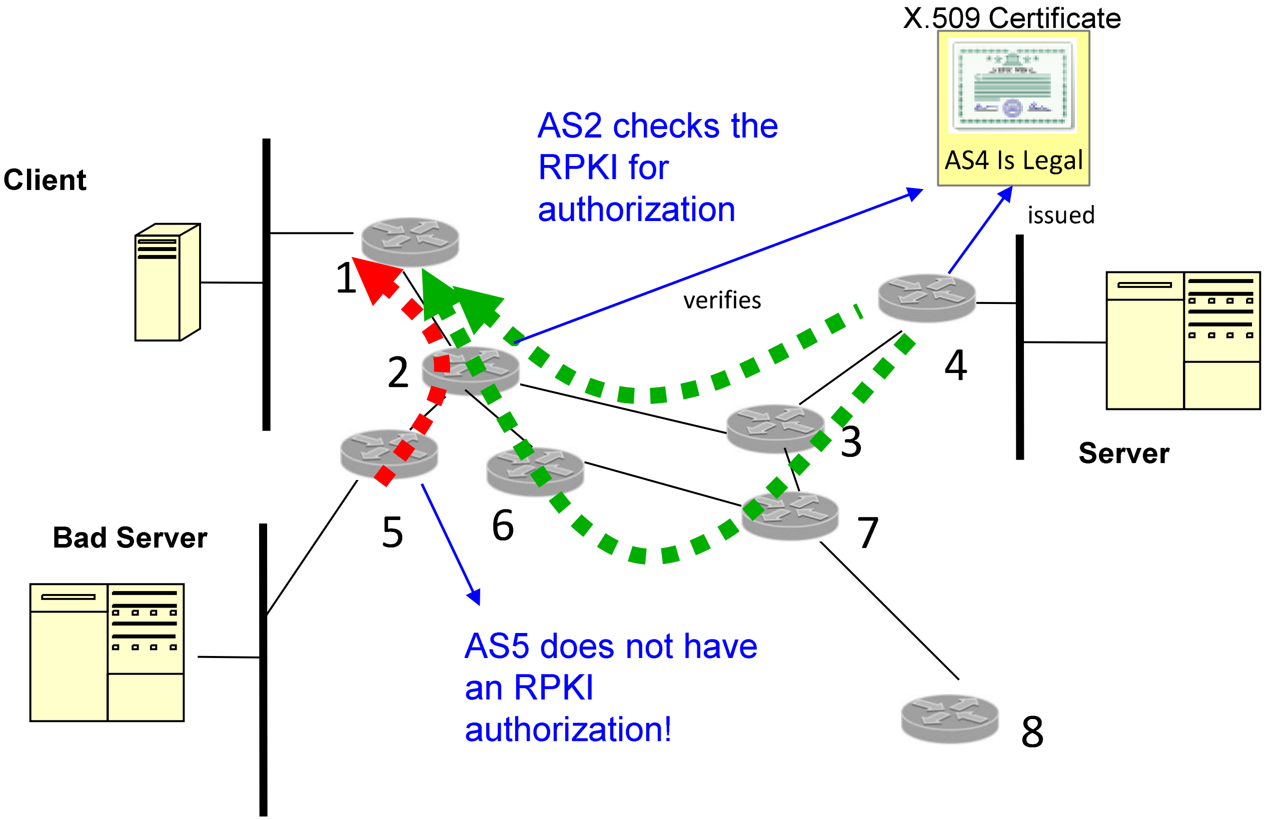
The Need For BGP Path Validation

Wes Hardaker
<wes.hardaker@parsons.com>

Example RPKI Origin Validation



AS2 checks the RPKI for authorization

AS5 does not have an RPKI authorization!

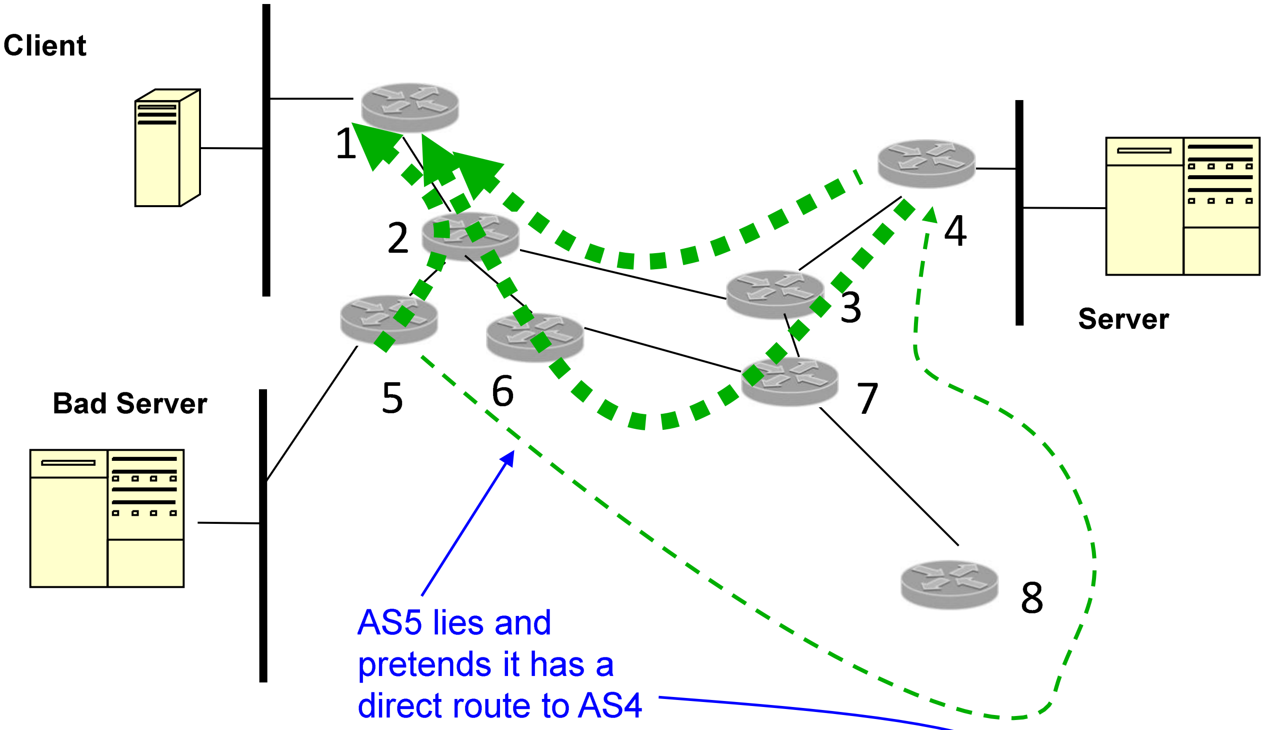
Will be rejected

RPKI Provides Origin Validation:

- Cryptographically signed authorization for AS4 to advertise Routes to Server

- INVALID (Doesn't Go To AS4): AS1 ► AS2 ► AS5
- VALID (Origin is AS4): AS1 ► AS2 ► AS3 ► AS4
- VALID (Origin is AS4): AS1 ► AS2 ► AS6 ► AS7 ► AS3 ► AS4

What If AS5 Lies?



AS5 lies and pretends it has a direct route to AS4

AS5 can still advertise a route with AS4 at the end:
(even though AS5 isn't connected to AS4)

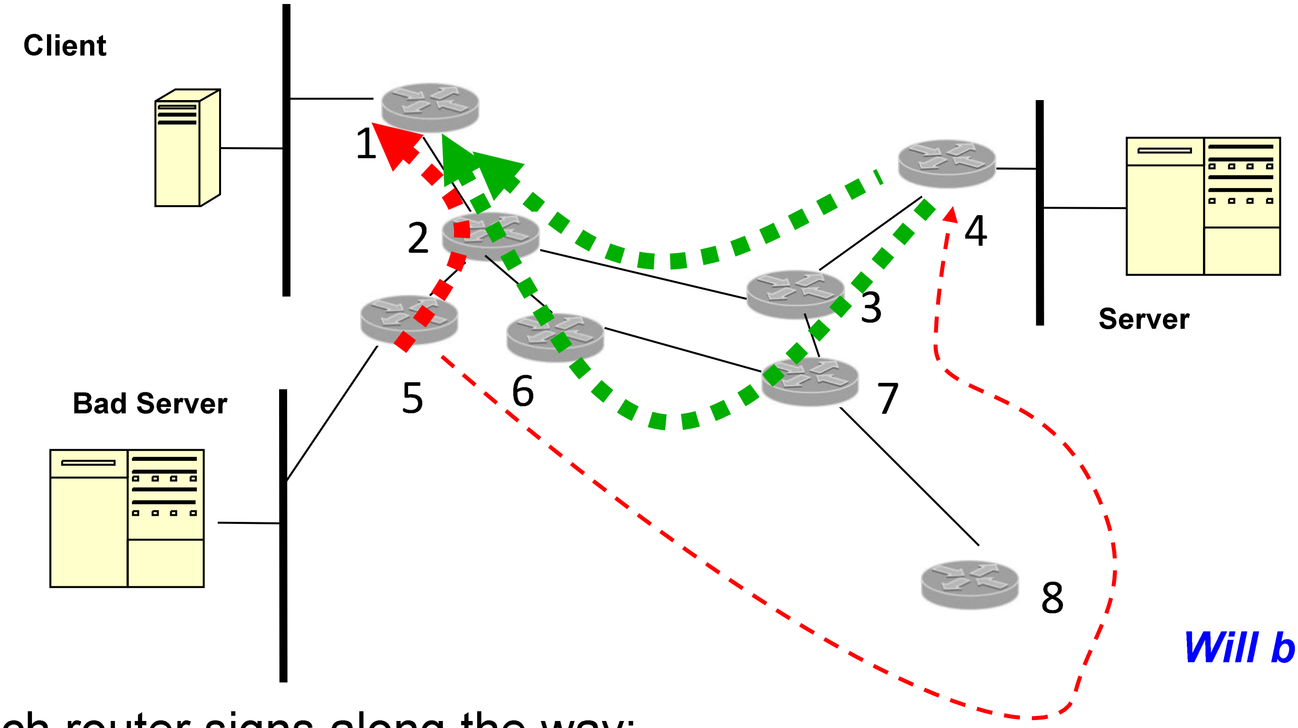
- VALID (Origin is AS4): AS1 ▶ AS2 ▶ AS5 ▶ AS4
- VALID (Origin is AS4): AS1 ▶ AS2 ▶ AS3 ▶ AS4
- VALID (Origin is AS4): AS1 ▶ AS2 ▶ AS6 ▶ AS7 ▶ AS3 ▶ AS4

Path Validation Is Critical

Step 2 in the Routing Security Solution!

- AS4 **must** prove it started the route
  - It **must** prove that only AS3 is next in its path
  - No other router can reuse or copy its initial route
- ASes can be assured the entire path is valid
- Enter BGPSEC!
  - Lies can now be detected!

BGPSEC's Path Validation

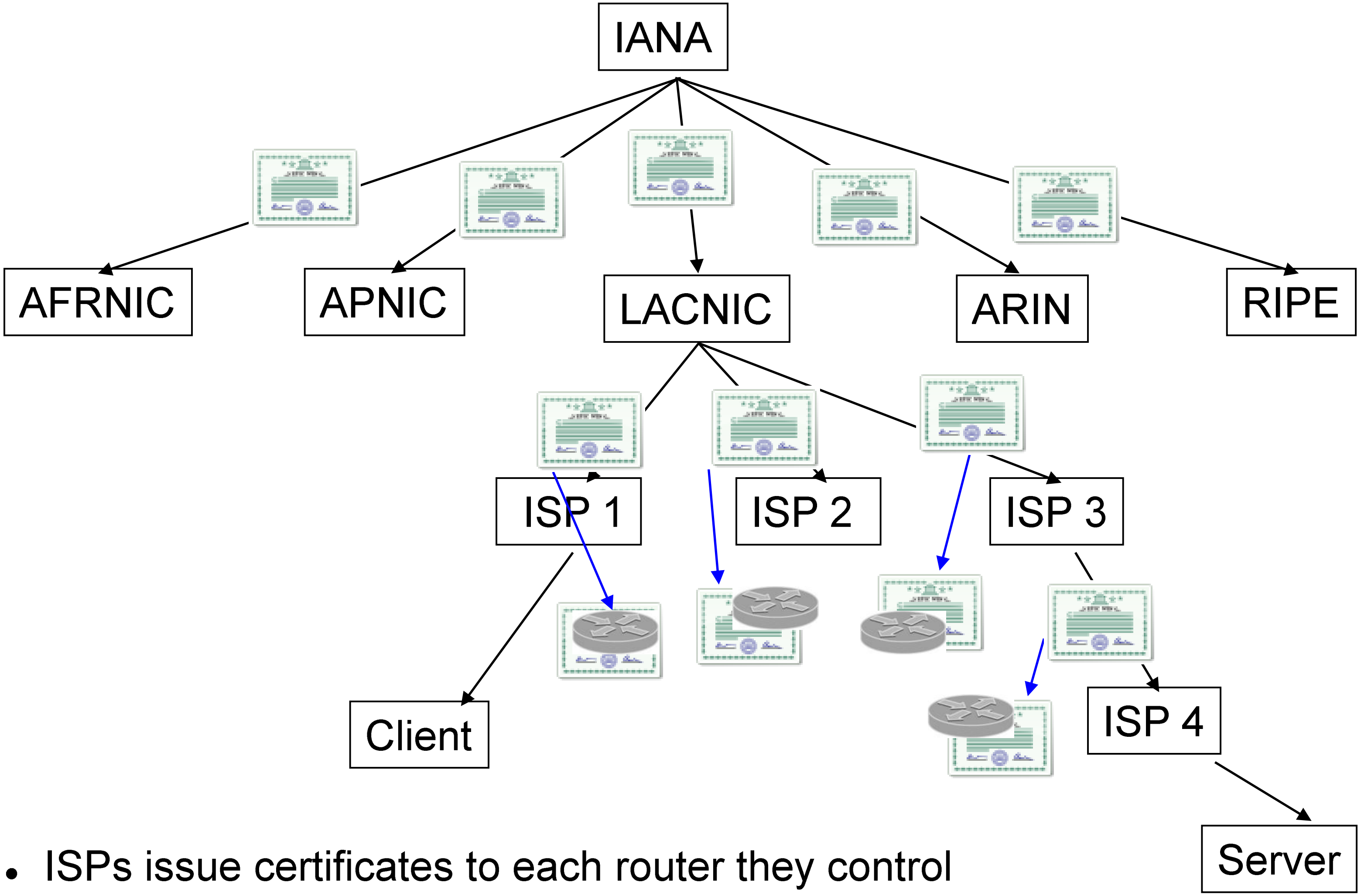


Will be rejected again.

Each router signs along the way;
the paths can not be spoofed or modified

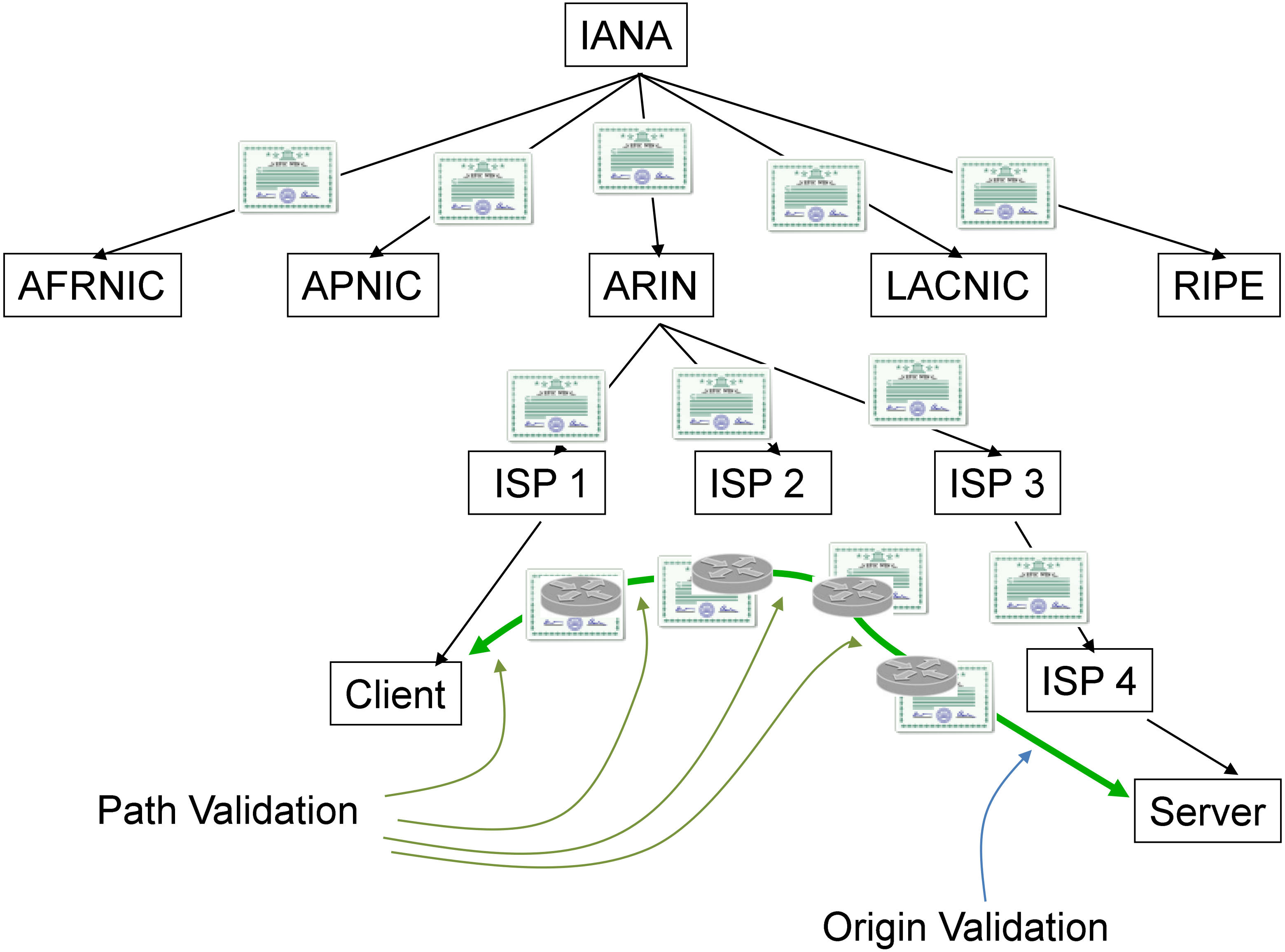
- INVALID (Origin signed, path is not): AS1 ▶AS2 ▶ AS5 ▶ AS4
- VALID (Origin and path signed): AS1 ▶AS2 ▶ AS3 ▶ AS4
- VALID (Origin and path signed): AS1 ▶AS2 ▶ … ▶ AS3 ▶ AS4

RPKI and BGPSEC – Certificate Tree



- ISPs issue certificates to each router they control

BGPSEC – Router Certificates



IANA

AFRNIC

APNIC

ARIN

LACNIC

RIPE

ISP 1

ISP 2

ISP 3

ISP 4

Client

Server

Path Validation

Origin Validation