Control Plane Security for Hybrid Networks

Chris Tracy
Mid-Atlantic Crossroads (MAX)

Tom Lehman
University of Southern California
Information Sciences Institute East (USC/ISI-E)
Why are Hybrid Networks Vulnerable?

- Data channels may be operating at layer 1 and layer 2, but ...
- Management and control channels operate at layer 3!
  - Protocols used to provision services are IP-based
  - Protocols for configuration and monitoring are also IP-based
Motivations for Malicious Attacks

• Many temptations are similar to L3 nets:
  – Denial-of-Service
    • Capability to “take down” the network
  – Ability to send huge flows
    • Instead of using botnets, maybe attacker gets access to a host with 10GigE NIC and has ability to provision services
  – Traffic snooping
    • How valuable is the traffic?
    • Is it proprietary or confidential?

• Others are not:
  – Creation of backdoor routes
    • Ability to bypass the regular IP network
    • Ability to bypass firewalls or IDS systems
Generic Network Element

Consider all of the components in a network element:

- Management Plane
  - monitoring
  - configuration
  - provisioning

- Control Plane
  - signalling
  - routing
  - path computation
  - link management

- Data Plane
  - switch fabric
  - cross-connects
  - data interfaces

Telnet, ssh, TL1, SNMP, NTP, syslog, TFTP, HTTP, etc.

control channels to adjacent elements

data channels (OC-192, 10GigE, DWDM, etc.)
Identifying Attack Vectors

- **User access control and policy**
  - Web pages and APIs are increasingly being used to provide end-user with interface for creating circuits
  - Potential for hijacking of end-user credentials
  - Potential for compromised certificate authority

- **Attacks on the control plane**
  - Major concern: injection or snooping of control traffic
  - May compromise the ability to manage or provision new services
  - Example: Denial-of-Service attacks
    - Does not require attacker to be able to generate large inbound flows!
    - Attacker must have some access to control channels
      - Spoofing control plane traffic
      - Man-In-The-Middle (forgery/injection)
Identifying Attack Vectors

• **Attacks on the management plane**
  – Using public IP addresses with no access restriction
    • Opens up more holes for attackers
  – Exploiting weak passwords
    • Vulnerable to dictionary attacks
  – Snooping of management plane traffic
    • Recover passwords from Telnet/TL1/HTTP sessions
  – Bad crypto implementation by vendor
    • Predictable initialization vector

• **Attacks on the data plane**
  – Fiber tapping
  – Backdoor routes to bypass IP network
    • May be done to bypass firewalls or IDS systems
Case Study: Control Channels

- **GMPLS allows for separation of control and data plane**
  - Unlike MPLS, control traffic
  - Underlying transport technology for data channels is not necessarily IP
    - Not forwarding traffic based on IP headers
    - May be able to carry IP but are not L3 packet-switch capable (PSC) routers
    - E.g. WDM, SONET/SDH, 802.1Q VLANs
  - **Realization of control channels**
    - May be in-fiber, in-band (SONET overhead bytes)
    - May be in-fiber, on separate lambda (1310nm OSC)
    - GMPLS also allows for control channel to be out-of-band – for example: over an IP network
Case Study: Control Channels
DRAGON Virtual Label Switching Router (VLSR)

- Linux PC implements GMPLS control plane protocols
- Control channels may be provisioned in-band or out-of-band

One goal of DRAGON’s VLSR software is to provide GMPLS protocol support for devices which do not support GMPLS
Assuming underlying network uses Ethernet VLANs, control channels may be provisioned in-band with static control VLANs.

In-band control channels are considered somewhat less vulnerable than out-of-band (RFC3945).
Case Study: Control Channels
DRAGON Virtual Label Switching Router (VLSR)

- Control channels could also be provisioned out-of-band via GRE tunnels over an IP network

IPsec is one of several mechanisms recommended for securing out-of-band control channels provisioned over IP networks (RFC3945)
Case Study: Control Channels
Mitigation Strategies

• **Control Plane:**
  – Minimize risk of attackers being able to snoop/inject traffic
  – Threat is dependant on how control channels are provisioned
    • Use IPsec to secure out-of-band control channels
      – E.g. encrypt GRE tunnel traffic between adjacent nodes
    • In-band control channels may be considered less vulnerable

• **Management Plane:**
  – Use ACLs on routers/firewalls
    • Limit access to trusted hosts or networks
  – Implement a VPN for accessing management plane
    • Use private addresses to access nodes
  – Use strong passwords, avoid re-use
  – Consider using SNMPv3 (if supported)

• **Data Plane:**
  – Rely on physical security
  – Implement local administrative policy
    • Limit total available bandwidth to particular user/group at a particular time
References

- **IETF**
  - RFC3945 – GMPLS Architecture
  - RFC4230 – RSVP Security Properties
  - draft-ietf-mpls-mpls-and-gmpls-security-framework-02 (MPLS WG draft)

- **OIF**
  - OIF-SEP-01.0 - Security Extension for UNI and NNI
  - OIF-SEP-02.1 - Addendum to the Security Extension for UNI and NNI
  - OIF-SMI-01.0 - Security for Management Interfaces to Network Elements
  - OIF-SMI-02.1 - Addendum to the Security for Management Interfaces to Network Elements
Thank You

• **Questions?**
  – **Chris Tracy**
    • chris at maxgigapop.net
  – **Tom Lehman**
    • tlehman at east.isi.edu

• **DRAGON Software available as part of the I2 DCN Software Suite:**
  – https://wiki.internet2.edu/confluence/display/DCNSS