Security of Networks, Services, and Systems

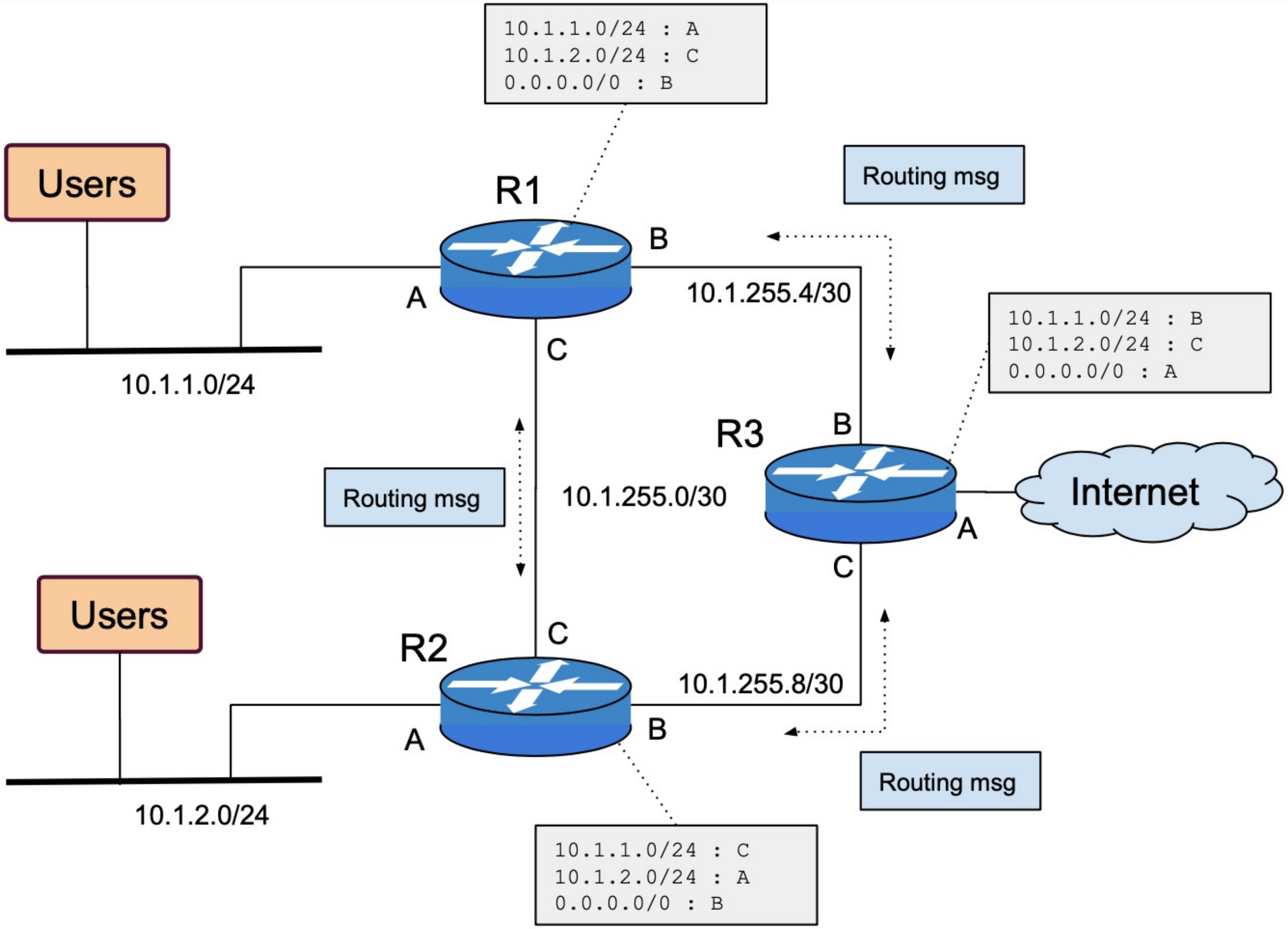
Routing Vulnerabilities

Ricardo Morla

FEUP – SSR/M.EEC, SR/M.EIC

Routing Example

- Routing tables updated by routing messages
- Two user networks
- Three routers
- One egress to the Internet
- All good



R1:

```
10.1.1.0/24 : A
10.1.2.0/24 : C
0.0.0.0/0 : B
```

R3:

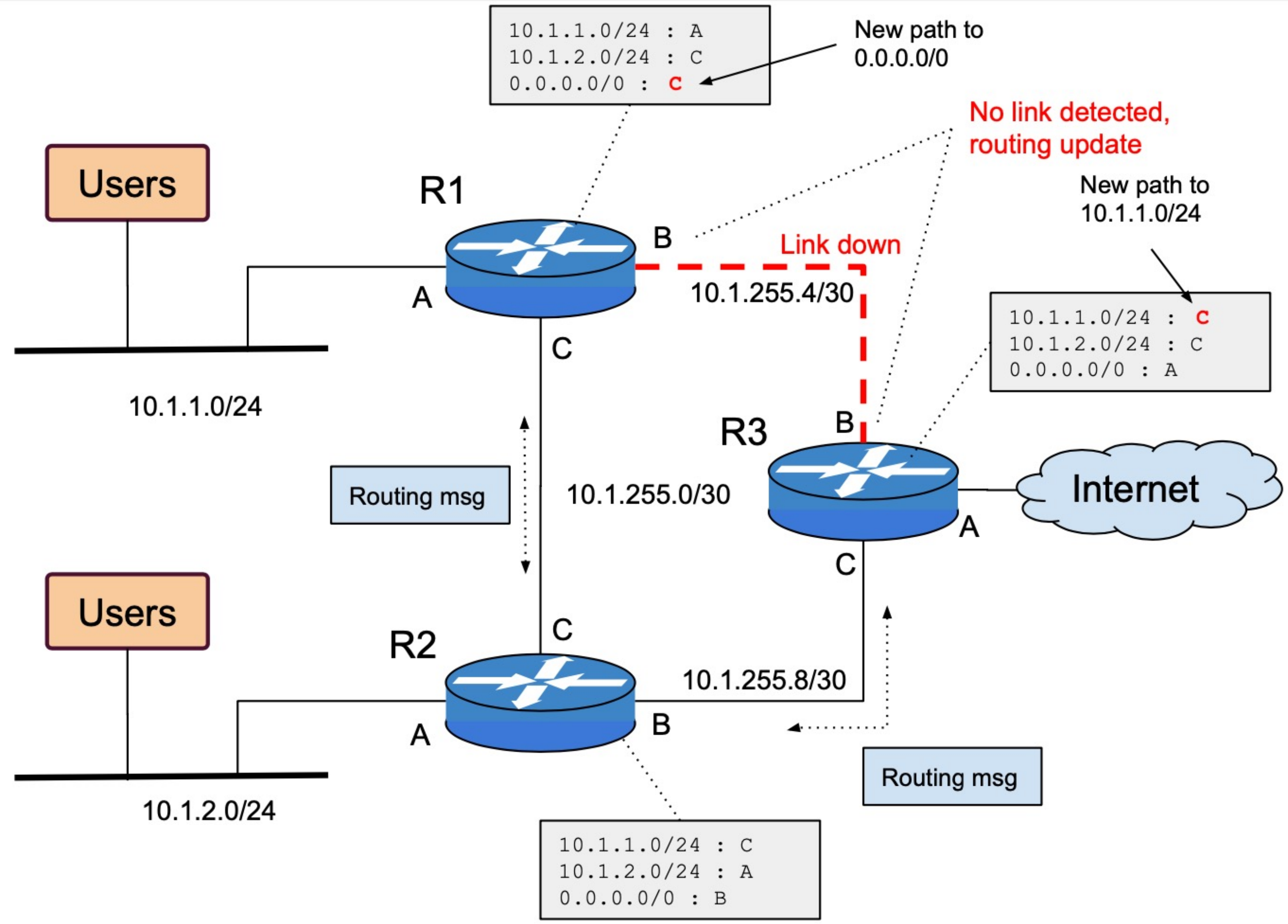
```
10.1.1.0/24 : B
10.1.2.0/24 : C
0.0.0.0/0 : A
```

R2:

```
10.1.1.0/24 : C
10.1.2.0/24 : A
0.0.0.0/0 : B
```

Link down

- R1, R3 detect link down on port B
- Run routing algorithm again without R1-R3 link
- Update routing table:
  - New default gateway on R1
  - New exit port for 10.1.1.0/24 on R3
- All still good – need to replace R1-R3 link



```
10.1.1.0/24 : A
10.1.2.0/24 : C
0.0.0.0/0 : C
```

```
10.1.1.0/24 : C
10.1.2.0/24 : C
0.0.0.0/0 : A
```

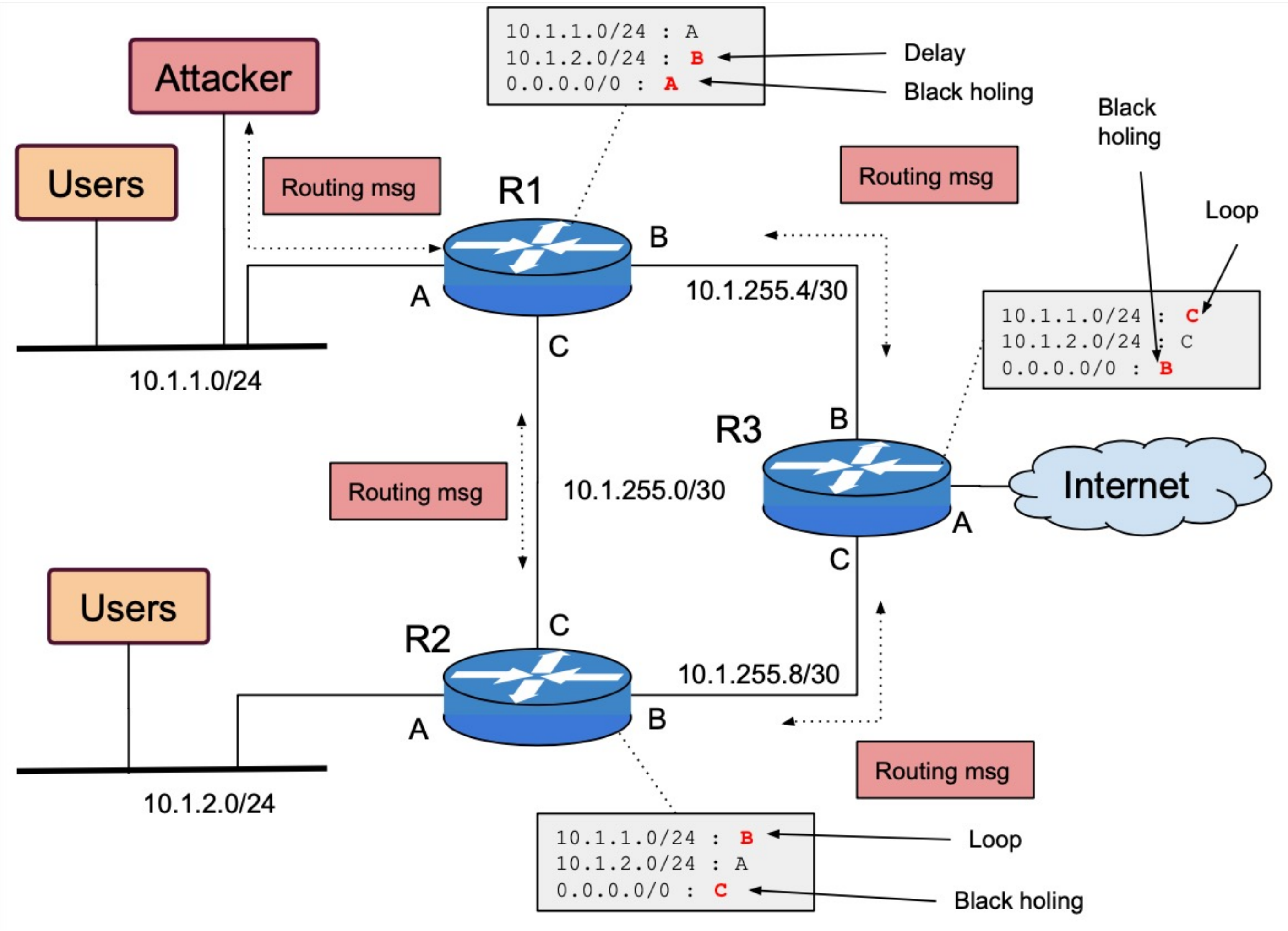
```
10.1.1.0/24 : C
10.1.2.0/24 : A
0.0.0.0/0 : B
```

Overview of vulnerabilities

- Data plane vs. control plane
    - Accessible ports
- Generic vulnerabilities
    - https://datatracker.ietf.org/doc/rfc4593/
    - Threats: disclosure of routing information, routing table poisoning, DoS, remote code execution
    - Consequences: eavesdropping, delay, congestion, loops, blackholing, partition, routing instability

Routing Attack (high level)

- Attacker injects malicious routing messages
- Default gateway on R1 port A: black hole default gw
- R1 to R2 via R3: add delay
- Loop between R2 and R3 for 10.1.1.0/24



RIP

- Distance vector protocol
  - Each router announces the distance to networks from this router
- Attacks
  - Host announces yourself as router
    - Router impersonation
  - Claim zero distance to non-directly connected networks
    - Prefix impersonation, black holing
  - Claim smaller distance to destination
    - Shorter distance attack – eavesdrop then redirect to destination
  - Claim longer distance to destination
    - Avoid traffic, cause network congestion on other links
  - Send arbitrary routing messages – poison routing tables, loops, routing instability

https://link.springer.com/content/pdf/10.1007%2F978-3-540-24852-1_8.pdf

OSPF

- Link state protocol
  - Each router announces the local links it has with its neighboring routers (LSA messages, link state announcements)
- Attacks
  - Falsify LSA of a router the attacker owns, small local impact
  - Falsify LSA of other, active routers
    - OSPF has fight-back mechanism, victim routers detect attack and send their legitimate LSA ; causes temporary instability in the routing
  - Falsify LSA of non-existing / phantom router
    - Not trigger fight-back, no impact on routing since both ends of a link must announce it, can overflow router LSA database
  - Others: remote false adjacency, disguised LSA, router RCE vulnerabilities

BGP

- Path vector protocol
  - Like distance routing but announces ids of nodes in path rather than distance
  - BGP updates with new paths to subnets are shared between ASs
- False updates
  - Announce route it does not have – cannot route packets to destination
  - Announce subnet prefix it does not own – zero distance from prefix
- Consequences
  - Black holing, session hijacking, instability

Some references for different protocols

- RIP
  - https://link.springer.com/content/pdf/10.1007%2F978-3-540-24852-1_8.pdf
- OSPF
  - http://theory.stanford.edu/~dabo/papers/ospf.pdf
  - https://www.sanog.org/resources/sanog28/SANOG28-Tutorial_OSPF-Security-Attacks-and-Defences-Manjul.pdf
- BGP
  - https://www.cc.gatech.edu/~dovrolis/Papers/ccr-bgp.pdf

Security of Networks, Services, and Systems

Routing Vulnerabilities

Ricardo Morla

FEUP – SSR/M.EEC, SR/M.EIC