Infrastructure Security

Nicolas FISCHBACH [nico@colt.net]

Senior Manager - IP Engineering/Security

RIPE46, nsp-sec BoF - Sept. 2003

Agenda

- DDoS and Trends
- How to mitigate these risks: Infrastructure Security
- Conclusion

- "Contributors"
  - COLT Telecom: Marc Binderberger, Andreas Friedrich
  - Cisco Systems: Michael Behringer
  - Subscribers from:
    - nsp-sec*: http://puck.nether.net/mailman/listinfo/nsp-security[-discuss]
    - emea-sp-sec-forum: (talk to Michael [mbehring@cisco.com])

DDoS and Trends (1/2)

- What's the trend in attacks ?
  - Yesterday: bandwidth abuse, exploiting bugs
  - Today: packets-per-second, also against (core) routers
  - Tomorrow:
    - QoS/"extended" header
    - (InterAS) MPLS VPNs' trust model
    - IPv6 (transition)
    - Somewhere in the forwarding path code
    - Non-spoofed sources (who cares if you have 100k+ bots anyway)
    - Protocol complexity attacks (mixed with/hidden in/part of "normal" traffic): ie. low bandwidth "special" packets
    - Another "what's that packet with tcp.win == 55808" ?
    - Is the issue really BGP/DNS hijacking ?

DDoS and Trends (2/2)

- What if ?
  - The guys who wrote recent worms had a clue (or different objectives) ?
  - The latest major IOS bug had leaked or Cisco decided to do a public release ?
  - This is only the top of the iceberg… and our future ?

burning bridges where we can

Phenoelit

Cisco Vulnerabilities - The Past, The Present and The Future
http://www.phenoelit.de/stuff/camp2003.pdf

More (Vulnerable) Embedded Systems
http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-FX.pdf

Infrastructure Security (1/4)

- (Where/What) should you filter/rate-limit...
  - Edge and/or Core
  - Transit and/or Peerings
- … depending on …
  - I’m a Tier1 transit provider
  - I’m a Tier2/3 access provider (w/ broadband home users)
  - I’m an enterprise
- …. and also on ...
  - Capabilities/limits of the HW/SW deployed
  - Scalability and ease of operations of the solution
- … and what ?
  - Protocols, source/dest IPs, source/dest ports, other parts of the (extended) header, etc.

Infrastructure Security (2/4)

- Router Security 101
  - VTY ACLs, avoid passwords like “c”, “e”, “cisco”, “c1sc0”, use AAA
  - Account for BGP sessions (will you notice if somebody adds a session in a full-mesh configuration or on a peering router with 60+ peers ?)
  - Configuration/ROMMON/IOS integrity
  - Minimal services, logging, restricted SNMPd
  - Leaking configurations to customers with shared/common passwords/communities/etc.
  - Apply the same strict policies to peerings and transits than to customers
  - uRPF (this is not really deployed, even in loose mode)
  - etc.

Infrastructure Security (3/4)

- iACLs (Infrastructure ACLs)
  - why should any person connected to the Internet be able to talk to your core routers ?
- rACLs (Receive ACLs)
  - makes it easier to maintain and protect the RP
- tACLs (Transit ACLs)
  - filter on the forwarding path (core<->{edge,transit/peering} (permit ip any any) to allow easy changes

Infrastructure Security (3/4)

- Re-colouring
  - {out,in}coming: enforce (on) your administrative boundaries
- Rate-limiting
  - which protocols and what does it break ?
- Diversion capabilities
  - see “MPLS-based traffic shunt” f.e.

The Future

- What will LI (Lawful Intercept) also provide ?
  - A cool remote sniffer for Network Operations to dump traffic without having to pray or say “oops!” each time they press “Return” after entering “debug ip packet details” ?
  - An easy way for an attacker to do the same ?
    - The router is not the only device you may have to own, the MD (Mediation Device) is also part of the game
- What if somebody comes up with an attack that can be triggered on the forwarding path ?
  - Well, let’s ask the PSIRT crew ;-))
- “Commercial” worms
- Netflow and BGP as the “next-generation” forensics tools ?

Thank you