Network Infrastructure

Router and Switch Protection

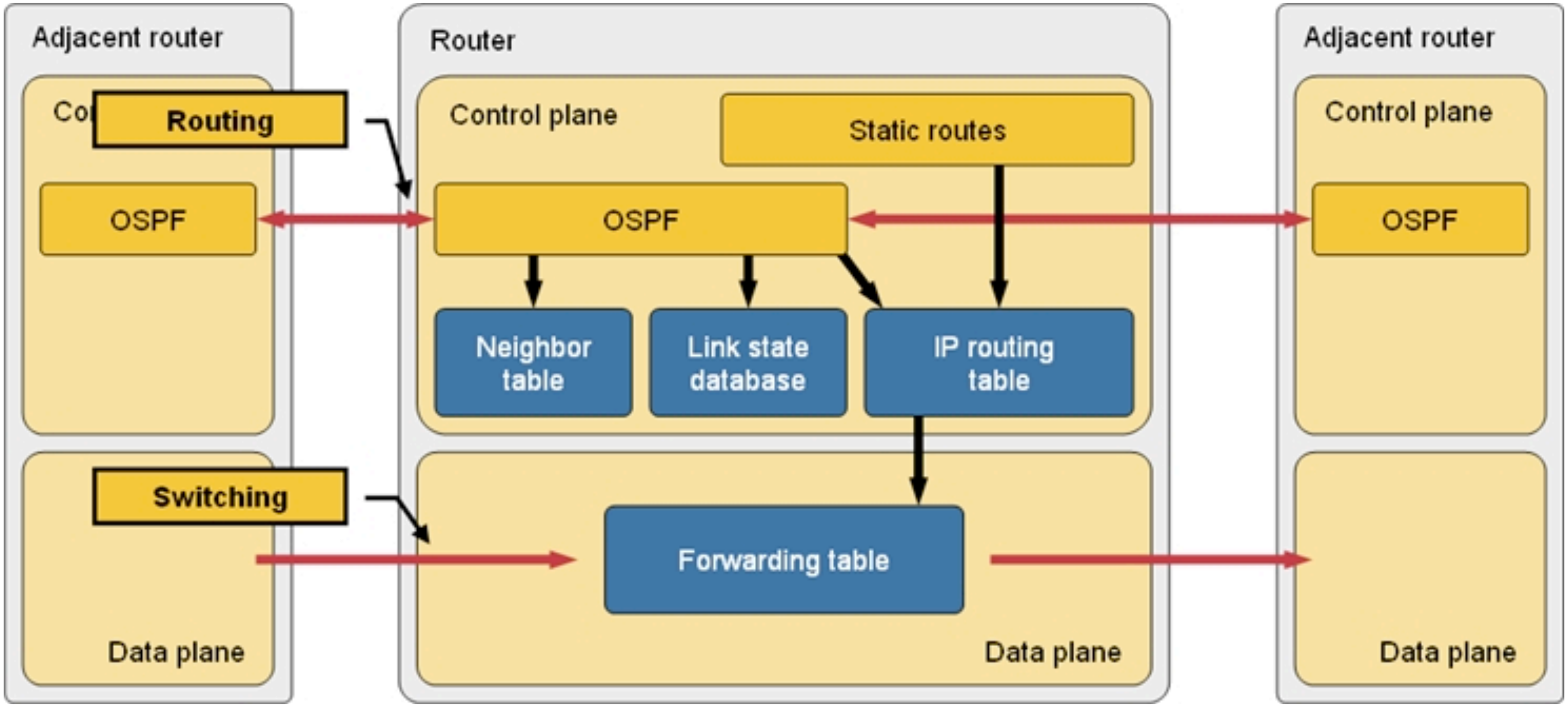
version : 2.0

Fakrul (Pappu) Alam
fakrul@dhakacom.com

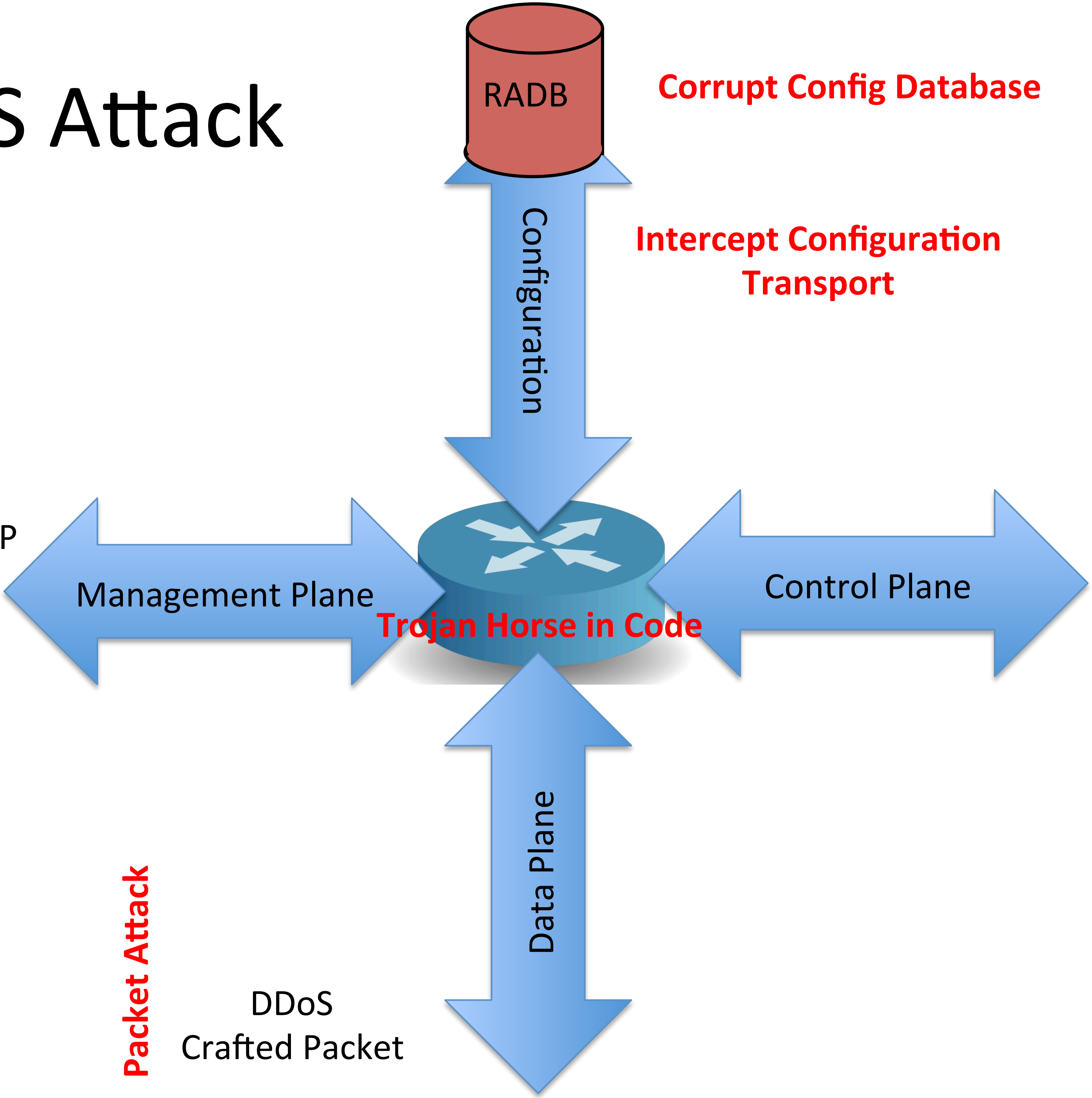
Acknowledgement

- Original slides prepared by Randy Bush

Inside Router



R&S Attack



RADB

Corrupt Config Database

Configuration

Intercept Configuration
Transport

Management Plane Attack

SNMP
SSH
FTP

Management Plane

Trojan Horse in Code

Control Plane

OSPF
IS-IS
BGP
LDP

Routing Protocol Attack

Data Plane

Packet Attack

DDoS
Crafted Packet

Attack Vector

- Could Spy on Protocols, Data, or Configuration
- Could Alter Protocols, Data, or Configuration
- Would Require Vendor Collusion
- Nation State Attack
- Considered Unlikely
- Only Protection is Code Audit

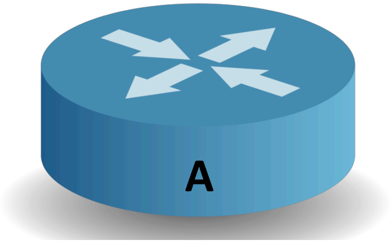
Securing Control Plane (Config)

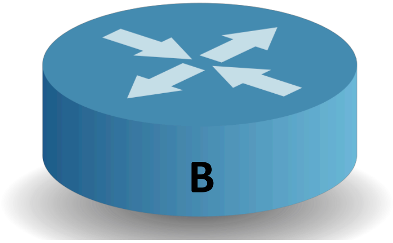
- Tapping Configuration Session
  - Stealing Password
  - Stealing Configuration
- DO NOT USE Telnet
- Configure Over SSH
- Restrict SSH to Special Hosts

Securing Control Plane (OSPF)

```
interface Loopback0
  ip address 70.70.70.70 255.255.255.255
 !
 interface Serial0
  ip address 192.16.64.2 255.255.255.0
  ip ospf message-digest-key 1 md5 c1$c0

!--- The Key value is set as "c1$c0 ".
!
router ospf 10
  passive-interface default
  no passive-interface Serial0
  network 70.0.0.0 0.255.255.255 area 0
  network 192.16.64.0 0.0.0.255 area 0
  area 0 authentication message-digest
```



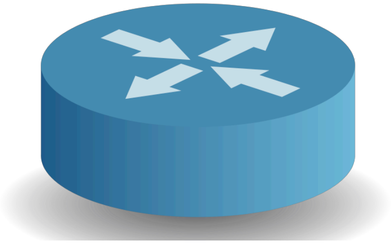


```
interface Loopback0
ip address 172.16.10.36 255.255.255.240
!
interface Serial0
ip address 192.16.64.1 255.255.255.0
ip ospf message-digest-key 1 md5 c1$c0

!--- The Key value is set as "c1$c0 ".
!
router ospf 10
passive-interface default
no passive-interface Serial0
network 172.16.0.0 0.0.255.255 area 0
network 192.16.64.0 0.0.0.255 area 0
area 0 authentication message-digest
```

Securing Control Plane (BGP)

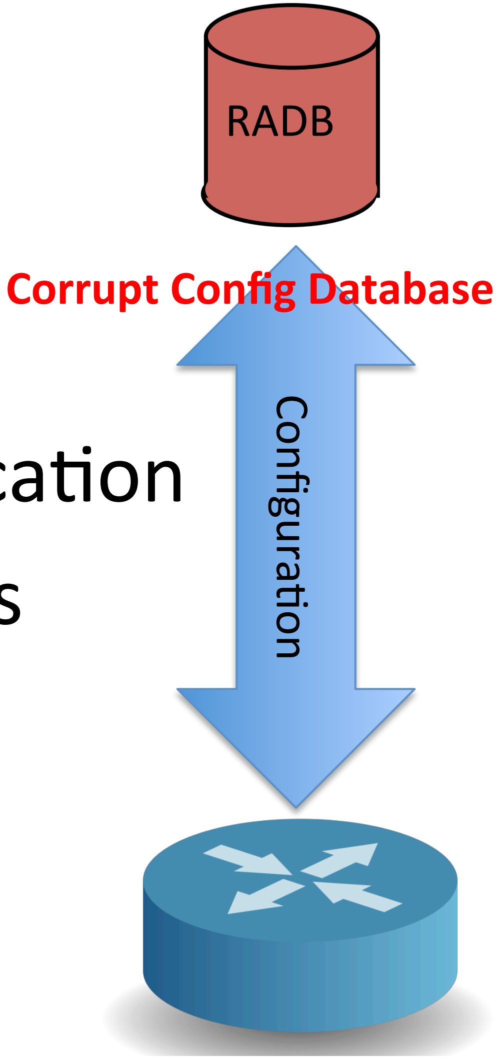
```
router bgp 64496
        neighbor 10.10.10.1 remote-as 64500
        neighbor 10.10.10.1 ttl-security hops 2
        neighbor 10.10.10.1 soft-reconfiguration inbound
        neighbor 10.10.10.1 description eBGP with ISP64500
        neighbor 10.10.10.1 password bgpwith64500
        neighbor 10.10.10.1 version 4
        neighbor 10.10.10.1 prefix-list default-in in
        neighbor 10.10.10.1 prefix-list announce out
!
ip prefix-list announce description Our allowed routing announcements
ip prefix-list announce seq 5 permit 192.0.2.0/24
ip prefix-list announce seq 10 deny 0.0.0.0/0 le 32
!
ip prefix-list default-in description Receive default route only
ip prefix-list default-in seq 5 permit 0.0.0.0/0
ip prefix-list default-in seq 10000 deny 0.0.0.0/0 le 32
```



http://www.team-cymru.org/ReadingRoom/Templates/secure-bgp-template.html

Securing Control Plane (Config)

- Protect Your Provisioning
- Against Intrusion and Employees
- Isolate and Protect Servers
- Secure All Inter-System Communication
- Two-Factor Authenticate all Access


RADB
Corrupt Config Database
Configuration