Backbone Infrastructure Attacks and Protections

draft-savola-rtgwg-backbone-attacks-01.txt

Pekka Savola

Introduction

- Describes a view of ISP backbone network attacks
  - Lots of folks in IETF and elsewhere had quite different ideas what’s out there
  - Particularly on..
    - The need for TCP-MD5
    - Ingress/egress filtering at borders
  - This very operational document tries to harmonize that view

- Administrativia
  - It is not clear what is the right home for this
  - RPSEC? OPSEC? Invididual? Drop?

Document structure

- Scope
  - Backbone infra and critical protocols required to function for legitimate traffic to be correctly forwarded
  - Out of scope e.g., AAA, NTP, syslog, SNMP, DNS, ...
- Assumptions and threat model
- Typical attack vectors
- Countermeasures
- Protocol analysis
  - how countermeasures apply to the attack vectors

Assumption and threat model

- Assumption
  - SP is doing at least some filtering at the borders
    - So that no one can spoof infrastructure addresses
- Threat model focused on external attacks, e.g.,
  - DoS attacks directed at infrastructure
  - DoS attacks directed at whoever but cause harm to infrastructure
  - Infrastructure access hijacking attemps
- Out of scope, e.g.,
  - Lower-layer attacks (e.g., MITM insertion on a fiber)
  - Insider attacks or router compromise
    - Likely detected by change management etc.

Typical attack vectors

- Lower-layer attacks
  - Physical link security is typically not an issue
- Generic DoS on the Router
  - E.g., sending hop-by-hop options that get punted to slow-path
- Generic DoS on a Link
- Cryptographic Exhaustion
  - E.g., TCP/MD5 or control-plane IPsec attacks
- Unauthorized Neighbor or Routing
  - E.g., careless IGP configuration or BGP filtering
- TCP RST Attacks
- ICMP Attack
  - Even worse than TCP RST attacks

Typical countermeasures

- Filtering addresses in packets
  - Ingress filtering your own blocks assumed
  - Egress filtering that allows only your own addresses recommended
- Filtering addresses in routing updates, e.g.,
  - Filter out your own routes and more specifics
  - Define maximum prefix limits to avoid de-aggregation
- GTSM
  - Deploy on eBGP sessions as 1st order protection
  - GTSMbis spec should say define TCP-RST TTL handling
- TCP-MD5 and other custom authentication
- IPsec and IKE
  - Heavyweight, not well supported, difficult to configure

Protocol Analysis (1/2)

- ICMP attacks apply to all the protocols :-(

- OSPF
  - Config audits to prevent unauthorized neighbors
  - OSPF protocol needs to be blocked at borders
- IS-IS
  - Config audits to prevent unauthorized neighbors
- BFD
  - Uses GTSM so OK

Protocol Analysis (2/2)

- BGP
  - iBGP requires no protection (spoofing protection enough)
  - eBGP with GTSM is typically good enough
    - single-homed customers require no protection
    - multi-homed customers a bit trickier, depends on whose p2p addresses used
    - upstream may use TCP-MD5 but only upstream could reset
    - IX peering fabrics should probably use TCP-MD5
  - Content security (routing update verification) a SIDR topic
- LDP
  - Removed due to lack of experience
- Multicast protocols (PIM-SM, MSDP, etc.)
  - draft-ietf-mboned-mroutesec
  - draft-savola-pim-lasthop-threats
  - Bottom line: vendor-specific rate-limiters etc.

Summary

- Protecting IGP is rather straightforward
- Protecting BGP transport is relatively easy with filtering and GTSM
  - TCP-MD5 just reduces the attack vector
  - Threats and necessity of TCP-MD5 seem overemphasized
- Various router DoS attacks require vendor-specific rate-limiting etc.

- Open issues for the IETF
  - ICMP attacks against non-TCP protocols
    - E.g., IPsec’s by-default ICMP handling is underspecified
    - SCTP, DCCP, UDP, ...
  - GTSM TCP-RST clarification wrt TTL