Security of Networks, Services, and Systems

Network Access Control

Ricardo Morla

FEUP – SSR/M.EEC, SR/M.EIC

Network Access Control

- Internal vs. external access
- Physical access
- Same LAN access
- IP routing access
- Service access
- End-user device and VM isolation

Internal vs. external access

- Perimeter defense
  - Think circle and circumference – inside circumference: safe; outside: unsafe
  - Where should we define the perimeter? Internet? DMZ? Admin network?
  - NAT, don’t route internal IPs out
  - Firewall, filter incoming ports and IPs
- Threat model expanded
  - From external threats only
  - To external and internal threats
  - Internal networks safe?
  - To which point do I trust sub-networks and end points – desktops, mobile?
  - Multiple perimeters: external, between sub-networks, end-point perimeter

Physical access

- Unsused ports on accessible network devices
- Unplug ethernet cable from desktop computer
- Insecure wifi AP

- Harden access
  - Restrict access to given MAC/IP (vulnerable to spoofing)

    ```
    switchport port-security mac-address 01:02:03:05:07:0B
    ```
  - 802.1x on both wireless and wired
  - Secure physical access to rooms with cables and sockets

Same LAN access

- Numerous vulnerabilities can be exploited if the attacker has access to the Ethernet layer
- So why should different types of users be on the same LAN?

- Split your network into sub-networks, use VLANs
  - This prevents funny stuff at layer 2 across the network
  - Funny stuff at layer 2 can still happen inside the sub-network
  - Watch out for VLAN hopping, management VLAN, and other vulnerabilities

- Why can’t you have a VLAN for each user?

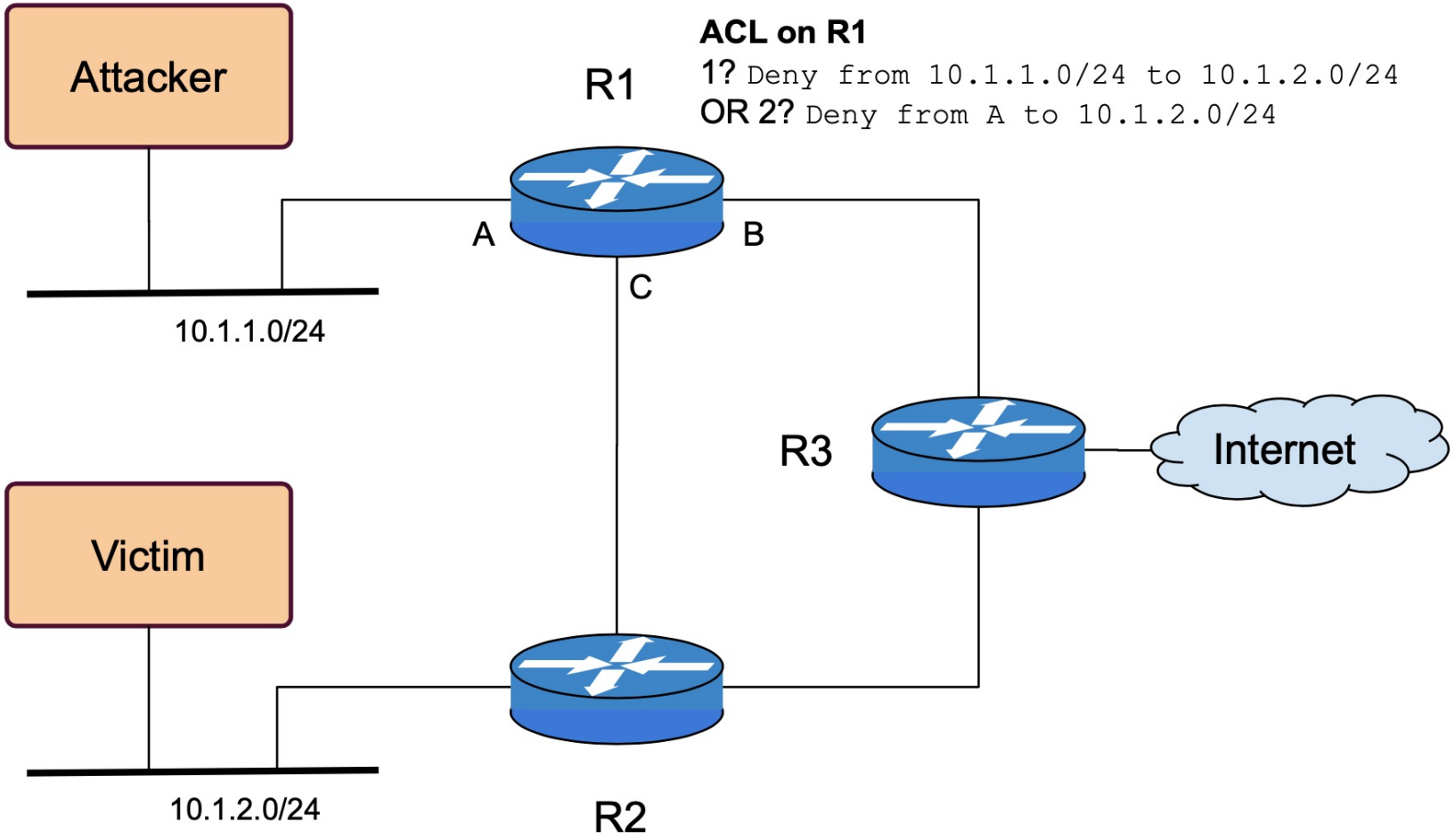
IP routing access (1/2)

- If the attacker can't send IP packets to the victim, then it has a harder time doing its business
- Why should you allow all-to-all routing inside your network? Do your users really need to contact any IP address?

- Write strict access control lists on your routers, allow only traffic that makes sense
  - This prevents funny stuff at layer 3 across the network Funny stuff at layer 2 can still happen inside the sub-network

```
access-list 101 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
int fa0/0 ; ip access-group 101 in
```

IP routing access (2/2)



Service access

- Vulnerable services (TCP/UDP)
- Prevent access to these services from specific networks
  - Router ACLs or firewalls?
- More on firewalls on another set of slides

End-user device and VM isolation

- End user devices or VMs can be compromised
- Extend the perimeter to these devices and VMs
  - I’m sure therer’s a good reason for not simply unplugging them

- Make sure you still provide basic networking
  - move to quarantine network
  - apply rules on hypervisor

- If basic networking is enough… why did you provide more?

How complex is your access control?

- Keeping track of which communication patterns make sense and which don’t is a lot of work
  - Alternative models? No security on the network, push all security to end points? Problems?
- Rely on:
  - Knowledge of your nework, services, users
  - Security mechanisms available on the network devices
  - Automation

Security of Networks, Services, and Systems

Network Access Control

Ricardo Morla

FEUP – SSR/M.EEC, SR/M.EIC