OPEN SHORTEST PATH FIRST

PWN

How to take advantage of routing protocols

ABOUT ME

Studied network and security at the Technical University of Troyes (France)

Working at WienCERT (Stadt-Wien)

AGENDA

What is a routing protocol?

How to use a vulnerable configuration?

Consequences and how to avoid it.

WHAT IS A ROUTING PROTOCOL

Photo courtesy of Dawson Construction Co. BP Refinery project

ROUTING IN IP NETWORKS

IP Networks & Masks

IP	Network	Mask
10.0.0.9/29	10.0.0.8	255.255.255.248

ROUTING IN IP NETWORKS

IP: `192.168.42.1/24`

Network	Gateway
`10.0.0.0/8`	R1
`10.0.0.0/24`	R2
`0.0.0.0`	R3

To reach 10.0.**0.1** ⇒ GW **R2**

To reach 10.0.**1.1** ⇒ GW **R1**

To reach 192.168.1.1 ⇒ GW **R3**

HISTORICAL ROUTING

All routers controlled by the same administrative authority

Security wasn't really a preoccupation

Internet grew to fast to implement security changes

WHAT IS A ROUTING PROTOCOL?

Share routes through the network in an automated way

IGP vs. EGP

link-state vs. distance-vector

OSPF: A ROUTING PROTOCOL

Interior Gateway Protocol

Multicast (224.0.0.5 or FF02::5)

Link-State Protocol ⇒ Keep state with

UPDATE packets

Encapsulated directly in IP (protocol 89)

Network Bravo

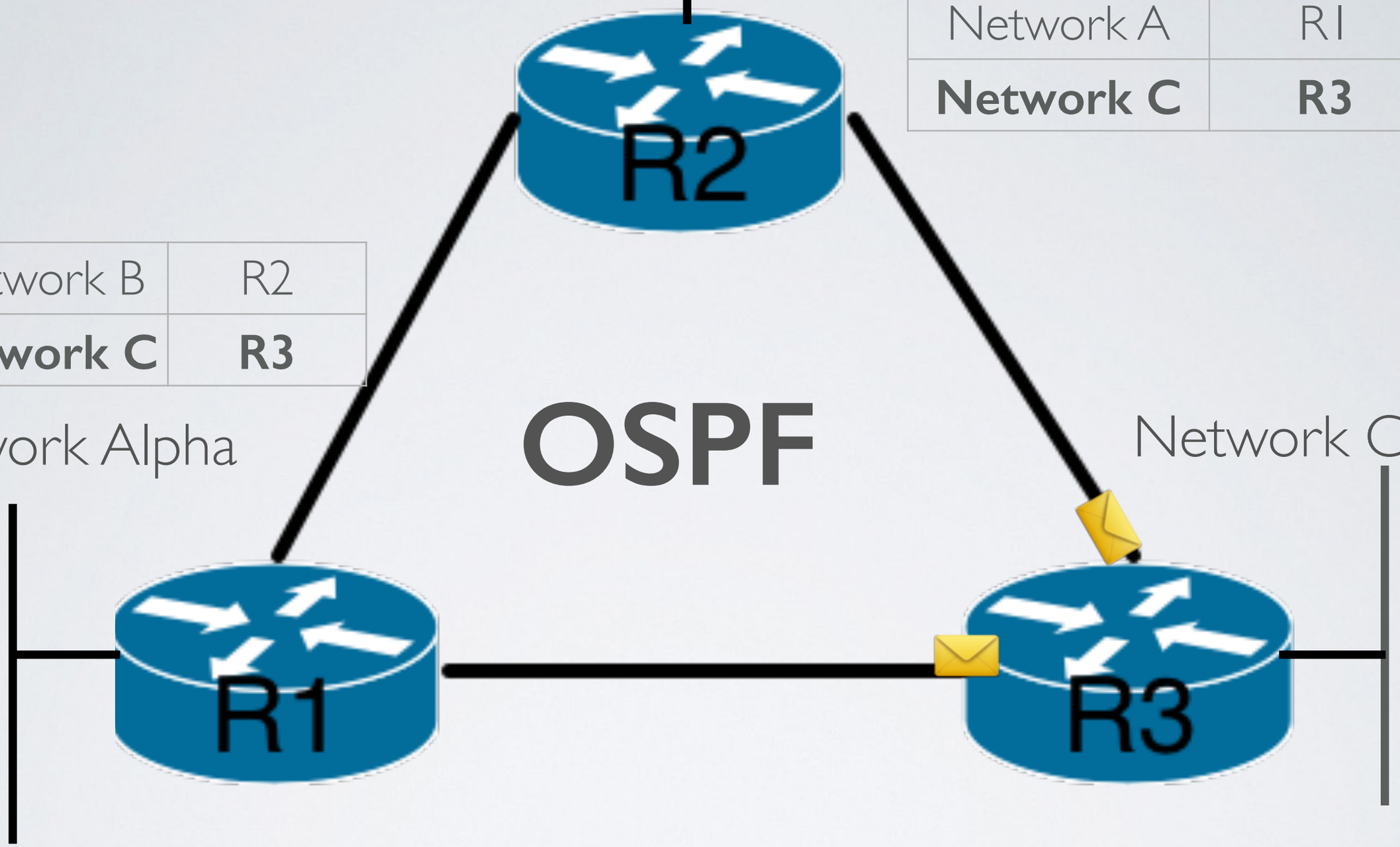
Network A	R1
Network C	**R3**

Network B	R2
Network C	**R3**

Network Alpha

OSPF

Network Charlie



DYNAMIC ROUTING

HOW TO EXPLOIT A VULNERABLE CONFIGURATION

bit.ly/1vkWpOP

MULTIPLE VULNERABILITIES

Old protocol (last RFC in 1998)

Information sent in clear text …

OSPF HEADER

```
▷ Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
▷ Ethernet II, Src: b8:6b:23:6c:d8:74 (b8:6b:23:6c:d8:74), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
▷ Internet Protocol Version 4, Src: 10.0.0.1 (10.0.0.1), Dst: 224.0.0.5 (224.0.0.5)
▽ Open Shortest Path First
  ▽ OSPF Header
      Version: 2
      Message Type: Hello Packet (1)
      Packet Length: 44
      Source OSPF Router: 10.0.0.1 (10.0.0.1)
      Area ID: 10.0.0.20 (10.0.0.20)
      Checksum: 0xceb8 [correct]
      Auth Type: Simple password (1)
      Auth Data (Simple): P4ssW0rd
  ▽ OSPF Hello Packet
      Network Mask: 255.255.255.0 (255.255.255.0)
      Hello Interval [sec]: 0
    ▷ Options: 0x12 (L, E)
      Router Priority: 1
      Router Dead Interval [sec]: 1
      Designated Router: 10.0.0.1 (10.0.0.1)
      Backup Designated Router: 0.0.0.0 (0.0.0.0)
```

MULTIPLE VULNERABILITIES II

Standard configuration of routers

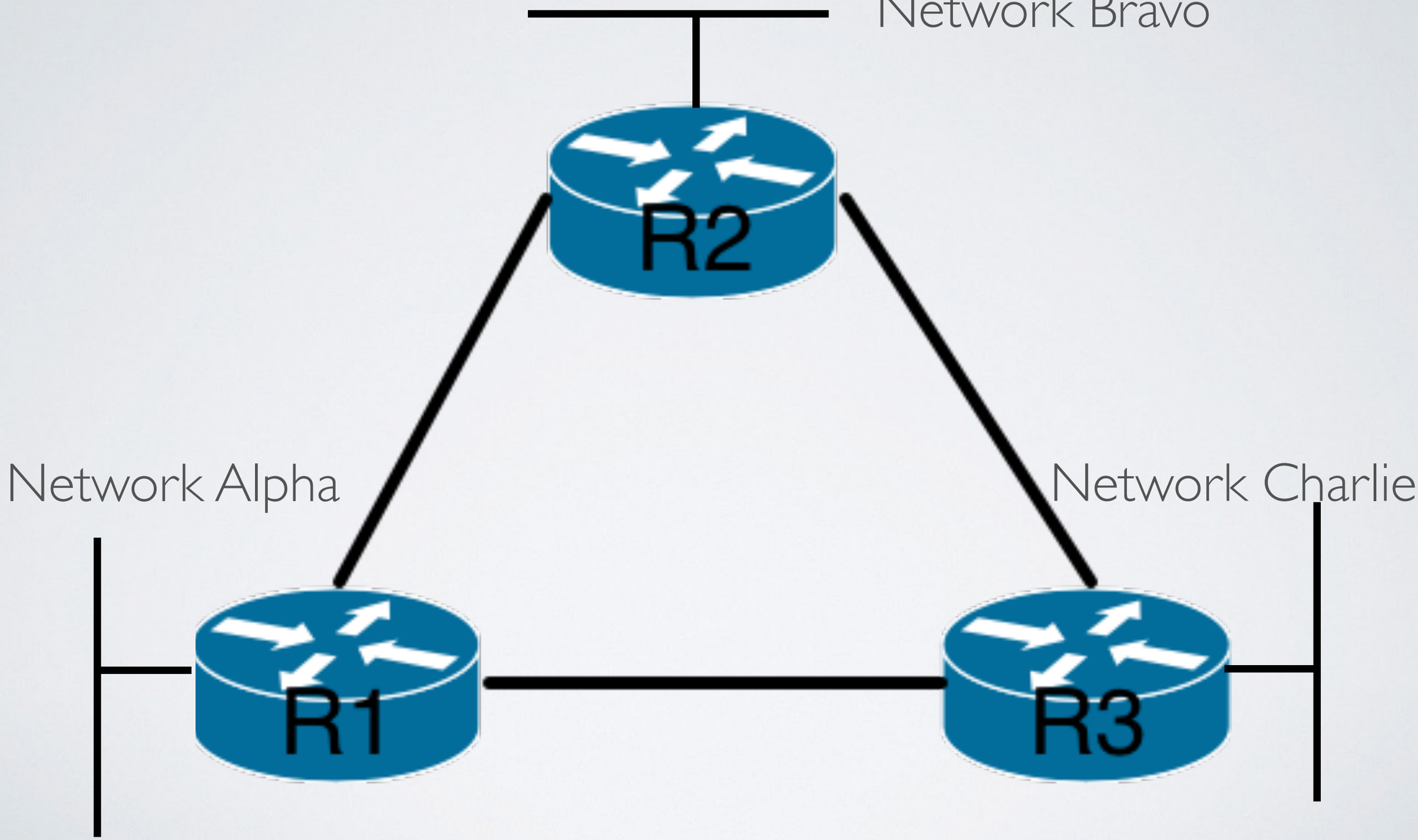
⇒ Clear text auth

⇒ add router to the network

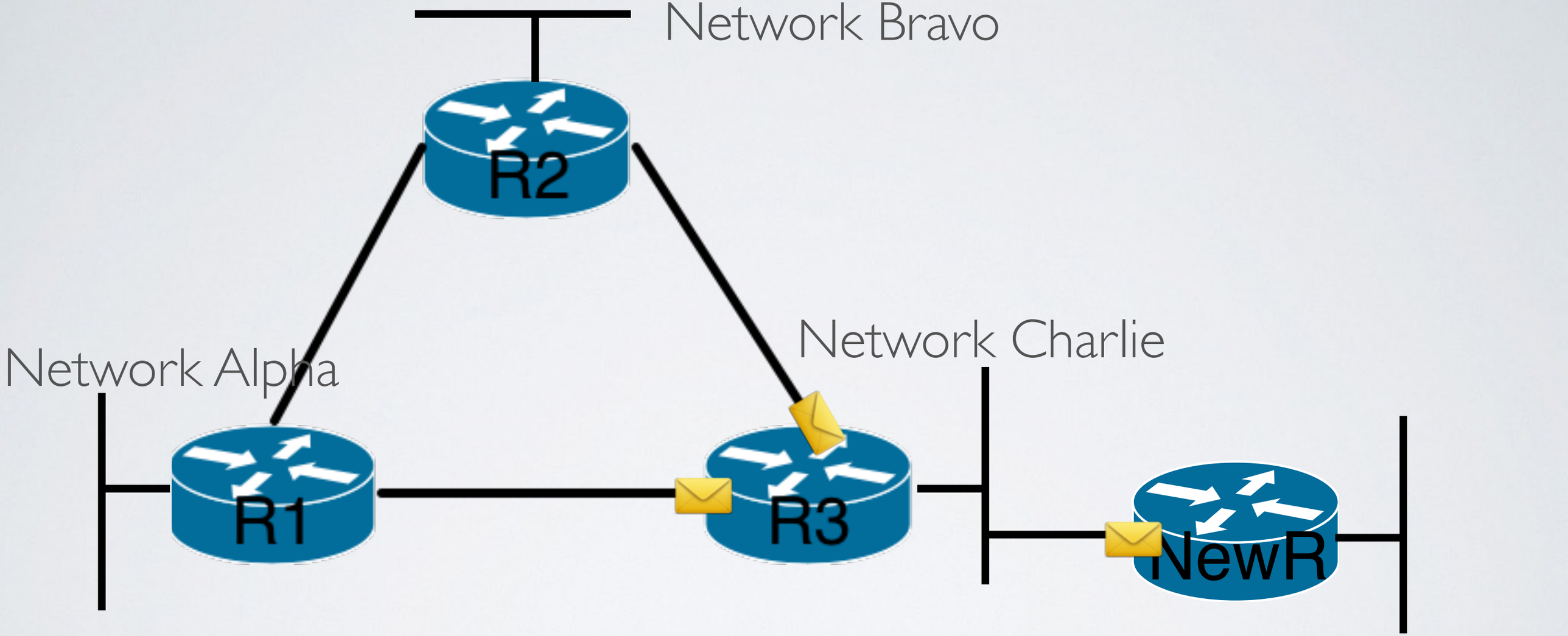
⇒ and then add new routes to the protocol

DYNAMIC ROUTING

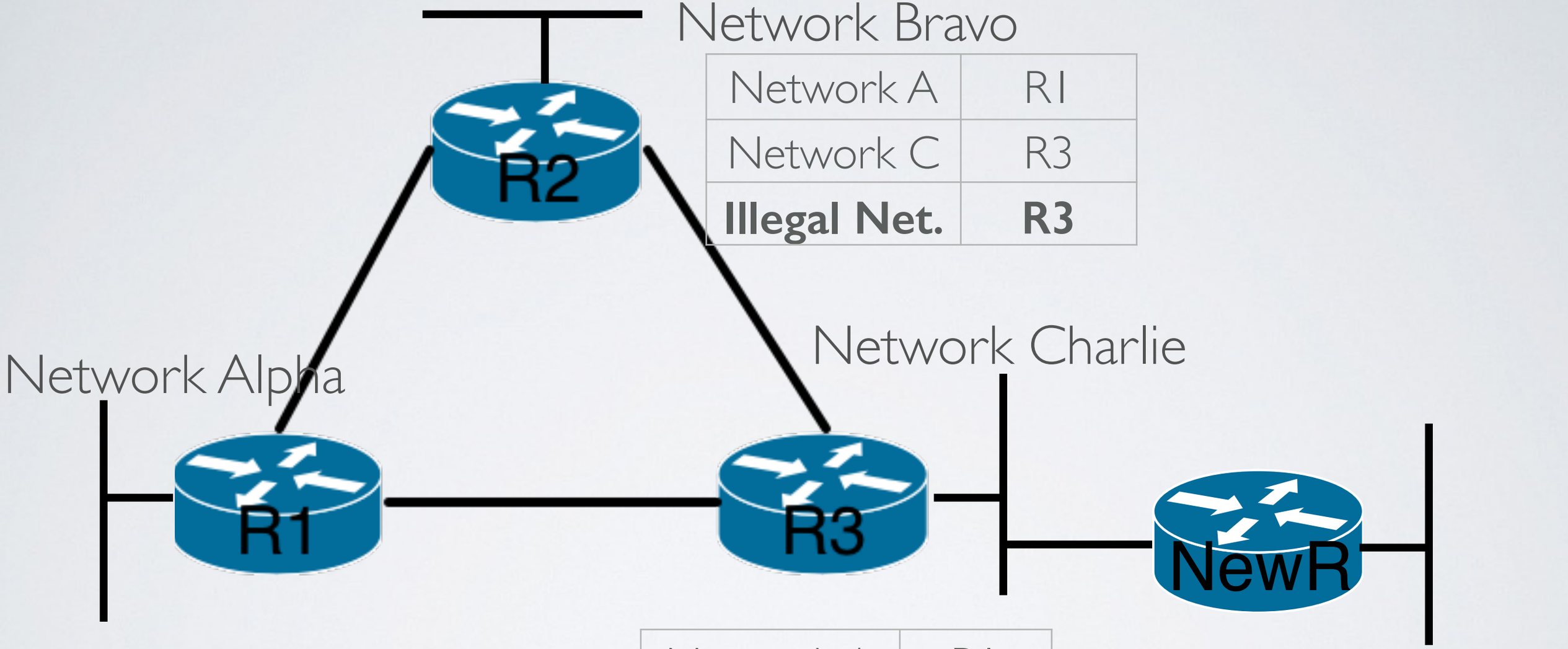
Network Bravo



DYNAMIC ROUTING



DYNAMIC ROUTING



Network A	R1
Network C	R3
Illegal Net.	**R3**

Network B	R2
Network C	R3
Illegal Net.	**R3**

Network A	R1
Network B	R2
Illegal Net	**NewR**

CONSEQUENCES

Re-route internal IP-traffic

Manipulate connections (DNS, DHCP, …)

Reroute external IPs to internal servers

WHAT ABOUT OTHER PROTOCOLS?

EIGRP

Distance-Vector Cisco Routing Protocol

```
▽ Cisco EIGRP
    Version: 2
    Opcode: Hello (5)
    Checksum: 0xeecb [correct]
  ▷ Flags: 0x00000000
    Sequence: 0
    Acknowledge: 0
    Virtual Router ID: 0 (Address-Family)
    Autonomous System: 1
  ▽ Parameters
      Type: Parameters (0x0001)
      Length: 12
      K1: 1
      K2: 0
      K3: 1
      K4: 0
      K5: 0
      K6: 0
      Hold Time: 15
  ▷ Software Version: EIGRP=12.4, TLV=1.2
```

```
▽ Cisco EIGRP
    Version: 2
    Opcode: Hello (5)
    Checksum: 0x617b [correct]
  ▷ Flags: 0x00000000
    Sequence: 0
    Acknowledge: 0
    Virtual Router ID: 0 (Address-Family)
    Autonomous System: 1
  ▽ Authentication MD5
      Type: Authentication (0x0002)
      Length: 40
      Type: MD5 (2)
      Length: 16
      Key ID: 1
      Key Sequence: 0
      Nullpad: 0000000000000000
      Digest: d894ae09c540ad2a8f66324f02efcf64
  ▷ Parameters
  ▷ Software Version: EIGRP=12.4, TLV=1.2
```

RIPv2

Distance-Vector Routing Protocol

```
▽ Routing Information Protocol
    Command: Request (1)
    Version: RIPv2 (2)
  ▽ Authentication: Simple Password
      Authentication type: Simple Password (2)
      Password: mysupersecurekey
  ▽ Address not specified, Metric: 16
      Address Family: Unspecified (0)
      Route Tag: 0
      Netmask: 0.0.0.0 (0.0.0.0)
      Next Hop: 0.0.0.0 (0.0.0.0)
      Metric: 16
```

```
▽ Routing Information Protocol
    Command: Request (1)
    Version: RIPv2 (2)
  ▽ Authentication: Keyed Message Digest
      Authentication type: Keyed Message Digest (3)
      Digest Offset: 44
      Key ID: 1
      Auth Data Len: 20
      Seq num: 6
      Zero Padding
    ▽ Authentication Data Trailer
        Authentication Data: 30 4d 80 fa f7 f5 35 0d
  ▽ Address not specified, Metric: 16
      Address Family: Unspecified (0)
      Route Tag: 0
      Netmask: 0.0.0.0 (0.0.0.0)
      Next Hop: 0.0.0.0 (0.0.0.0)
      Metric: 16
```

BGP

Exterior Gateway Protocol

This vulnerability is not applicable

Neighboring required to route

TOOLS

Wireshark

Loki

Quagga

Scapy (contrib module; no md5)

NRL Core

Nemesis

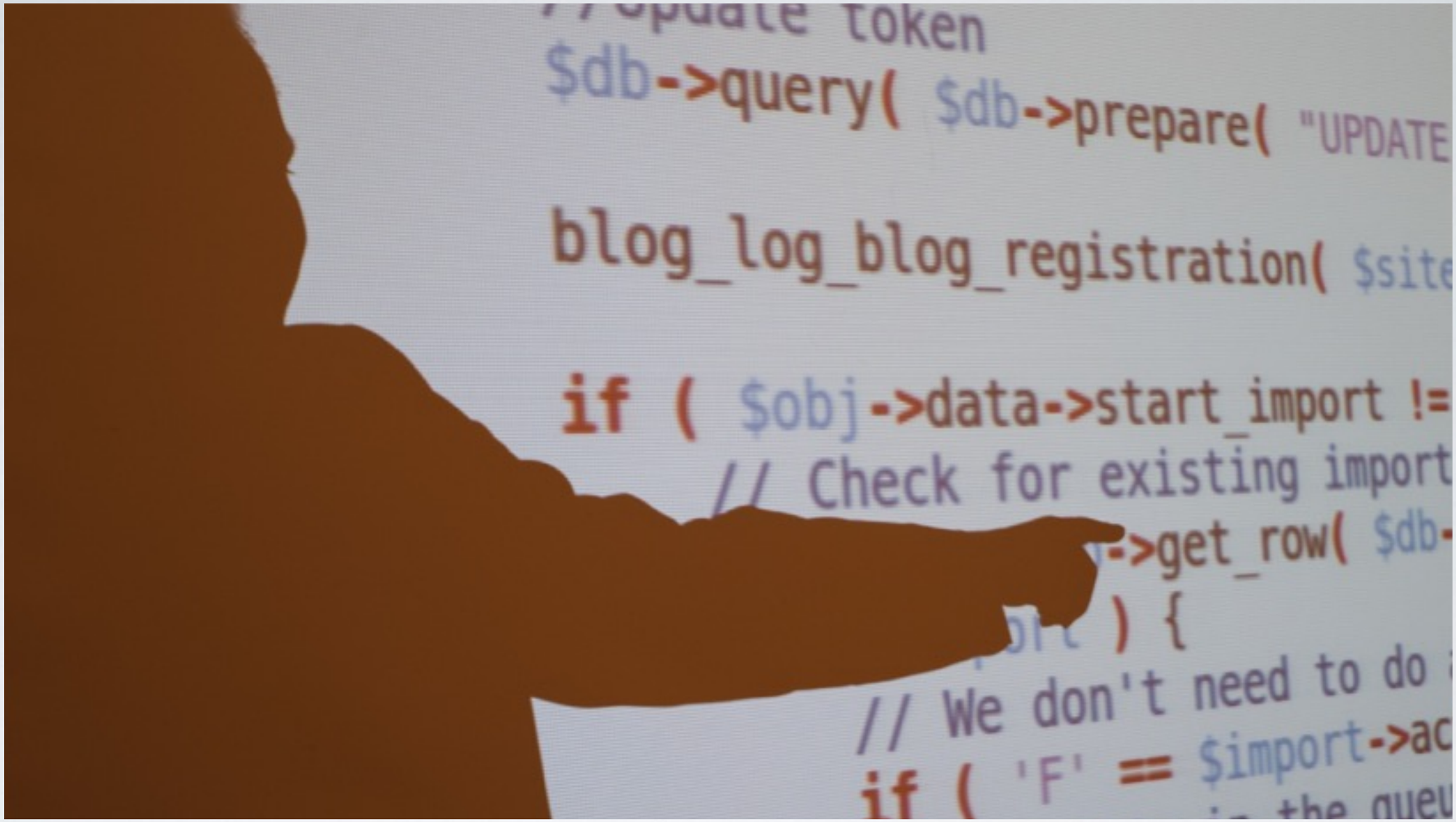
IP Sorcery

Cain&Abel

Net Dude

Collasoft

IRPAS



HOW TO AVOID MIS-CONFIGURATION

CONFIGURATION

Know your routers!

Review your configuration periodically

Limit the scope of your routing protocol

Test your configuration

JUNOS EXAMPLE

```
# show protocols ospf area 0.0.0.0
interface vlan.1 {
    retransmit-interval 5;
    hello-interval 2;
    dead-interval 10;
    authentication {
        md5 1 key "mypassword";
    }
}
interface ge-0/0/1.0 {
    passive;
}
```

QUAGGA EXAMPLE

```
router ospf
 ospf router-id 10.0.0.1
#
network 10.1.2.0/24 area 0
network 10.2.4.0/24 area 0
passive-interface eth0:1
#
redistribute kernel
redistribute connected
redistribute static
default-information originate
#
```

CISCO EXAMPLE

```
router ospf 1
 router-id 10.0.0.1
 log-adjacency-changes
 area 10.0.0.20 authentication
 redistribute connected metric 50 subnets
 redistribute static subnets
passive-interface default
no passive-interface FastEthernet0
network 10.11.12.0 0.0.0.255 area 20
network 192.168.42.0 0.0.0.255 area 20
```

CISCO EXAMPLE

```
interface FastEthernet0
 ip address 10.0.0.1 255.255.255.0
 ip ospf authentication message-digest
 ip ospf authentication-key P4ssW0rd
 ip ospf 1 area 10.0.0.20
 duplex auto
 speed auto
```

CISCO EXAMPLE

```
▽ Open Shortest Path First
  ▽ OSPF Header
      Version: 2
      Message Type: Hello Packet (1)
      Packet Length: 44
      Source OSPF Router: 10.0.0.1 (10.0.0.1)
      Area ID: 10.0.0.20 (10.0.0.20)
      Checksum: 0x0000 (None)
      Auth Type: Cryptographic (2)
      Auth Crypt Key id: 0
      Auth Crypt Data Length: 16
      Auth Crypt Sequence Number: 1408605512
      Auth Crypt Data: ef8a1311e6fd3d42ddc5b9ff1dd8dbd1
  ▽ OSPF Hello Packet
      Network Mask: 255.255.255.0 (255.255.255.0)
      Hello Interval [sec]: 0
    ▷ Options: 0x12 (L, E)
      Router Priority: 1
      Router Dead Interval [sec]: 1
      Designated Router: 10.0.0.1 (10.0.0.1)
      Backup Designated Router: 0.0.0.0 (0.0.0.0)
```

PATCH MANAGEMENT

Patch your network devices

Learn about new protocol (OSPFv3 w/ AH&ESP)

Use the new protocols

OTHER VULNERABILITIES?

Spoofed LSA (CVE-2013-0149)

CONCLUSION

Consider Routing as a critical asset

Monitor your network

Audit your network periodically

SPECIAL THANKS

WienCERT
IKT-Sicherheit im Magistrat

CERT.at

StaDt Wien
Wien ist anders.

WienCERT PGP-Key:
9B2C C43A 0B5A 6269 A438
A1FC 07FA F5B9 948A D027

CONTACT

louis@durufle.eu

@louisdurufle

REFERENCES

IP RFC https://tools.ietf.org/html/rfc791

OSPF v2 RFC http://tools.ietf.org/html/rfc2328

OSPF for IPv6 RFC http://tools.ietf.org/html/rfc5340

"An Experimental Study of Insider Attacks for the OSPF Routing Protocol" Brian Vetter, Feiyi Wang, S. Felix Wu (1997)

"Persistent OSPF Attacks" Gabi Nakibly and al. http://crypto.stanford.edu/~dabo/pubs/papers/ospf.pdf

"OSPF Security Project" Michael Sudkovitch and David I. Roitman, http://webcourse.cs.technion.ac.il/236349/Spring2013/ho/WCFiles/2009-2-ospf-report.pdf

Scapy OSPF Module https://raw.githubusercontent.com/d1b/scapy/master/scapy/contrib/ospf.py