# Securing the Router Infrastructure

Ross Callon
Distinguished Engineer

Juniper™ NETWORKS

# Agenda

- **Securing the router infrastructure**
- **Examples of attacks and defenses**
- **A call to action**
- **References**

# Agenda

- **Securing the router infrastructure**
- Examples of attacks and defenses
- A call to action
- References

# Securing the Router Infrastructure

- Links, routers, routing protocols, and management thereof
  - Are critical network components
  - Must work securely
- These can be strongly secured
  - Very few systems have a valid reason to send traffic *to* the router's control plane

    (rather than *via* the router's data plane)

# Invisible Routers

- Packet filters block end user data to routers
  - Not *via* routers, of course ;-)
- Configuration (or filters) blocks data from routers to end users
- "Holes" are poked in filters for
  - Other internal routers
  - EBGP peers
  - Network management stations
  - Directly attached hosts / subnets (eg, servers)

# Filter Issues

- Location
  - At ingress to the network, or
  - At ingress to the router
- How to specify "all packets to routers in this net"
  - If routers use dedicated common address prefix, this may be easy to specify
  - Otherwise, may be difficult or impractical
- Performance must be acceptable
- Packet filters versus “null” routes at edge

# Untouchable Routers

- In some cases routers may need to be visible
  - Eg, ICMP to directly attached hosts, PE routers, allow traceroute, multicast
- Traffic to routers can be limited
  - Filtered to limit access
  - Rate limited to prevent resource saturation
  - Source address verification to prevent hackers from getting around filters
  - (Stateful filters to protect E-BGP sessions, directly attached hosts)

# Protecting Routing Protocols

- Routing traffic may be authenticated or encrypted
  - Prevents unauthorized systems from hijacking routing protocols
- Compromised routers are a potential problem
- Does not protect against DoS
  - Protect router's CPU
  - Prioritize routing traffic on links
  - Compartmentalize resources

# Protecting Network Management

- Compromised routers are potentially very bad
- Network Management is a significant current vulnerability
  - Poor password selection
  - Simple passwords + decryption / sniffing tools
  - "Password crackers can now break anything that you can reasonably expect a user to memorize"

    (Bruce Schneier, Secrets and Lies)

# Management and Control

- Login Authentication
  - One-time passwords
  - Change control
  - Logging
  - Secure the machines that control all of this
- Out-of-band management access

  (logical or physical)
- Filtering access to management plane
- Automate repetitive tasks

# Router Implementation Details

- Separate Data Plane from Control Plane
- Prioritize critical control traffic and processes
  - On ingress to router, egress from router
  - CPU, memory, data paths internal to router
- Compartmentalize resources
  - Guarantee resources to specific processes
  - Limit resources used by multicast
  - This puts requirements on Operating System

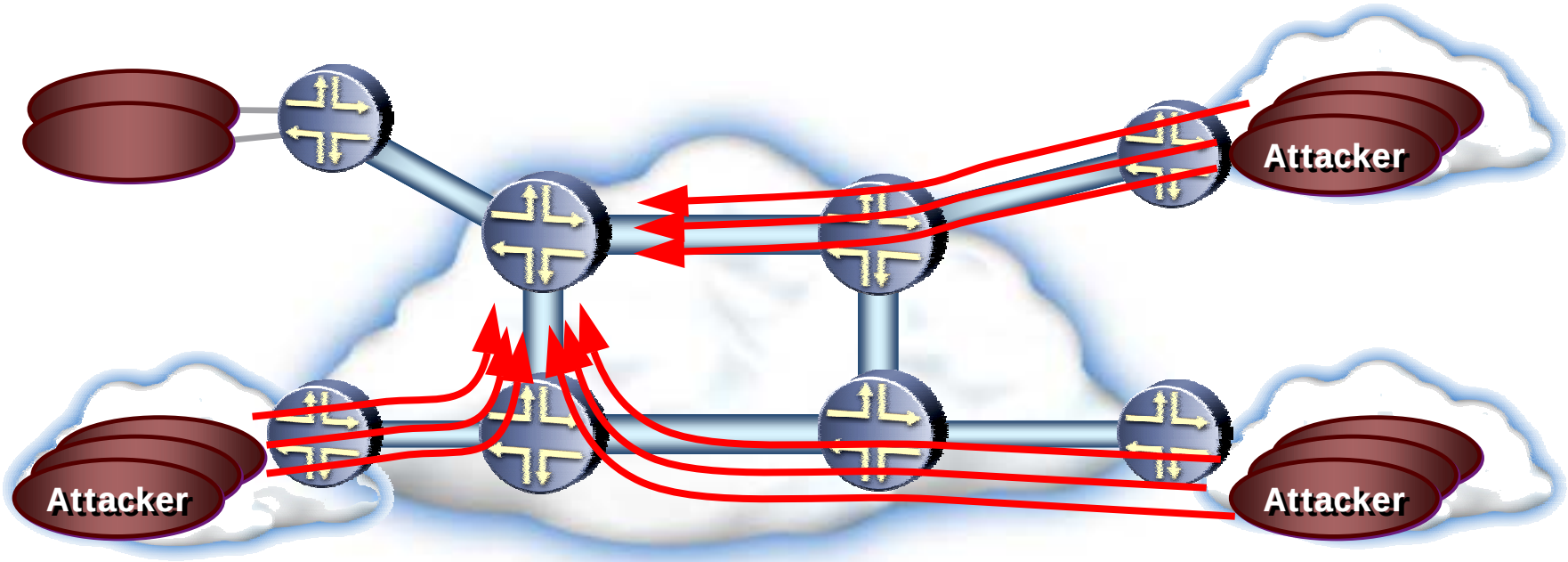
# Servers on the Router?

- Some have proposed putting servers on the routers
- Servers are *fundamentally* less secure
  - Many systems have a legitimate reason to send traffic to most servers (eg, DNS, WWW)
  - Server software is frequently not secure
- In theory this might be securable
- In practice, opens up major vulnerability

# Agenda

- Securing the router infrastructure
- **Examples of attacks and defenses**
- A call to action
- References

# DDoS Attacks versus Routers




- Attacker compromises multiple hosts, using them for coordinated attack
- Any device attached to network *will* be attacked (including routers)
- Packet filters are most direct way to handle DDoS vs routers
  - Preferably turned on a priori

# Slammer, January 2003

- Slammer worm
  - Self-contained worm in one UDP message
    - Used otherwise unused UDP ports
  - Random source and destination addresses
  - Very rapid propagation (doubles in ~8sec)
  - Widespread congestion throughout Internet
- Results were “interesting” from a router and network design viewpoint

# Some Slammer Lessons

- One major service provider was unaffected
  - Had turned off unused UDP Ports a priori
- Packet filters used to shut down attack
- Many networks were seriously impacted
  - Many deployed routers have inability to filter without severe performance impact
  - Some routers lost Hellos $\Rightarrow$ links disconnected
  - Network management failures
  - Processor failure / congestion

# Agenda

- Securing the router infrastructure
- Examples of attacks and defenses
- **A call to action**
- References

# Critical Basic Router Security

- Protect Network Management
  - Eg, Log access, One-time passwords
- Line-rate packet filtering and rate limiting
- Protect control traffic during congestion
  - Routing should be stable at all times (even during a DoS attack)
  - Network management should be available at all times (even during a DoS attack)

# A Call to Action

- Security is a long term issue
- Develop security strategy
- Educate staff
- Deploy the most obvious protection
- Deploy equipment which is *capable* of critical basic router security
  - When you need it, this turns a major forklift upgrade into a configuration problem
- Pay attention to performance

# Agenda

- Securing the router infrastructure
- Examples of attacks and defenses
- A call to action
- **References**

# NRIC Best Practices for Security

- Network Reliability and Interoperability Council (NRIC) has put together best practices for network security
  - Go to NRIC Main Page:  www.nric.org
  - Click on "NRIC best practices". This takes you to the Best Practices Selector Tool
  - In the "Add Keywords" box at the bottom left, select "Cyber Security"
  - Scroll down, Hit "Go"
  - See 175 cyber-security best practices
- SPs are encouraged to: Study, prioritize, deploy *where appropriate*

# **RFC 3871**: Operational Security Requirements for Large ISP IP Network Infrastructure

- This is based (with permission) on internal requirements of a major service provider
- Provides excellent overview of requirements for secure equipment
- IETF OPsec working group is continuing effort
  - General Discussion: opsec@ops.ietf.org
  - To subscribe: opsec-request@ops.ietf.org
  - In Body: subscribe

# Juniper Papers

- Juniper Networks Router Security, Best Common Practices for Hardening the Infrastructure

  www.juniper.net/solutions/literature/app_note/350013.pdf

- Internet Processor II ASIC: Fortifying the Core

  www.juniper.net/solutions/literature/app_note/350002.pdf

- Minimizing the Effects of DoS Attacks

  www.juniper.net/solutions/literature/app_note/350001.pdf


Juniper™ NETWORKS

Thank You