Protecting your IP network infrastructure

“how to secure Cisco routers and (multi-layer) switches running IOS/ CatOS and the networks they interconnect”

> Nicolas FI SCHBACH
Senior IP and Security Engineer
Professional Services Team - COLT Telecom
nico@securite.org - http://www.securite.org/nico/

> Sébastien LACOSTE-SERIS
IP R&D Manager - Security Officer - COLT Telecom
kaneda@securite.org - http://www.securite.org/kaneda/

version 1.05BH
Agenda

- **Network Security**
  - Layer 2, layer 3 and routing protocols attacks
  - DDoS/worm attacks detection, protection and filtering
  - Network traffic analysis

- **Router Security**
  - SNMP and remote administration
  - AAA and ACLs
  - Integrity checking

- **MPLS/IPv6**

Disclaimer: we don’t work for Cisco and we don’t have Cisco stock :-}
Layer 2 protocols

- Layer 2 protocols and traffic
  > ARP - Address Resolution Protocol
  > CDP - Cisco Discovery Protocol
  > VLAN - Virtual LAN
  > STP - Spanning Tree
  > {D/V}TP - Dynamic, VLAN Trunking Protocol
  > Unicast, Broadcast and Multicast addressing and traffic
Protocol attacks

- **Well known (not to say old) attacks**
  - ARP cache poisoning and ARP/DHCP spoofing
  - Tools: dsniff suite, hunt, etc.

- **New (not so old) attacks**
  - HSRP/VRRP spoofing
  - STP/VTP attacks
  - VLAN jumping

- **Future (to come) attacks?**
  - Advanced routing protocols attacks
  - Rootkits and Loadable Kernel Modules
MAC address and STP filtering

- Filter MAC addresses (and add static IP-to-MAC)
  
  ```
  set port security <mod/port> enable 01-02-03-04-05-06 shutdown
  ```

- Activate BPDU-guard (Bridge PDU) to filter STP
  
  ```
  ! MLS (Multi Layer Switch) in hybrid mode (Sup w/ CatOS, MSFC w/ IOS)
  set spantree disable
  set spantree portfast bpdu-guard-enable

  ! MLS in native mode (CatIOS on the Sup and MSFC)
  spanning-tree portfast bpdu-guard
  ```

- Limit broadcast traffic
  
  ```
  set port broadcast <mod/port> 0.01%
  ```
VLANs: Layer 2 partitioning (1)

- **The problem with VLANs**
  > VLANs have never been designed for security but are used to enforce it
  > (Multi-layer) switches become single point of security failure
  > Do not use the Native VLAN 1

- **Do not use VMPS**
  > VLAN Management Policy Server allows dynamic VLAN membership based on the MAC address
VLANs: Layer 2 partitioning (2)

- **VLAN jumping**
  > Is possible: if you use DTP, if a port is in the same VLAN as the trunk’s port Native VLAN (inject 802.1q frames)

  ```
  set vlan 2 <mod/port>
  clear trunk <mod/port> 1
  ```

  > VLAN bridges allow bridging between VLANs for non-routed protocols

- **Private VLAN (6k, 4k) and Edge ports (29xx, 35xx)**
  > Port isolation, not based on IP/MAC/VLAN
  > Devices in the same VLAN can’t talk directly to each other
Protocols : VTP

- **VLAN Trunking Protocol**
  > Enables central VLAN configuration (Master/Slaves)
  > Message format : like CDP (SNAP HDLC 0x2003)
  > Works only over trunk ports

- **Security measures**
  > Put your switches in transparent VTP mode and use a password

```bash
set vtp domain <vtp.domain> password <password>
set vtp mode transparent
```
Protocols : DTP

- **Dynamic Trunking Protocol**
  - Enables automatic port/trunk configuration
  - Message format: like CDP (SNAP HDLC 0x2004)
  - All switch ports are in auto mode by default

- **Security measures**
  - Turn DTP off on all the ports
  
```bash
set trunk off all
```
Protocols: CDP (1)

- CDP (Cisco Discovery Protocol)
  - Cisco proprietary
  - Works on any HDLC capable link/device
  - Multicast traffic
  - Information leaked to other peers: device id/name, network address, port id, capabilities, software version, platform and IP network prefix

- Message format

<table>
<thead>
<tr>
<th>SNAP HDLC Protocol Type: 0x2000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination: 01-00-0C-CC-CC-CC-CC</td>
</tr>
<tr>
<td>Version (1 or 2)</td>
</tr>
<tr>
<td>List of TLVs (Type-Length-Value)</td>
</tr>
</tbody>
</table>
Protocols : CDP (2)

- **Open to DoS attacks**
  - Discovered by FX (see the Cisco Security Notice)

- **Security measures (router)**
  - Global deactivation
  - Per interface deactivation
    - `no cdp run`
    - `interface xy
      no cdp enable`

- **Security measures (switch)**
  - Global/per interface deactivation
    - `set cdp disable <mod/port>`
Layer 3 protocols

- **The network layer**
  - IP: no built-in security
  - ICMP: information leakage and side effects
  - HSRP / VRRP: provide next-hop redundancy
  - RIP / RIPv2: no authentication (v1) and flooding
  - OSPF: multicast (adjacencies and DR/BDR at risk)
  - BGP: core of the Internet (RR/peerings at risk)

- **Not well known or not so used in enterprise networks**
  - IS-IS
  - (E)IGRP
Protocols: BGP (1)

- **BGP (Border Gateway Protocol)**
  > Version 4
  > Runs on port 179/tcp
  > Authentication: MD5 (not often used)
  > Point-to-point over directly connected interfaces or multi-hop between non adjacent routers
  > BGP route injection tools exist (in private circles)

- **BGP (UPDATE) message format**
  
<table>
<thead>
<tr>
<th>Marker: Auth Value</th>
<th>Length</th>
<th>Type: Update</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unfeasible Routes Length</td>
<td>Withdrawn Routes</td>
<td>Total Path Attributes Length</td>
<td>Path Attributes: Origin AS_path Next_hop</td>
</tr>
<tr>
<td>Network Layer Reachability Information IP Prefixes</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Protocols : BGP (2)

- Where are the risks?
  - Internet Exchanges: all providers are usually connected to the same shared infrastructure (a switch for example): do prefix/AS_path filtering
  - Your direct {up,down}stream: IP filter on interfaces
  - Multi-hop configurations (Man-in-the-middle attack)

- What to monitor
  - AS_path you receive from upstreams
  - AS_path that other ISPs are getting that contains your ASN (route servers)
  - Are the paths changing (especially the best path)?
  - ARP changes (IX public switches)
Protocols: BGP (3)

- Additional security measures
  > Do not use the same password with all the peers
  > Log changes and use IPSec

```
router bgp 65000
  bgp log-neighbor-changes
  network x.x.x.x
  neighbor y.y.y.y remote-as 65001
  neighbor y.y.y.y password <MD5password>
  neighbor y.y.y.y version 4
  neighbor y.y.y.y prefix-list theirnetworks in
  neighbor y.y.y.y prefix-list ournetworks out
  neighbor y.y.y.y maximum-prefix 120000
  neighbor y.y.y.y route-map ourASpath out

  ip prefix-list ournetworks seq 5 permit z.z.z.z/17
  ip prefix-list ournetworks seq 10 deny 0.0.0.0/0 le 32
  ip prefix-list theirnetworks seq 5 permit k.k.k.k/19
  ip as-path access-list permit ^<AS>( <AS>)*$

  route-map ourASpath permit 10
  match as-path 99
```
Protocols : BGP (4)

- BGP route injection tool : what is the challenge ?
  > Find the eBGP peer
    - MITM
    - SNMP
    - route-servers and looking glasses
    - directly adjacent IPs, .1, .254, etc
  > Inject the update
    - MITM (or ARP spoofing on IX switches)
    - synchronize with/hijack the TCP session

- Future ?
  > S-BGP
Sequence number prediction

- ISN problems on Cisco routers

- "Fixed" as of 12.0(15) and 12.1(7)
- ISNs are (still) time dependant

Source: http://razor.bindview.com/publish/papers/tcpseq.html
Protocols: OSPF (1)

- OSPF (Open Shortest Path First)
  > Protocol type 89
  > Multicast IP: “easy” to inject LSAs

- Security measures
  > Authenticate OSPF exchanges

```plaintext
interface xy
!ip ospf authentication-key <key>
ip ospf message-digest-key 1 md5 <key>
router ospf 1
area 0 authentication [message-digest]
```

> Turn your network into a NBMA network

```plaintext
interface xy
ip ospf network non-broadcast
router ospf 1
neighbor x.x.x.x
```
Protocols: OSPF (2)

- **Security measures**
  - Don’t put the interfaces that shouldn’t send or receive OSPF LSAs in your network statement or then exclude them with a passive-interface statement.
  - Log changes
    ```
    router ospf 1
    log-adjacency-changes
    network x.x.x.x
    passive-interface default
    no passive-interface xy
    ```
  - You can’t filter what is injected into the local area (the network statement meaning is misleading) only to other ASes.
  - You can filter what you receive
    ```
    router ospf 1
    distribute-list <ACL> in
    distribute-list <ACL> out
    ```
Protocols : HSRP/ VRRP (1)

- HSRP (Hot Standby Routing Protocol)
  > Provides next-hop redundancy (RFC2281)
  > Information disclosure : virtual MAC address
    > 00-00-0c-07-ac-<group>
  > HSRP virtual interface doesn’t send ICMP redirects
  > You can have more than 2 routers in a standby group, no need to kill a router, becoming the master is enough

- VRRP (Virtual Router Redundancy Protocol - RFC2338)
  > Supports MD5 for authentication (IP Authentication Header)
Security measures

- Use password authentication

```
interface xy
standby 10 priority 200 preempt
standby 10 authentication p4ssw0rd
standby 10 ip x.x.x.x
```

- Change the virtual MAC address

```
interface xy
standby 10 mac-address <mac-address>
```

- Use IPSec (Cisco recommendation) but is not trivial (multicast traffic, order of processing, limited to a group of 2 routers)
DDoS detection (1)

- **The “old way”**
  > ACLs logs, CPU and line load, *IDS

- **Netflow**
  > Accounting data (AS, IP flows, protocols, etc)
  > Send in clear text over the network (UDP) to a gatherer
  > With CEF activated Netflow will only do accounting
  > Without CEF the router will do netflow switching
    > Only counts outgoing traffic on the interface
  > How to export the data
    
    ```
    ip flow-export version 5 origin-as
    ip flow-export destination x.x.x.x
    interface xy
    ip route-cache flow
    ```

> How to view the data : `sh ip cache flow`
DDoS detection (2)

- **(Un)usual traffic distribution per protocol**
  - TCP : ~90 % (HTTP, FTP and P2P tools)
  - UDP : ~10 % (DNS, SNMP, streaming)
  - ICMP : <1 %
  - IGMP : <1 %

- Mostly 64 bytes packets
- RRDtool and Netflow can be used to graph trends, detect changes and anomalies

Source: Flowscan from UW-Madison (http://wwwstats.net.wisc.edu/)
DDoS detection (3)

- **Netflow data on Multi-Layer Switches**
  - Netflow-based MLS flow-mode is “destination-only” (no source address is cached)
  - Enable “full-flow” mode (performance impact on SE1)

```plaintext
! MLS in hybrid mode
set mls flow full

! MLS in native mode
mls flow ip full
```

- Display the entries

```plaintext
! MLS in hybrid mode
set mls ent

! MLS in native mode
show mls ip
```

- **Poor man’s netflow : ntop ?**
DDoS prevention (1)

- **Unicast RPF (Reverse-Path Forwarding)**
  - Needs CEF (Cisco Express Forwarding) or dCEF
  - Requires IOS 12.x and uses ~30MB of memory
  - Strict: IP packets are checked to ensure that the route back to the source uses the same interface
  - Only the best path (if no multi-path or equal cost paths) is in the FIB
    - Asymmetric routes are supported (really :)
    - Check the BGP weight if you use strict mode in a multi-homed configuration
DDoS prevention (2)

- **Unicast RPF (Reverse-Path Forwarding)**
  - Strict (you can use an ACL for exceptions or for logs)
    ```
    ip cef [distributed]
    interface xy
    ip verify unicast reverse-path [allow-self-ping] [acl]
    ```
  - “Loose check” (allowed if the prefix exists in the FIB)
    ```
    ip verify unicast source reachable-via any
    ```
DDoS prevention (3)

- ICMP, UDP, TCP SYN rate-limiting

```plaintext
interface xy
  rate-limit input access-group 100 8000 8000 8000 \ 
  conform-action transmit exceed-action drop
  rate-limit output access-group 100 8000 8000 8000 \ 
  conform-action transmit exceed-action drop
<...>
access-list 100 deny tcp any host x.x.x.x established
access-list 100 permit tcp any host x.x.x.x
access-list 101 permit icmp any any echo
access-list 101 permit icmp any any echo-reply
```

> UDP rate-limiting can be a problem if your customer is a streaming company
DDoS prevention (4)

- TCP Intercept
  - Can do as much good as bad
  - If enabled: process switching and not “full” CEF anymore
  - The “destination” host must send a RST (no silent drops) or you’ll DoS yourself
  - Same is true if you use “blackholed” routes (route to Null0)

```
ip tcp intercept list 100
ip tcp intercept connection-timeout 60
ip tcp intercept watch-timeout 10
ip tcp intercept one-minute low 1500
ip tcp intercept one-minute high 6000

access-list 100 permit tcp any x.x.x.0 0.0.0.255
```
DDoS prevention (5)

- **Advanced ICMP filtering**
  > Only let the “mission critical” ICMP messages in

```
interface xy
  ip access-group 100 in
access-list 100 deny icmp any any fragments
access-list 100 permit icmp any any echo
access-list 100 permit icmp any any echo-reply
access-list 100 permit icmp any any packet-too-big
access-list 100 permit icmp any any source-quench
access-list 100 permit icmp any any time-exceeded
access-list 100 deny icmp any any
access-list 100 permit ip any any
```

> ICMP filtering is a source of dispute (unreachables, parameter-problem, etc). YMMV.
**DDoS prevention (6a)**

- **Advanced technique 1 (1/2) : BGP/ Null0**
  > Pick an IP address from TEST-NET and add a static route to Null0 for it (on all your routers)
  > Have a “master” BGP router set the next-hop for the source network you want to “drop” to the selected IP
  > Have BGP redistribute it to the routers in your AS only and uRPF will drop it (at the LC level, not on the RP)

```plaintext
router bgp <AS>
  network <sourceOfDDOS> mask <netmask> route-map ddos-nh
  route-map ddos-nh
  set ip next-hop <TEST-NETIPaddr>
  ip route <TEST-NET> 255.255.255.0 Null0

> Do not redistribute it to your peers : use a private AS or a “no-export” community
```
DDoS prevention (6b)

- Advanced technique 1 (2/2) : BGP/ Null0

- Master BGP router (set the next-hop for the DDoS sources to 192.0.2.10)

- Propagate the new next-hop

- Core/Access Routers (route 192.0.2.10 to Null0)

- Internet or Customers

- Route reflectors

- iBGP sessions
DDoS prevention (7)

- Advanced technique 2 (1/2) : BGP/ CAR/ FIB
  > Set a special community for the network you want to rate-limit on your “master” BGP router and send this community to your iBGP peers

```
router bgp <AS>
  network <destOfDDOS> mask <netmask>
  neighbor x.x.x.x route-map ddos-rl out
  neighbor x.x.x.x send community
  access-list 10 permit <destOfDDOS>
  route-map ddos-rl
  match ip address 10
  set community <AS>:66 no-export
  ip route <destOfDDOS> 255.255.255.0 Null0
```
DDoS prevention (8)

- Advanced technique 2 (2/2) : BGP/ CAR/ FIB
  > On the routers change the QoSID entry in the FIB based on this special community
  > Use the QoSID entry of the FIB to rate-limit

```
router bgp <AS>
  table-map ddos-rl
  ip community list 1 permit <AS>:66
  route-map ddos-rl
  match community 1
  set ip qos-group 66
  interface xy
  bgp-policy source ip-qos-map
  rate-limit input qos-group 66 ...
```
Ingress/ egress filtering (1)

- **What you should never route/ see/ allow through**
  - RFC 1918 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)
  - 0.0.0.0/x, 127.0.0.0/8
  - 169.254.0.0/16 (auto-configuration when no DHCP)
  - 192.0.2.0/24 (Netname: TEST-NET, like example.com)
  - Multicast blocks (D Class) and Martian networks (E+)
    - “Hijacked” space by some vendors
      (192.0.0.192 for some printers)
    - (ARIN) Reserved blocks (bogon networks)
    - Packets to broadcast addresses or where source == destination

- **What you should route/ let through**
  - Your network prefixes (anti-spoofing)
Ingress/egress filtering (2)

- Example with ACLs
  > Filter on network border: CPE/IX/uplinks

```plaintext
interface xy
  access-group in 100
  access-group out 100
  access-list 100 deny ip host 0.0.0.0 any
  access-list 100 deny ip 127.0.0.0 0.255.255.255 255.0.0.0 0.255.255.255
  access-list 100 deny ip 10.0.0.0 0.255.255.255 255.0.0.0 0.255.255.255
  access-list 100 deny ip 172.16.0.0 0.15.255.255 255.240.0.0 0.15.255.255
  access-list 100 deny ip 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255
  access-list 100 deny ip 192.0.2.0 0.0.0.255 255.255.255.0 0.0.0.255
  access-list 100 deny ip 169.254.0.0 0.0.255.255 255.255.0.0 0.0.255.255
  access-list 100 deny ip 240.0.0.0 15.255.255.255 any
  access-list 100 permit ip any any
  ! Or permit ip <your network prefixes only>
```

- Example with route to Null0

```plaintext
ip route 10.0.0.0 255.0.0.0 null0
ip route 172.16.0.0 255.240.0.0 null0
ip route 192.168.0.0 255.255.0.0 null0
```
Worm detection and protection (1)

- **How to detect a new worm**
  > New/unusual number of HTTP/SMTP flows and server logs

- **How to protect with NBAR (Network-Based Application Recognition)**
  > Needs CEF
  > Available as of 12.1(5)T
  > Like TCP Intercept - do we need it?
  > Side-effect: the TCP handshake is already done but the server never receives the HTTP GET request
  > Performance impact: ~20% CPU
Worm detection and protection (2)

- Inbound classification with NBAR and outbound filtering with ACLs

```plaintext
! Class-based inbound marking
class-map match-any http-hacks
  match protocol http url "*cmd.exe*"
! Policy map to mark inbound
policy-map mark-inbound-http-hacks
class http-hacks
  set ip dscp 1
! Apply the service policy to the « attacking » interface
int xy
  service-policy input mark-inbound-http-hacks
! Block with an ACL
access-list 100 deny ip any any dscp 1 log
access-list 100 permit ip any any
! Apply the ACL to the « protected » interface
int xy
  ip access-group 100 out
```
Worm detection and protection (3)

- Inbound classification with NBAR and class-based policing

```plaintext
! Class-based inbound marking
class-map match-any http-hacks
  match protocol http url "*cmd.exe*"
! Policy map to mark inbound
policy-map drop-inbound-http-hacks
class http-hacks
  policy 8000 4000 2000 conform-action drop exceed-action drop violate-action drop
! Apply the service policy to the « attacking » interface
int xy
  service-policy input police-inbound-http-hacks
```
Inbound classification with NBAR and policy based routing

```
! Class-based inbound marking
class-map match-any http-hacks
    match protocol http url "*cmd.exe*"
! Policy map to mark inbound
policy-map mark-inbound-http-hacks
class http-hacks
    set ip dscp 1
! Apply the service policy to the « attacking » interface
int xy
    service-policy input mark-inbound-http-hacks
! Create a route-map
access-list 100 permit ip any any dscp 1
route-map route2null 10
    match ip address 100
    set interface Null0
! Apply the routing policy to the « attacking » interface
int xy
    ip policy route-map route2null
```
Worm detection and protection (5)

- **NBAR Restrictions and limitations**
  - Supports up to 24 concurrent URLs, hosts or MIME types matches
  - Can’t match beyond the first 400 bytes in a URL
  - Can’t deal with fragmented packets
  - HTTPS traffic (that’s normal ;-)
    - Packets originating from/sent to the router (you can’t protect the local HTTP server)
  - Doesn’t support Unicode (UTF-8/%u)

- **Tune the scheduler and the timeout**
  
  ```
  ip nbar resources 600 1000 50
  scheduler allocate 30000 2000
  ```
DDoS/ worm research/ future

- **Worse to come**
  - A lot of research has been done but nothing has been published/disclosed: “risks are too high”
  - Most of the worms we’ve seen were quite gentle
  - Will the next worm affect IIS/Outlook users again?
  - What are the effects on the Internet stability?

- **What are the trends?**
  - Routers are used as source (CERT)
  - Getting more complex and agents are becoming more intelligent
  - Temporary “use” of non allocated blocks (Dug Song - Arbor Networks)
{tcpdump,snoop}ing on routers

- What can be done with local output
  - Debug with ACLs
    - access-list 100 ...
    - debug ip packet detail 100
  - Always use the buffer and don’t debug to the console
    - logging buffered 64000 debugging
  - Performance impact: check the router’s load with `sh proc cpu`

- How to send to a remote device
  - Use a GRE tunnel to a remote host and inject the traffic back from there (tunnelx)
{tcpdump,snoop}ing on switches

- No local output
- How to send to a remote device
  > Mirror ports or a VLAN to another port
    - ! MLS in hybrid mode
    - set span <source (mod/port or VLAN)> <destination port>
    - ! MLS in native mode
    - monitor session <session id> ...
  > Can copy only designated traffic to be inspected (VAACL w/ “capture” keyword):
    - set security acl capture-ports <mod/port>
  > RSPAN dumps the traffic to a VLAN (needs end-to-end Cat6K)
  > 1 or 2 SPAN port(s) depending on the switch
  > Performance impact close to zero: check the CPU load with ps -c (hidden command)
Configuration basics (1)

- Turn off all the unneeded services
  - no ip bootp server
  - no tcp-small-servers
  - no udp-small-servers
  - no ip identd
  - no ip finger
  - service nagle
  - no cdp run
  - no boot network
  - no service config
  - no ip subnet-zero
  - no service finger
  - no service pad
  - no ip http server
  - no ip source-route

- Use syslog
  - service time log datetime localtime show-timezone msec
  - service time debug datetime localtime show-timezone msec
  - logging x.x.x.x
  - logging trap debugging
  - logging source loopback0
  - logging buffered 64000 debugging

- Use (authenticated) NTP
  - ntp authentication-key 10 md5 <key>
  - ntp authenticate
  - ntp trusted-key 10
  - ntp server x.x.x.x [key 10]
  - ntp access-group peer 20
  - access-list 20 permit host x.x.x.x
  - access-list 20 deny any
Configuration basics (2)

- **At the interface level**
  ```
  interface xy
  no ip source-route
  no ip directed-broadcast
  no ip proxy-arp
  no ip redirects
  no ip unreachables
  ! IP accounting for the traffic that fails the IP ACLs
  ip accounting access-violations
  no ip mask-reply
  no cdp enable
  ```

- **If multicast is used**
  ```
  interface xy
  ! To prevent Auto-RP messages from entering the PIM domain
  ip multicast boundary 10
  access-list 10 deny 224.0.1.39
  access-list 10 deny 224.0.1.40
  ```

- **Use loopbacks whenever possible**
  ```
  interface loopback0
  ip address x.x.x.x 255.255.255.255
  ```
Admin : SNMP (1)

- Simple Network Management Protocol
  - v1 : RFC1157 uses community strings for authentication
  - v2 : RFC1441/1446 adds security (party) and get-bulk
  - v3 : RFC2274 adds integrity checking, encryption and user authentication

- Known attacks/ problems
  - Netadmins use RW communities for management
    - Weak communities
    - Replay and DoS attacks
    - Information leak
    - Auto-discovery feature of management tools that “send” your community out of your network range (to external parties)
Admin : SNMP (2)

- **IP level filtering**
  > Define an ACL and activate it on a per interface basis

  ```
  interface Ethernet0/0
  access-group in 100
  access-list 100 permit udp host 192.168.1.1 host 192.168.1.2 eq snmp
  access-list 100 permit udp host 192.168.1.2 eq snmp host 192.168.1.1
  access-list 100 deny udp any any eq snmp log-input
  ```

- **Application level filtering**
  > Define an ACL and use it for application access control

  > Use views to restrict the exposure

  ```
  snmp-server community r3ad view cutdown RO 10
  snmp-server community wr1te RW 10
  snmp-server view cutdown ip.21 excluded
  snmp-server enable traps <...
  snmp-server host x.x.x.x
  snmp-server source loopback0
  access-list 10 permit x.x.x.x
  ```
Admin : SNMP (3)

- **SNMP v3**
  > Define a user/group and what the group can do

```
snmp-server group engineering v3 priv read cutdown 10
snmp-server user nico engineering v3 auth md5 myp4ss priv des56 mydes56
snmp-server view cutdown ip.21 excluded
access-list 10 permit x.x.x.x
access-list 10 deny any log
```

- **Two security advisories**
  > The “hidden” ILMI community (show snmp community shows all communities)
  > Read-write community available with a read only access
Admin : Secure Shell (1)

- **SSHv1 (client and server) support**
  > Routers : as of 12.1(1)T/12.0(10)S (go for an image with 3DES), scp as of 12.2T
  > Switches : CatOS 6.x

- **What are the risks/ limitations ?**
  > Cisco’s implementation is based on SSH v1 and suffered from the same bugs : key recovery, CRC32, traffic analysis (SSHow), timing analysis and attacks
  > You can’t force 3DES only nor use keys
  > Fixed in 12.0(20)S, 12.1(8a)E, 12.2(3), ...
Admin : Secure Shell (2)

- **SSH configuration**
  
  hostname `<hostname>`
  ip domain-name `<domainname>`
  crypto key generate rsa
  ip ssh timeout 60
  ip ssh authentication-retries 3

- **scp configuration**

  ip scp server enable
Admin : IPSec (1)

- **IPSec configuration**
  - Deny all traffic except IPSec related/decrypted

```plaintext
interface xy
  ip address y.y.y.y 255.255.255.0
  ip access-group 100 in
  access-list 100 permit udp host x.x.x.x host y.y.y.y eq 500
  access-list 100 permit esp host x.x.x.x host y.y.y.y
  access-list 100 permit ahp host x.x.x.x host y.y.y.y
  access-list 100 permit ip <remoteLAN> <localLAN>
```

- Define a SA (Security Association) : traffic to encrypt

```plaintext
access-list 110 permit ip x.x.x.x <wildcard> y.y.y.y <wildcard>
```

- Define an IKE policy

```plaintext
crypto isakmp policy 1
  hash md5
  encryption 3des
  authentication pre-share
  ! DH group (1024 bits)
  group 2
  crypto isakmp key <key> address y.y.y.y
```
Admin : IPsec (2)

- **IPSec configuration**
  > Define the transform-sets (tunnel mode is better, use transport with Win2K -- easier)

```
crypto ipsec transform-set 3desmd5 esp-3des esp-md5-hmac
```

> Put all together in a crypto-map

```
crypto map mycryptomap 10 ipsec-isakmp
set peer y.y.y.y
set transform-set 3desmd5
match address 110
```

> And affect it to an interface

```
interface xy
crypto-map mycryptomap
```
Admin : local users/ passwords (1)

- **Local users**
  > Encryption type 7 is reversible, MD5 as of 12.1(8a)E

- **Enable secret**
  > Use MD5 (type 5)

  
  ```
  service password-encryption
  enable secret 5
  ```

- **Access method**
  > Remove telnet and enable SSH

  ```
  service tcp-keepalives-in
  line vty 0 4
  exec-timeout 0 60
  access-class 10 in
  transport input ssh
  transport output none \ transport preferred none
  access-list 10 permit x.x.x.x
  ```

  > Don’t forget the console and AUX port
Admin : local users/ passwords (2)

- Switches

set password <password>
set enablepass <password>

! For access via sc0
set ip permit enable
set ip permit x.x.x.x y.y.y.y telnet
set ip permit x.x.x.x y.y.y.y ssh
set ip permit z.z.z.z y.y.y.y snmp
AAA: Authentication / Accounting

- Authentication/accounting: RADIUS/TACACS+
  - aaa new-model
  - aaa authentication login default tacacs+ enable
  - aaa authentication enable default tacacs+ enable
  - aaa accounting exec default start-stop group tacacs+
  - ip tacacs source-interface loopback0
  - tacacs-server host x.x.x.x
  - tacacs-server key K3y

- Command accounting (TACACS+ only)
  - aaa accounting commands 15 default start-stop group tacacs+
AAA: Authorization

- Privilege levels
  > 1 : user EXEC “view only”
  > 15 : privileged EXEC “enable”
  > Change the privilege level (reduces information disclosure and avoids a stepping stone)
  > A user can only see parts of the configuration he is allowed to change or gets a view-and-disconnect

```
privilege exec level 15 connect
privilege exec level 15 telnet
privilege exec level 15 ssh
privilege exec level 15 rlogin
privilege exec level 15 show logging
privilege exec level 15 show [ip] access-lists
username seeandgo privilege autocommand show running
```

- Command authorization
  > Only supported with TACACS+
AAA: Kerberos (1)

- **Cisco Routers**
  - Kerberized Telnet and password authentication using Kerberos (telnet, SSH and console)
  - Can map instance to Cisco privilege (locally defined)
  - Feature name: Kerberos V client support (Enterprise)
  - Not supported on all hardware (16xx, GSR, etc)

- **Cisco Switches**
  - Telnet only (SSH available as of 6.1 but w/o Kerberos support)
  - At least SE Software Release 5.x
  - Only supported on Catalyst 4K, 5K and 6K/6500 (with SE I, not SE II)
AAA: Kerberos (2)

- Kerberos on a router

  ```
  aaa authentication login default krb5-telnet local
  aaa authorization exec default krb5-instance
  kerberos local-realm COLT.CH
  kerberos srvtab entry host/... 
  kerberos server COLT.CH 192.168.0.14
  kerberos instance map engineering 15
  kerberos instance map support 3
  kerberos credentials forward
  line vty 0 4
  ntp server 192.168.0.126
  ```

- Kerberos on a switch

  ```
  set kerberos local-realm COLT.CH
  set kerberos clients mandatory
  set kerberos credentials forward
  set kerberos server COLT.CH 192.168.0.82 88
  set kerberos srvtab entry host/...
  set authentication login kerberos enable telnet primary
  set authentication enable kerberos enable telnet primary
  set ntp client enable
  set ntp server 192.168.0.11
  ```
ACLs (1)

- **IP filtering with ACLs**
  - Is not stateful and doesn’t do any reassembly
  - log-input also logs the source interface and the source MAC address
  - Only the first fragment is filtered (unless you use the fragment keyword)

- **Well known ACL types**
  - Standard: source IP address only (1-99, 1300-1999)
  - Extended: limited to IP addresses, protocols, ports, ACK/RST (established) bit is set, etc. (100-199, 2000-2699, “named” ACLs)
ACLs (2)

- Other “kinds” of ACLs
  - TurboACL: uses a hash table, benefits when 5+ ACEs
  - Reflexive: enables on-demand dynamic and temporary reply filters (doesn’t work for H.323 like protocols)
  - Dynamic: adds user authentication to Extended ACLs
  - Named: allows you to delete individual ACEs
  - Time-based: adds a time-range option
    - Context-Based Access-Control: “inspects” the protocol (helper/proxy/fixup-like), used in conjunction with ACLs
  - MAC: filters on MAC address (700-799 for standard, 1100-1199 for extended)
  - Protocol: filters on protocol type (200-299)
ACLs (3)

- Example: Extended ACL on a router

```plaintext
no access-list 100
access-list 100 permit <...>
access-list 100 deny tcp any range 1 65535 any range 0 65535 log
access-list 100 deny udp any range 1 65535 any range 0 65535 log
access-list 100 deny ip any any log-input
```

- ACLs on a Multi-Layer Switch
  > ACLs defined on Layer 3 (S/E/R/D) are pushed to the NMP (TCAM)
  > Traffic will not hit the MSCF if you don’t use log[-input], ip unreachables, TCP Intercept
  > VACLs (VLAN): Can filter IP level traffic and are pushed from the PFC to the switch
Switches

- **High-end switches (6509)**
  - Native (IOS only)
  - Hybrid (IOS and CatOS)
  - Wire-speed with IP ACLs

- **CatOS 6.2 integrates IOS Firewall feature set**
  - Authentication proxies, CBAC, TCP Intercept, RACLs
  - No IDS and no encryption support
  - Roadmap: MAC-layer VACLs (for IP traffic)

- **CatOS 12.1.x supports**
  - IP Unicast-RPF, TCP Intercept, etc
Router integrity checking (1)

- Four steps to build a tripwire-like for IOS/ CatOS
  > 1. Store your routers and switches configurations in a central (trusted) repository (CVS for example)
  > 2. Get the configuration from the device (scripted telnet in Perl or expect, rsh, tftp, scp) or have the device send you the configuration (needs a RW SNMP access)
  > 3. Check : automatically (cron/at job), when you see “configured by <xyz>” or a router boot in the logfile or when you get the “configuration changed” SNMP trap

  ```snmpset -c <community> <routerIP> v1.3.6.1.4.1.9.2.1.55.<tftpserverIP> s <filename>```
Router integrity checking (2)

- **Four steps to build a tripwire-like for IOS/ CatOS**
  > 4. Diff the configuration with your own script or use CVS

- **Limitations and details**
  > You still have to trust the running IOS/CatOS (no Cisco “rootkit” yet) and your network (MITM attacks)
    > The configuration is transmitted in clear text over the network (unless you use scp or IPSec to encrypt the traffic)
    > Do not forget that there are two “files”: startup-config and running-config
    > Do the same for the IOS/CatOS images
    > Cisco MIBs : CISCO-CONFIG*
Router integrity checking (3)

- Cisco IOS rootkit/ BoF/ FS : is it possible ?
  > Proprietary, closed source OS running on MIPS (newer models) or Mot68K (older models)
  > ELF 32-bit MSB executable, statically linked, stripped
  > What is possible with remote gdb access :
    gdb {kernel|pid pid-num} ?
  > Is the ROMMON a good starting point (local gdb) ?

"Inside Cisco IOS software architecture" - Cisco Press :
- “In general, the IOS design emphasizes speed at the expense of extra fault protection”
- “To minimize overhead, IOS does not employ virtual memory protection between processes”
- “Everything, including the kernel, runs in user mode on the CPU and has full access to system resources”
Router integrity checking (4)

- Cisco IOS rootkit/ BoF/ FS : open questions/ issues
  - No (known) local tools/command to interact and “play” with the kernel, memory, processes, etc.
  - What can be done in enable engineer mode?
  - Is it possible to upload a modified IOS image and start it without a reboot (like “Linux two kernel monte”)?
    - A lot of different images exist (but providers usually go for ~12.0(x)S) and a tool to patch images would be required
  - What will happen with IOS-NG (support for loadable modules)?
**MPLS (1)**

- **MultiProtocol Label Switching**
  - Virtual Circuits, not encrypted/authenticated VPNs
  - “Equivalent” to a layer 2 VPN (ATM/FR)
  - IPSec can be used to secure the traffic
  - VPN partitioning done at routing layer
  - One routing table per VPN on each PE router (VRF)
  - MPLS label added to the IP packet to identify the VPN
    - Each router (LSR) on the MPLS path (LSP) has a local table (LIB)
    - The label only has a “local” meaning and is/may be changed on each hop
MPLS (2)

- **Attacks**
  > Labeled packets injection:
    - blocked by default on all interfaces (CE/PE)
    - easy if access to the MPLS routers
  > Inject data in the signaling protocols ((MP-)BGP and IGPs) to modify the VPN topology

- **Security measures**
  > Good configuration of all routers
  > Difficult to gather MPLS information from the routers
IPv6

- IPv6
  - Basically no new risks/big changes
  - “Native” IPSec support
  - Higher risks during the transition phase from IPv4 to IPv6?
  - MAC address can be part of the IP address
That’s all folks :-) 

- Latest version of this document < http://www.securite.org/presentations/secip/ >
- Q&A

Thanks to the members of the eXperts Group for the proofreading and feedback, FX for working with us on synchronizing the speeches, the BlackHat staff, and of course, you for attending :-) 

Image: http://www.inforamp.net/~dredge/funkycomputercrowd.html