Enforcement to prevent auto-erase. Work is going on within the G8 to provide trans-border requests and some form of fast divulge to allow multi-hop traceability.
“Real anonymity”

• Chained remailers (use Chaum MIXs)
• Freedom network (zeroknowledge.com)
• Anonymising caches
  not all they seem (www.privada.com)
• Onion routing (encrypted source routeing)
• “Crowds” (pass the parcel)
• DC-nets (Chaum again)
Review

- 2-way traffic means IP address trustworthy
- Registries and traceroute will locate ISP
- ISP logging will locate the account
- Account details will reveal user
- CLI will reveal dialup user
- Local records (NAT/DHCP) will reveal a LAN user
“Practical anonymity”

- Steal a password
- Use a free account and withhold your CLI
- Use a pre-paid WAP phone
- Use a cybercafe
- Use a LAN
- Multiple jurisdictions will slow tracing down
- NB: Best Practice is far from universal