The Limits of Traceability

Richard Clayton

Presented at: Internet Awareness Day @ NSY, Wed 1st Oct 2003

What’s in this talk?

- Refresher on Internet “traceability”
- How to cock it up!
- Authenticity failures
- How to subvert (all of) the assumptions
- Real world anonymity
- What does this mean?

Refresher

- Start with an IP address & the time
  - from web logs or email headers
- Work out which ISP it belongs to
  - traceroute, asking RIPE etc
- Ask that ISP for who used the IP address
  - RADIUS logs give the account
  - customer records will yield user identity
- Break down the door!

How to cock it up!

- Incorrect timestamp => incorrect person
  - check those clocks!
- Incorrect timezone => incorrect person
  - learn to deal with -0500 (and BST)!
- Avoid typos (use cut & paste!)
  - 224.xx.xx.xx is detectable, others will not be!
- and who owns 172.31.5.29 ?
  - IANA: it is in RFC1918 address space !

The need for tools

http://www.LloydsTsb.co.uk:account@2162688020

http://www.barclays.co.uk:account@0200.232.0.20

http://www.paypal.com%2f@%32%31%31%2e%31
%31%33%2e%31%38%36%2e%34%32/%70%70/%70
%72%6F%63%65%73%73%69%6E%67%2E%68%74%6D

Authenticity failures

- Logs need to be authentic & correctly timed
- DNS needs to be trustworthy
  - Best Practice is to log IP addresses as well
- IP allocations need to be documented
- Machines need to be secure
- Staff need to be trustworthy

nightmare scenario :

chasing a sysadmin or ISP staff

Assuming IP address is correct ?

- Is it a web cache ?
  - Perhaps there are records? (gotta be QUICK!)
- Is it DHCP ?
  - Perhaps there are records? (or no changes!)
- Is it a NAT box ?
  - Perhaps there are records? (you’re joking!)
- Is the IP address spoofed ?
  - Do you have a database that records the risk?

TCP spoofing

- Standard TCP 3-way handshake:

A-->B	SYN	client offset
A<--B	SYN-ACK	server offset
A-->B	ACK	

- If offset (& other info) is predictable don't need to see the return traffic to have a successful conversation
- Described by Morris (85) and CERT (95)
  - Still happens in obscure devices & FreeBSD (2000)

Assuming IP ownership ?

- Trafalgar House IP block “stolen”
  - first they knew was a phone call to their abuse desk
- Many more IP blocks have been borrowed
  - spammer forges documents to send to ARIN
  - spammer persuades ISP to route the packets
  - all routes lead to true owner (off-Internet usage)
- Community now active in monitoring this
  - Richard Cox: “hijacked” mailing list

Assuming account = person ?

- Usually credentials are just a password
  - available to anyone nearby (from yellow sticky)
  - available to maintenance staff (eg Kwong Leu Wong)
  - may be available to Usenet readers
  - can be available to ISP staff
  - always available to a “social engineer”
  - and many accounts are “company” accounts anyway
- WiFi available to anyone within range
  - after 8 hours, even if encrypted

ADSL credentials

- DSLAM sets up PVC to “Home Gateway”
- Home Gateway passes the credentials along to the ISP’s RADIUS system
- ISP allocates IP address to user
  - probably doesn’t even need to change the routeing
- Note that only the Home Gateway can know which DSLAM the IP packets are being sent towards -- so check its logs (oops!)

“Academic” anonymity

- MIXmaster and MIXminion remailers
  - provably secure anonymity properties
  - NYM servers hide identities
  - NSA might be able to attack them, but so what?
- JAP web mixes
  - provably secure, except that servers were in one room, so fell to a court order (& then a search warrant!)
- Usenet
  - broadcast nature means receiver anonymity

Real world anonymity

All these fancy systems are a pain to use…

… so what would I recommend ?

How to hide in cyberspace: I

- Steal a password
  - but CLI will finger you
- Withhold your CLI
  - but telco switch (C7) logging may catch you
- Use a pre-paid mobile
  - but don’t give your number to mum!
- Steal a wireless connection
  - but don’t check your email whilst you’re online

How to hide in cyberspace: II

- Use other people's machines
  - 680,000 machines are "open relays" for email
  - worked really well for the Sobig.f author
- Use a cybercafe (or an airport, or a hotel…)
  - but beware of the CCTV
  - however, WiFi will allow you to collect passwords
- Use your office machine
  - but "borrow" an IP address or even a MAC address

Top tip !

Use multiple jurisdictions

Review

- Locating the account from the IP address is only the start of the process
- Many simple ways to hide the connection between an ISP account and a person
  - this isn't an accident, who's paying for traceability?
- A skilled adversary can readily "frame" an innocent bystander
  - so think about what sort of person you're chasing

What does this mean?

Traceability is NOT infallible

even when you don’t cock it up

You need to ask if the result that traceability produces is entirely credible -- and to be prepared to keep an open mind as other evidence becomes available to you

More at…

http://www.cl.cam.ac.uk/~rnc1/