Introduction to Routing
Security Problems

Matthias Wählisch
m.waehlisch@fu-berlin.de
www.cs.fu-berlin.de/~waehl
Routing Security Problems
Routing should enable reachability
Routing should enable reachability
Routing should enable reachability
Routing should enable reachability
Why should you care?

Exploiting BGP Updates can lead to traffic interception
… to break privacy
… to break service availability
(e2e protection doesn’t help!)
Routing Security Problems
BGP [RFC 4271]: Main security problem

BGP is based on trust

A BGP peer cannot verify the correctness of prefixes, AS paths, etc.
Threat models for BGP

Prefix Origin Hijacking

AS Path Manipulation

Route Leaks
Threat models for BGP

Prefix Origin Hijacking
- Originate an IP prefix that you don’t own

AS Path Manipulation
- Change the AS path compared to the original traversal

Route Leaks
Simple example

- Provider A
- AS Z
- AS V
- AS Y
- AS X
- AS W
- Provider B
- 10.20.0.0/16
- Customer
Simple example (1): Traffic flow

AS Z

AS V

Provider A

Customer

AS Y

AS X

AS W

Provider B

10.20.0.0/16

10.20.0.0/16

A V Z
Simple example (1): More specific wins

AS Z
10.20.0.0/16

AS V
10.20.0.0/16

Provider A

Customer

AS Y

AS X

AS W

Provider B

10.20.0.0/24
Simple example (2): Multiple upstreams

AS Z
 AS Y
 AS X
 AS W

Provider A

AS V

Customer

10.20.0.0/16

Provider B

10.20.0.0/16

A V Z

B W X Y Z
Shorter path wins, AS B configures:

```python
if net = 10.20.0.0/16 then {
    bgp_path.empty;
    bgp_path.prepend(B);
    bgp_path.prepend(Z);
    accept;
}
```
Simple example (2): Shorter path wins
Real-world examples – There are more!

2008: YouTube Hijack
Pakistan Telecom announced a more specific prefix from YouTube

2010: China Telecom Incident
China announced ~50k prefixes incorrectly

2017: Russian Routing Leak
AS39523 announced 80 prefixes incorrectly
Real-world examples – There are more!

2008: YouTube Hijack
Pakistan Telecom announced a more specific prefix from YouTube

2010: China Telecom Incident
China announced ~50k prefixes incorrectly

2017: Russian Routing Leak
AS39523 announced 80 prefixes incorrectly

Those cases could easily be prevented by proper (RPKI) filtering!
Threat models for BGP

- Prefix Origin Hijacking
- AS Path Manipulation
- Route Leaks

Announce prefixes conflicting with business expectations
Customer announces transit to provider
Conclusion & What’s next?

Conclusion

• BGP is based on trust. That is insufficient.
• You need to act now!

Remainder of this Webinar

• How to monitor Internet routing?
• Current and future solutions.