Cisco Router Security: Principles and Practise

The foundation of network security is router security.

Cisco Router Security: Principles and Practise

1) Router security within a general IT security plan, IOS software and standard access.

2) Password security and authentication.

3) Services, applications and protocol security.

4) NTP, logging and incident response.

Cisco Router Security: Principles and Practise

Risk Analysis.

$$R=v(1..n)*t(1..n)*c(1..n)$$

Where R= total risk cost, t=threat, v=vulnerability, and c=cost.

Cisco Router Security: Principles and Practise

Physical Security.

Think like a jealous Greek god. Or a resistentialist.

Think like a burglar.

No modems on the console port.

Cisco Router Security: Principles and Practise

Legal Security.

MOTD banners; the apocryphal “Welcome” message.

Protect against intruders, liability, warn about monitoring and acceptable use policies. Use implies consent.

Cisco Router Security: Principles and Practise

Secure the IOS.

Every IOS has security problems. Keep yours up-to-date.

Only GD (General Deployment) releases should be deployed

Cisco Router Security: Principles and Practise

Router Access.

Many ways to access a Cisco router, with variations in authorization; the console port, the auxiliary port, or network access through virtual TTYs (VTYs).

It is recommended that one of the five VTY passwords is kept different from the other four.

Cisco Router Security: Principles and Practise

Authentication and VTY/AUX Access.

Ensure that login names are required.

If VTY and AUX ports are not used then they should be disabled.

Cisco Router Security: Principles and Practise

```
Router#config terminal
Enter configuration commands, one per
 line.  End with CNTL/Z.
Router(config)#line aux 0
Router(config-line)#login local
Router(config-line)#no password
Router(config-line)#transport input none
Router(config-line)#no exec
Router(config-line)#exec-timeout 0 1
Router(config-line)#^Z
```

Cisco Router Security: Principles and Practise

Using NAS and TFTP.

Network Access Servers are an easier alternative to local usernames. Use TACACS+, RADIUS or Kerberos.

Configuration files on TFTP servers and routers as TFTP servers is significant risk.

Cisco Router Security: Principles and Practise

Remote Administration.

Basic methods are AUX, VTY and HTTP. Common dangers include sniffing, brute-force attacks, spoofing of source IP address, hijacking sessions, and compromise of trusted hosts. Don't use Telnet. Secure VTY. Use callback security. Disable HTTP access ('`no ip http server`' at global configuration).

Cisco Router Security: Principles and Practise

Passwords and Services.

Use '`password-encryption`' from global configuration for user level. Privileged level passwords should be set with the '`enable secret`' command . Different routers should have different passwords and backup configurations should be kept on secure servers. Services, such as connect, telnet, rlogin, show ip access-lists etc should be reconfigured.

Cisco Router Security: Principles and Practise

ICMP.

Selective ICMP packets should be disabled; on every interface ICMP redirects, broadcasts, mask replies, unreachables, and proxy ARPs. This is achieved through the '`no ip redirects`', '`no ip directed-broadcast`', '`no ip mask-reply`', '`no ip unreachables`' and '`no ip proxy-arp`' commands.

Cisco Router Security: Principles and Practise

Further, ICMP Timestamp and Information Requests should be blocked by an ACL to protect against network mapping by an attacker. e.g.,

```
Router#config terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#access-list 101 deny icmp any any timestamp-
request
Router(config)#access-list 101 deny icmp any any
information-request
Router(config)#access-list 101 permit ip any any
Router(config)#interface serial 0/0
Router(config-if)#ip access-group 101 in
Router(config-if)#^Z
Router#
```

Cisco Router Security: Principles and Practise

Other Services.

The following services should also be disabled (all at global config):

Source routing ('`no service source-route`'), small services ('`no service tcp-small-servers`', '`no service udp-small-servers`') and finger ('`no service finger`' or '`no ip finger`' on newer version of the IOS).

Cisco Router Security: Principles and Practise

CDP and Proxy ARP.

Make your network map. Then disable CDP, either globally ('`no cdp run`') or locally per interface ('`no cdp enable`'). Disable Proxy ARP on each interface ('`no ip proxy-arp`')

Cisco Router Security: Principles and Practise

Optionally.

Disable (all at global config) BootP, DNS, Network autoloading of configuration files, PAD, IP classless.

Cisco Router Security: Principles and Practise

SNMP.

Either disable or secure.

Especially dangerous with R/W Access and TFTP.

Version 3 (2004) is best available.

Cisco Router Security: Principles and Practise

```
Router#config terminal
Enter configuration commands, one
 per line.  End with CNTL/Z.
Router(config)#snmp-server community
 StrongStringReadOnly  RO
Router(config)#^Z
```

Cisco Router Security: Principles and Practise

Spoofing.

Prevented by ingress and egress filters.

Cisco has developed Unicast Reverse Packet Forwarding (uRPF)

Cisco Router Security: Principles and Practise

To enable uRPF, you must first globally enable CEF, and then uRPF on each needed interface:

```
Router#config terminal
Enter configuration commands, one per line.
 End with CNTL/Z.
Router(config)#ip cef
Router(config)#interface Serial 0/1
Router(config-if)#ip verify unicast reverse-
 path
Router(config-if)#^Z
```

Cisco Router Security: Principles and Practise

Routing Authentication.

Available on RIP2, OSPF, EIGRP, and BGP.

Minor differences on each protocol.

Cisco Router Security: Principles and Practise

RIPv2 example:

```
RouterOne#config terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterOne(config)#interface FastEthernet 0/0
RouterOne(config-if)#ip rip authentication key-chain 20
RouterOne(config-if)#ip rip authentication mode md5
RouterOne(config-if)#exit
RouterOne(config)#interface Serial 0/0
RouterOne(config-if)#ip rip authentication key-chain 20
RouterOne(config-if)#ip rip authentication mode md5
RouterOne(config-if)#exit
RouterOne(config)#^Z
```

Cisco Router Security: Principles and Practise

RIPv2 example cont:

```
Next, the key chain 20 is defined. Inside key chain 20,
  key number 1 is created with the string StrongPassword:

RouterOne#config terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterOne(config)#key chain 20
RouterOne(config-keychain)#key 1
RouterOne(config-keychain-ke)#key-string StrongPassword
RouterOne(config-keychain-ke)#^Z
```

Cisco Router Security: Principles and Practise

NTP.

Necessary for auditing purposes etc.

Different configuration options. Redundancy. Use ACLs and NTP authenication.

Cisco Router Security: Principles and Practise

Logging.

Console logging, buffered logging, terminal logging, syslog, SNMP traps, ACL logs.

AAA accounting (exec, system, command, connection, network).

Cisco Router Security: Principles and Practise

To configure your router to send log messages to the server 10.0.0.1 using facility local6 and severity informational:

```
RouterOne#config terminal
Enter configuration commands, one per line.  End
 with CNTL/Z.
RouterOne(config)#logging facility local6
RouterOne(config)#logging trap informational
RouterOne(config)#logging 10.0.0.1
RouterOne(config)#^Z
```

Cisco Router Security: Principles and Practise

Incident Response.

Attack or incident? What happened? Change nothing. Preserve evidence. Document completely. Recover. Prevent repetition.