Identity on the Internet

from the ISP viewpoint

17th June 2003

Richard Clayton, Thus plc

How do we know who people are?

- ISPs are just one more victim !
  - credit card fraud
  - “spam”
- Basic traceability
  - how TCP/IP works
  - who “owns” an IP address
  - dealing with dialup
- The “account owner” gap
- Practical anonymity on the Internet

Further reading

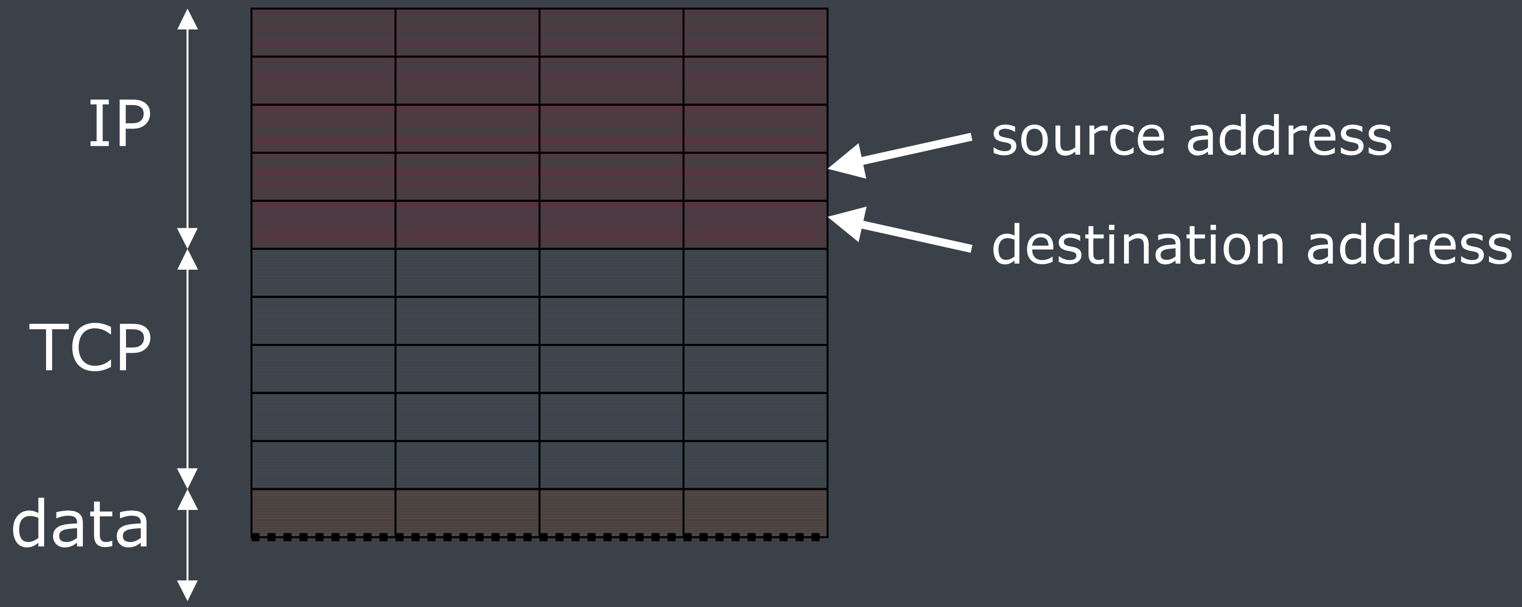
`http://www.linx.net/noncore/bcp/traceability-bcp.html`

written by UK ISP industry;
edited by Richard Clayton

`http://www.cl.cam.ac.uk/~rnc1/The_Limits_of_Traceability.pdf`

Richard Clayton

All you need to know about TCP/IP packets



Are addresses valid ?

- Destination address is always valid
- Source address is valid for 2-way traffic
  - spoofing is very rare
    and entirely reliant on old coding errors
- Can send single bad packets with 1-way traffic
  - ie denial of service (DoS, DDoS)
- Filtering would be a solution, but not practical

Who “owns” an address ?

- Regional registries issue numbers
- ie: ARIN, APNIC, RIPE & LACNIC
  - APNIC and LACNIC may delegate further
- ISPs reallocate within their blocks
- Hence “whois” will yield “owner”
- Reverse DNS *should* also yield a name

eg: for 100.101.102.103:
103.102.101.100.in-addr.arpa

- Traceroute will show you a route to them
  - the “upstream” network may know more

Traceability of email

```
Received: from pop3.demon.co.uk by rnc1.al.cl.cam.ac.uk with POP3
 id <"happyday.1009968986:20:22479:12".happyday@pop3.demon.co.uk>
 for <happyday@pop3.demon.co.uk> ; Wed, 2 Jan 2002 10:56:39 +0000
Return-Path: <mvcic@caramail.com>
Received: from punt-2.mail.demon.net by mailstore for
    richard@happyday.demon.co.uk
          id 1009968986:20:22479:12; Wed, 02 Jan 2002 10:56:26 GMT
Received: from servovalle.ipvcov.cl ([164.77.204.218]) by punt-
    2.mail.demon.net
           id aa2022374; 2 Jan 2002 10:56 GMT
Received: from mx2.mortgageloanfast.com (slip-12-64-210-233.mis.prserv.net
    [12.64.210.233])
    by servovalle.ipvcov.cl (8.9.3/8.8.7) with SMTP id HAA18642;
    Wed, 2 Jan 2002 07:13:59 -0300
From: mvcic@caramail.com
Date: Wed, 02 Jan 2002 03:55:22 -0700
To: yearned@internetz.com
Message-Id: <31gb2y88su1gmy.7gaa6vrr2gt@mx2.mortgageloanfast.com>
Subject: Save Money on Your Mortgage Payment!
```

```
% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html
inetnum:      158.152.0.0 - 158.152.255.255
netname:      DEMON-NET
descr:        DEMON INTERNET
descr:        UK's Premiere ISP
country:      GB
admin-c:      DHG5-RIPE
tech-c:       DIHD-RIPE
rev-srv:      ns0.demon.co.uk
rev-srv:      ns1.demon.co.uk
rev-srv:      ns2.demon.net
status:       ASSIGNED PA
mnt-by:       AS2529-MNT
mnt-lower:    AS2529-MNT
changed:      sam.bradford@demon.net 20000714
changed:      sam.bradford@demon.net 20010123
changed:      annap@demon.net 20011120
source:       RIPE
route:        158.152.0.0/16
descr:        DEMON-NET
origin:       AS2529
remarks:      *********************************************************
remarks:      * ABUSE CONTACT: abuse@demon.net IN CASE OF INTRUSIONS, *
remarks:      * ILLEGAL ACTIVITY, ATTACKS, SCANS, PROBES, SPAM, ETC.  *
remarks:      *********************************************************
mnt-by:       AS2529-MNT
changed:      sam.bradford@demon.net 20020607
source:       RIPE
```

"whois 158.152.30.53"

Identifying the user

- Ask them for name and address!
  - marketing people like this idea
- Credit card info
- Two way telephone calls
- Other relationship (store card, account no)
- Caller Line Identification (CLI)
  - can be withheld by user (141)
  - fails on international calls
  - fails with bulk carriers
  - fails at telco boundaries

Who uses an account ?

- 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

More complications !

- LANs are a broadcast domain
  - and 802.11 wireless is very insecure
- Network Address Translation
  - unlikely to be logged
- DHCP
  - dynamic allocation of addresses
  - logging can be problematic
- Logs may be poor
  - only containing DNS names
  - poor time synchronisation

“Practical Anonymity”

- Using MIXmaster remailers and NYM servers is (embarrassingly) hard to do. anonymizer.com and JAP are a nuisance…
- … and there’s lots of “real world” anonymity available without special tools!

- Examine the chain of deduction that is being called “Traceability”

  A) Almost any deductive link can be “attacked”

  B) Almost any link can fail through lack of “Best Practice”

A) Attacking the assumptions

- Steal a password
  - but CLI will catch you
- Use a free account and withhold your CLI
  - telco (C7) logging may track you
- Use a pre-paid WAP phone
  - but don’t give your number to mum!
- Use a cybercafe
  - but beware of CCTV
- Use a LAN (maybe steal a MAC/IP address)
  - but this is hard, even for techies

B) Authenticity failures

- 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

Top tip!

Use multiple jurisdictions

Review

- 2-way traffic makes an IP address trustworthy
- Registries and traceroute will locate ISP
- ISP logging will locate the account
- Account details will reveal user
- CLI will reveal dial-up user
- BUT the last hop may not lead you to exactly the right person, especially if looking for a skilled adversary who can “frame” an innocent bystander
- Real world anonymity can be ridiculously easy!