All your mailserver are belong to us

Dr Richard Clayton

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

LINX 60
11th February 2007

CAUTION

This talk describes attacks on Internet infrastructure, especially DNS & BGP. But, not all of these attacks work everywhere, and people may be reluctant to discuss whether they work or not in their part of the real world. So don’t assume it’s all entirely true! However, it isn’t entirely false either!

Any mention I make of particular networks, ISPs or countries is merely to make abstract ideas concrete, not an analysis of actual flaws.

NB: Do not try any of this at home (OR at work)

Threat Scenario

- I wish to capture a significant amount of incoming email to a major ISP mail server
  - email may contain passwords etc
  - email can be made to contain passwords etc
  - answering email often “proves” identity
  - obvious opportunity to blackmail the ISP, or just trash their reputation as being secure
- Attack should “scale” to many ISPs
  - 0-day exploit on `sendmail` not considered here

Resources

- Back bedroom attackers
  - now have control of a reasonable size botnet
- Criminal entrepreneurs
  - may own (or 0wn!) a smallish ISP in Ruritania
- Organised crime ??
  - simpler for them just to bribe an employee!
- I am NOT assuming that BGP or DNS are too obscure to be attacked effectively

Underlying Strategies

- Cannot just steal packets – people notice
- Accept email, resend to the correct ISP
  - top 50 senders is a give-away, so use botnet
- Reject end of data with a 4xx response
  - email generally re-delivered after a delay, so suitable for intermittent attacks
- Tunnel SMTP packets to correct place
  - either a peer of target or customer within target

DNS (I): Active Attacks

- DNS server asks for data
  - attacker supplies incorrect answer first
    - 16 bit identifier is not long enough!
    - but, modern software randomises request port
- Older software is flawed
  - predictable random numbers!
    - or even accepts non-authorised data!
- No-one monitors for attacks
  - however this scales badly, so of limited interest

DNS (II): Phishing

- Rock-phish gang spoofed GoDaddy Aug07
  - probably just wanted some cheap domains
  - BUT control of a registrar account permits changes to name server identities
- Registrars for grown-ups will check validity of changes out-of-band, $10 hosting will not
  - significant number of US banks were vulnerable
- Attack vector might also be malware…

Attacks on BGP

- Basic idea: announce a /32 for mailserver
- Traffic then flows to Ruritania
  - email contents are available for inspection
- /32 may not propagate, so /24 may be better
  - leads to complexity if other hosts or services
  - hence tunnelling packets back to ISP may be best (and just sniff them as they pass)
- Sniffing possible anyway at other ISPs
  - difference here is scale and remoteness

More Specifics…

- Route should not be accepted
  - mnt-lower prevents creation of new route objects
  - so everyone ought to notice that route isn't valid
  - complexities with multiple registries
- Route may be spotted by monitoring
  - MyASN @ RIPE, Renesys etc
  - note that bogon filtering hides route from owner! and so Best Practice prevents give-away failures

Unauthorised Announcements

- Existing route: hope to be a shorter AS path
  - so more effective in Ruritania than London
- May help to forge origin for peer to accept the route (entirely dependent on filters)
- Once again, monitoring detects wickedness
  - but registry data error-prone and incomplete so can perhaps only consider changes
  - and of course you need to know all about multi-homed customers! Is this possible?

SMTP Defence I: Encryption

- Opportunistic encryption (RFC3207)
  - uses STARTTLS capability & command
  - negotiate mutually acceptable algorithm
- Plus points:
  - works out of the box for major MTAs
  - only end-points can decrypt the traffic
- Minus points:
  - increases processing load (may not matter)
  - no “man-in-the-middle” protection

SMTP Defence II: Authentication

- Check certificates before sending email
  - prevents man-in-the-middle
- Plus points:
  - works out of the box for major MTAs
- Minus points:
  - increases processing load (may not matter)
  - needs a Public Key Infrastructure (or a lot of bilateral arrangements)

Network Defences

- Anti-spoofing filters on customer links
  - motherhood! (but tedious for custom customers)
- Much harder to do on border routers
  - unicast reverse path forwarding (RPF) can help
  - but at IXPs this may not be practicable
- Can check if traffic coming from correct peer
  - straightforward(ish) sFlow/Netflow analysis

Secure DNS/BGP

- Secure DNS almost here
  - some TLDs already signed, more to come
  - unlikely that will be fully deployed for years
- Secure BGP(s) experimental at present
  - concerns about performance (cf MD5)
  - concerns about key distribution
  - when will it be stable and inter-working?

Blended Attacks

- Some key distribution schemes use DNS
- Attack the DNS and you may be able to compromise systems that are “secure”
- Best use of a BGP attack may be to capture the DNS servers (think long TTL), and then you can go after the mail servers at leisure!
- …and of course you may just want to DoS
  - so you don’t mind if your attack is noticed

Negligence

- The failure to use reasonable care
- Current test for “duty of care”:
  - harm must be (1) reasonably foreseeable
    (2) there must be a relationship of proximity between the plaintiff and defendant and
    (3) it must be “fair, just and reasonable” to impose liability
- If one of my attacks is effective on your mailserver, are you negligent?

Best Practice

- Legal principle of the “reasonable person”
  - what are the community standards?
  - stating that it’s impractical to prevent bad route announcements is one thing, having a community document that says what is and is not effective to put in place is more useful
- No protection for the incompetent!
  - but raises standards all round
  - and limits expectations when security “too hard”

More BGP Stuff

- RIPE

  MyASN & lots of other initiatives

- Experimental alerting systems

  `http://iar.cs.unm.edu/alerts.php`

  `http://phas.netsec.colostate.edu`

- Anirudh Ramachandran and Nick Feamster

  SIGCOMM 2006: Understanding the Network-Level Behavior of Spammers

All your mailserver are belong to us

http://www.lightbluetouchpaper.org/

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

LINX 60
11th February 2007