

# Progress Toward Security the Routing Infrastructure

Sandra Murphy

[Sandra.Murphy@sparta.com](mailto:Sandra.Murphy@sparta.com),

[Sam.Weiler@sparta.com](mailto:Sam.Weiler@sparta.com)

*Supported by, or in part by, the U. S. Army Research Laboratory and the U. S. Army Research Office under contract/grant number W911NF-05-C-0113, through funding provided by Department of Homeland Security Directorate for Science and Technology*

# History of Routing Outages

## Commercial Internet -- specific network outages

- **Apr 1997 – AS 7007 announced routes to all the Internet**
- Apr 1998 – AS 8584 mis-announced 100K routes
- Dec 1999 – AT&T's server network announced by another ISP – misdirecting their traffic (made the Wall Street Journal)
- May 2000 – Sprint addresses announced by another ISP
- Apr 2001 – AS 15412 mis-announced 5K routes
- **Dec 24, 2004 – thousands of networks misdirected to Turkey**
- Feb 10, 2005: Estonian ISP announced a part of Merit address space
- **Sep 9, 2005 – AT&T, XO and Bell South (12/8, 64/8, 65/8) misdirected to Bolivia [the next day, Germany – prompting AT&T to deaggregate]**
- Jan 22, 2006 – Many networks, including PANIX and Walrus Internet, misdirected to NY ISP (Con Edison (AS27506))
- Feb 26, 2006 - Sprint and Verio briefly passed along TTNET (AS9121 again?) announcements that it was the origin AS for 4/8, 8/8, and 12/8
- **Feb 24, 2008 –Pakistan Telecom announces /24 from YouTube**
- March 2008 – Kenyan ISP's /24 announced by AboveNet
- Frequent full table leaks, e.g., Sep08 (Moscow), Nov08 (Brazil), Jan09(Russia)

# So Maybe It's Not So Bad ...

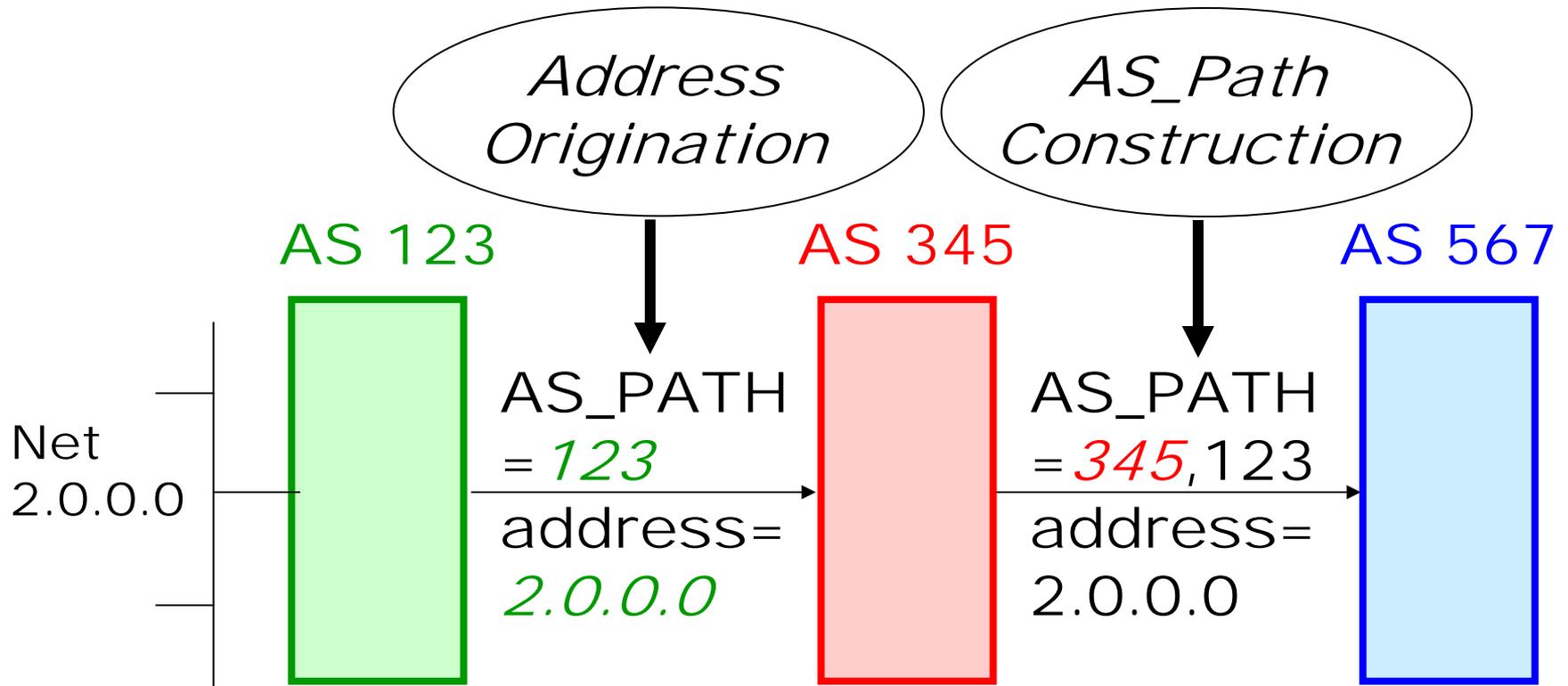
- Response is now under an hour
  - *but this is no one's idea of reliable networking*
  - *damage to applications, and to the Internet itself in terms of churn and routing table size*
- These are human mistakes, not attacks
  - *but anything possible through human error can be done by human intent*
  - *deliberate attacks would be repeatable at will*
- There are bigger outages due to hardware and software failures
  - *but those aren't exploitable deterministically and remotely*



# Progress in Security for Internet Routing

- The IETF is devising an architecture that will protect Internet routing
- This talk will
  - Review BGP
  - Discuss the IETF architecture
  - Discuss the architecture uses and integration in operation practices
  - Discuss issues being resolved and open issues

# Brief Synopsis of BGP

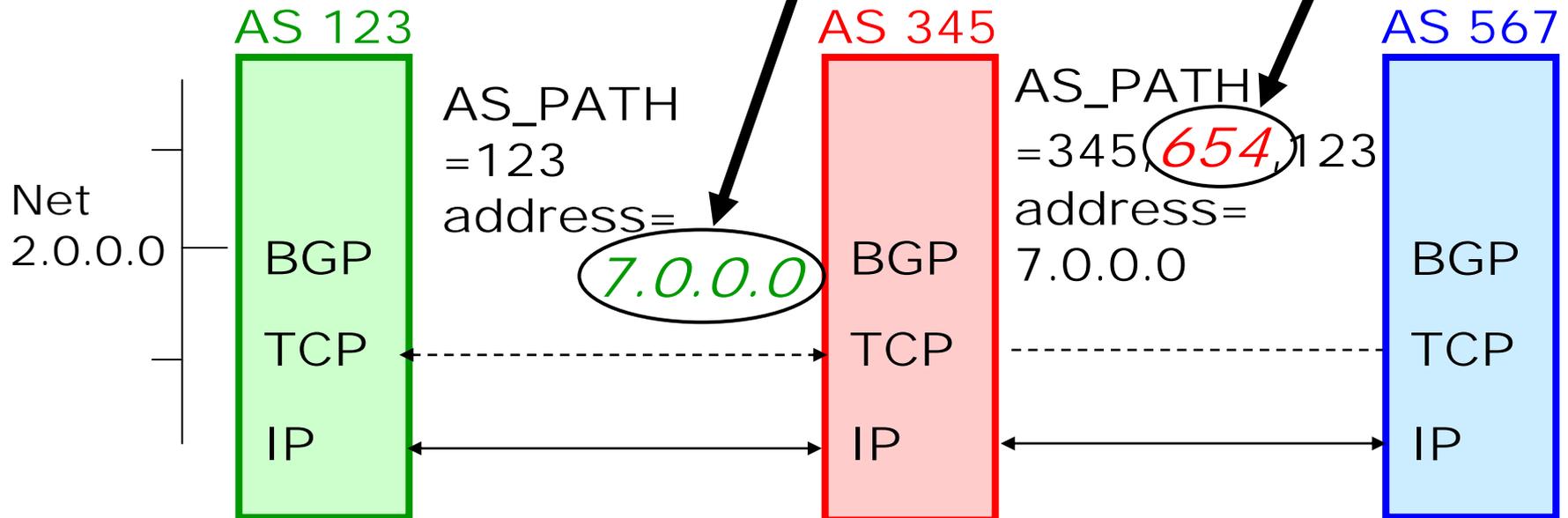


AS = an Autonomous System, i.e., ISP, enterprise  
 Each message announces reachability to an address  
 Each AS adds their AS number to the path – for loop detection

# BGP Vulnerabilities

*ROUTING  
INFO  
ATTACKS:*

*MIS-ORIGINATION      MIS-CONSTRUCTION of PATH  
e.g., AS\_PATH POISONING*

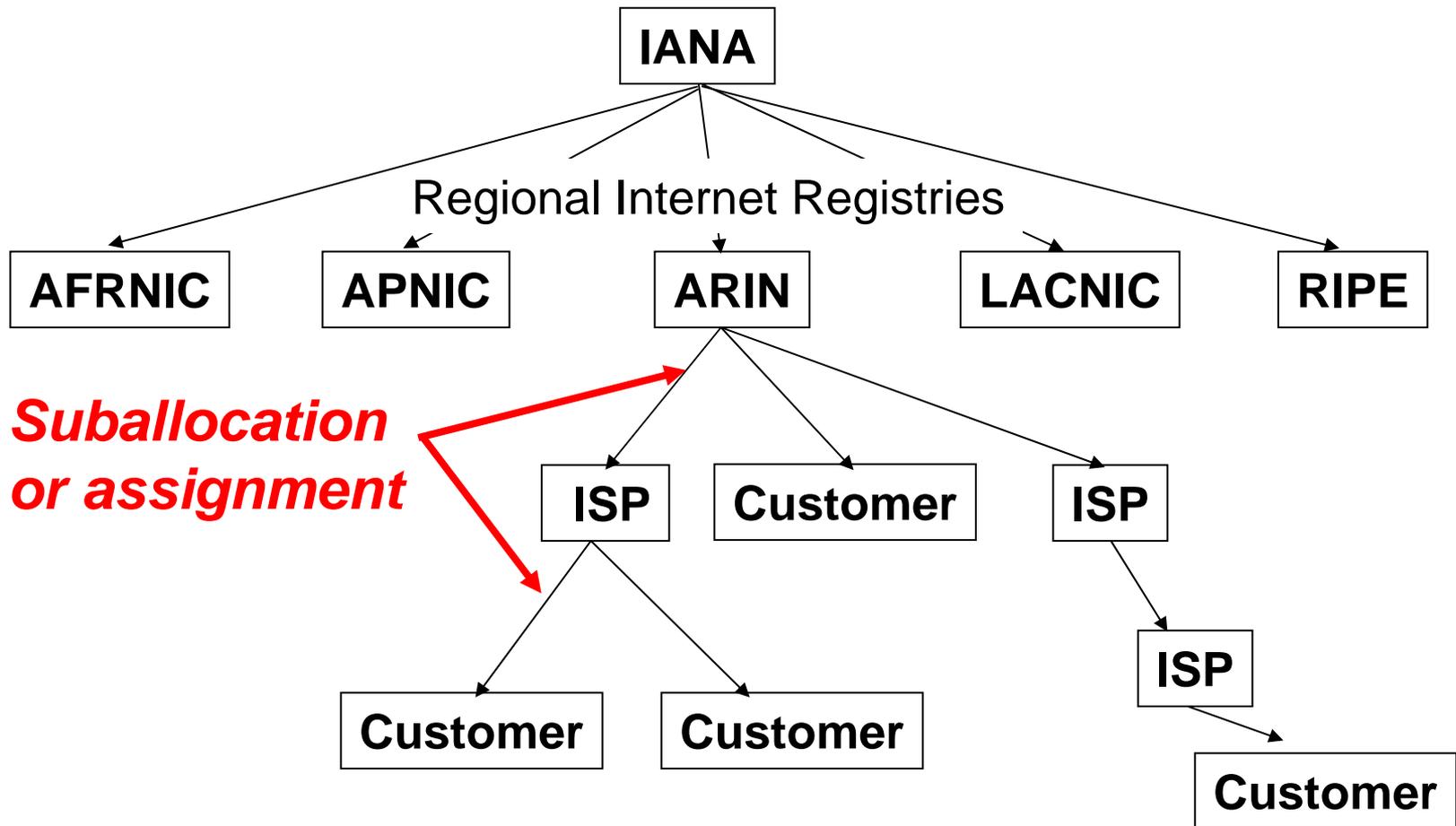


# Strategy of Protection

- The initial step in building a route is the *origination* of a route, showing a direct connection
- Most public routing incidents were mis-originations
- Start with authorizing origination of routes, based on who is allocated the use of the address

# Who is Allocated the Use of an Address

Internet Assigned Numbers Authority



# Current Practice: Routing Registries

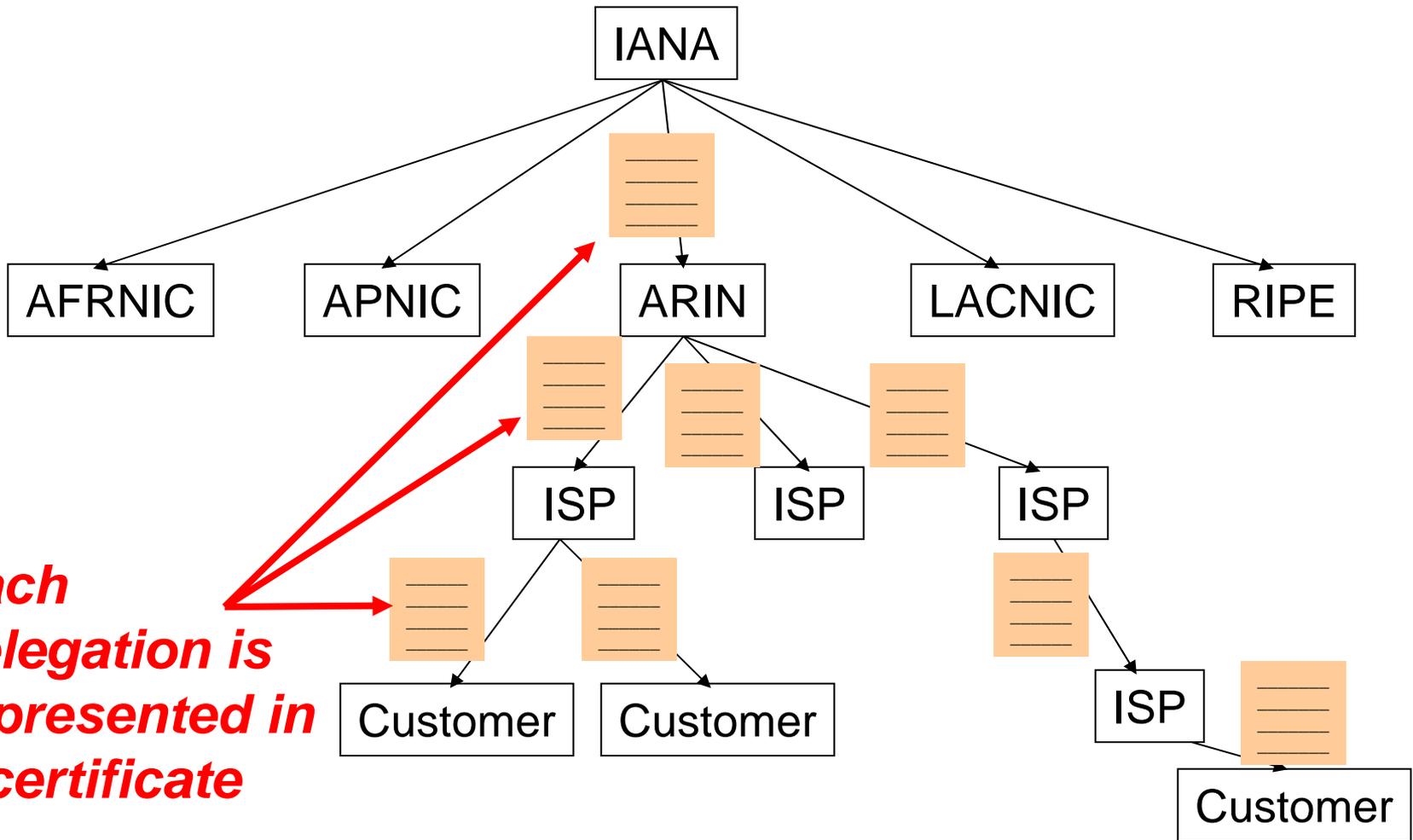
- Routing registries are databases
  - record an AS's *route objects* – addresses the AS asserts it may originate
- The desired authority is: only the address holder is authorized to speak for the routing of the address
  - But routing registries can not always authenticate the address holder, and so can not validate the registry of route objects.
  - Problems with stale and inaccurate data
- Trust model doesn't scale – channel security



# New Work: IETF Resource Public Key Infrastructure (RPKI)

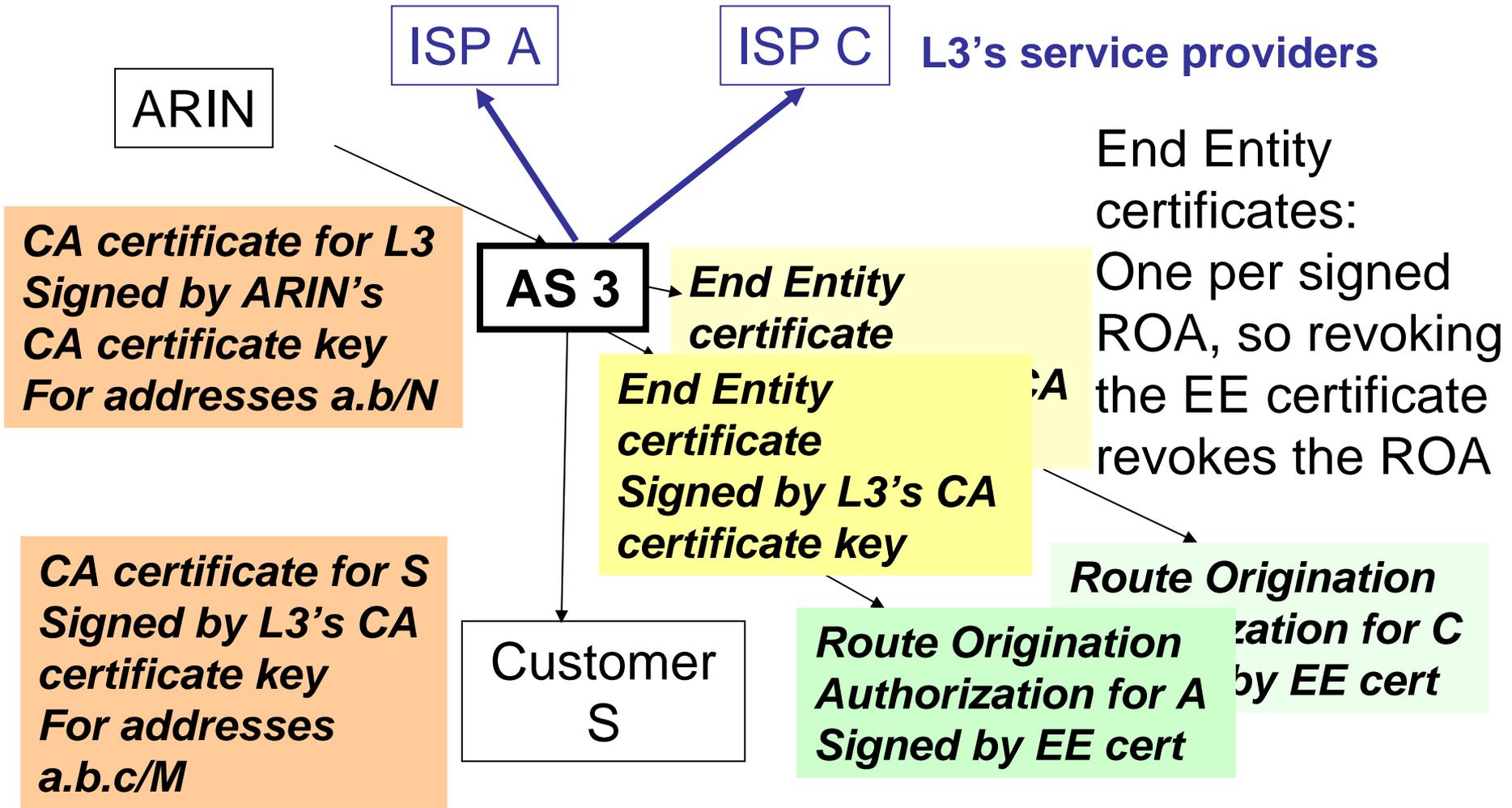
- Provides authorization for who can originate a route to an address
- Uses an object security model
- Three components:
  - Resource Certificates
  - Route Authorizations
  - Repository System

# RPKI - Resource Certificates



***Each delegation is represented in a certificate***

# RPKI - Route Authorizations



# RPKI – Repository System

- Each Certificate Authority manages a repository publication point
  - so there are many of these points distributed over the Internet
- Each publication point contains
  - the certificates and objects signed by that CA
  - a manifest listing everything that should appear
- Anticipated mode of use is: download everything periodically

# RPKI Uses

- Certificates/ROAs can be used to:
  - Validate customer routing requests
  - Validate address holder in problem resolution
  - Construct route filters
  - Verify origin of routing table entries
- None of this requires crypto in the routers
- All data transfer can be out-of-band
  - Potential future definition of in-band transfer for emergencies

# RPKI Architecture Roles

- **Service Provider (ISP)**
  - Receives allocated addresses and a CA certificate
  - Creates certificates when sub-allocating addresses
    - **IF** it wants customer to be able to sign its own ROAs
  - Signs ROAs for its own addresses
  - Maintains a CA repository
  - Retrieves contents of other CA repositories
- **Multi-homed End User**
  - May receive direct allocation/ CA certificate from RIR
  - Signs ROAs for its addresses for its providers

# RPKI Status

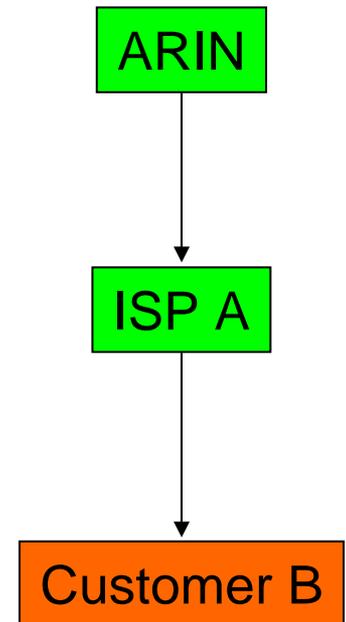
- RPKI data format specifications mature
- Remaining questions
  - Incremental deployment
  - Use in filter lists
  - Trust Anchors
  - 4-byte AS numbers

# RPKI Issue -- Incremental Deployment

- How to interpret absence of a ROA?
  - In full deployment, a BGP route with no matching ROA is invalid.
  - In partial deployment, a BGP route with no matching ROA **might** be valid.
- Use RPKI data to influence, not control, the BGP decision

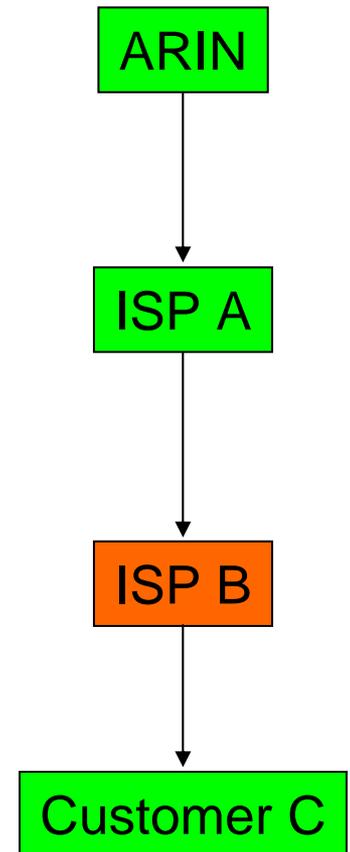
# RPKI Issue – Incremental Deployment

- Suppose ISP A participates in the RPKI, but customer B does not
  - Will ISP A create a CA certificate for clueless customer B?
  - Will ISP A sign ROAs for multi-homed customer B so B's routes will be believed?



# RPKI Issue – Incremental Deployment

- Suppose ISP B does not participate in the RPKI, but customer C wants to
- If ISP A is willing, it can create certificates for C
  - But it has no business relationship with C



# RPKI Usage – Incremental Deployment with Filter Lists

- Current best practice: create BGP Update filter lists from routing registry data
- Idea: translate ROAs to routing registry format
  - Benefit: reuse existing tools and practice
  - Caution: if no previous routing registry entries, could end up denying routes that were formerly accepted

# RPKI Open Issue – Trust Anchors

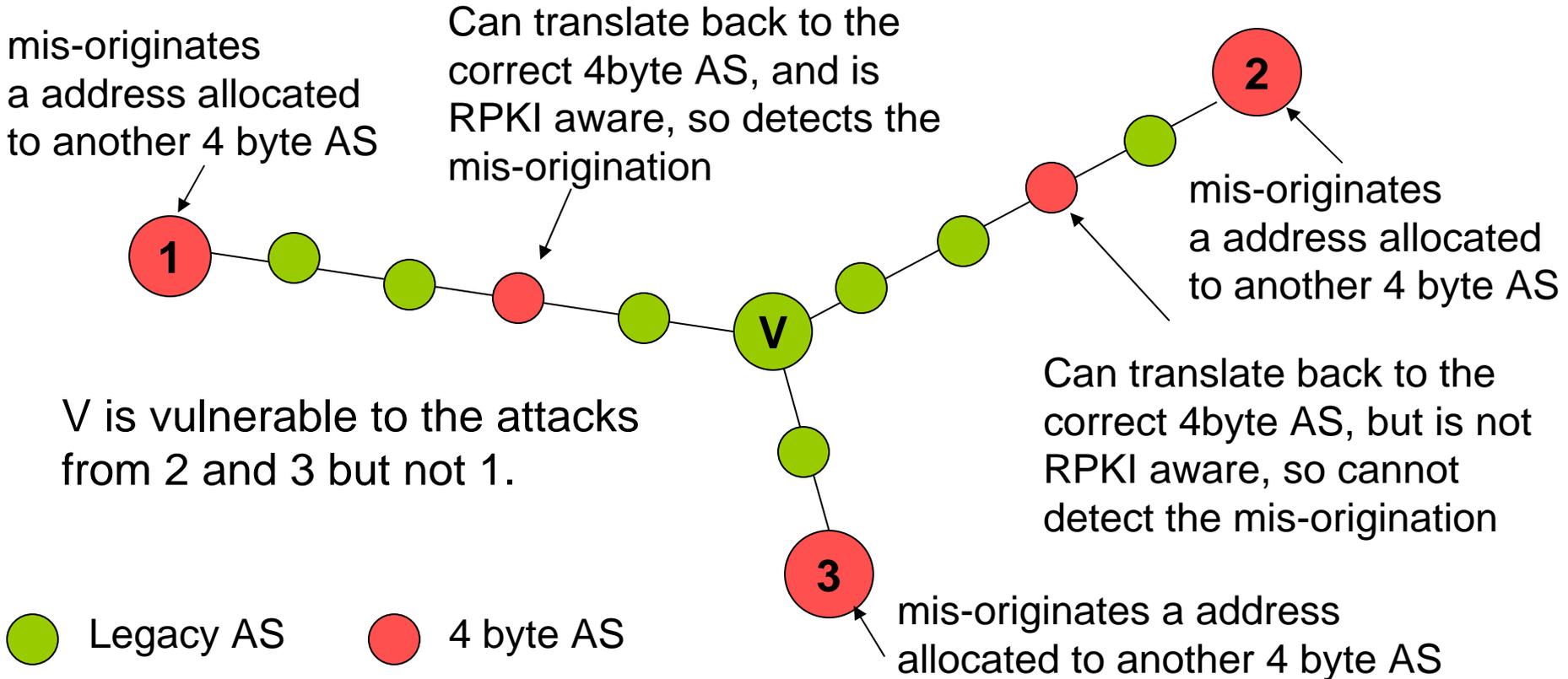
- Natural top of the RPKI tree is the top of the allocation tree – IANA
  - Trust anchor is easy – IANA is root for all addresses
- Suppose IANA is unwilling or unable to perform that function
  - Multiple trust anchors might then arise (one per RIR?)
  - Complex for operators to configure



# RPKI Open Issue – Four Byte AS Numbers

- Introduced in May 2007, not widely deployed
- Between a 4-byte AS and a legacy AS, any 4-byte AS in the AS\_PATH is translated into AS 23456
- A legacy AS sees 23456 as the origin of all addresses originated by any 4-byte AS

# RPKI Open Issue – Four Byte AS Numbers



***V's vulnerability to mis-origination by 4 byte ASs depends on its position in the topology wrt 4 byte ASs and RPKI use.***

# Summary

- Routing security is a decades old problem
- Solid progress is being made in the IETF standards
- Work on deployment issues is now needed
- Initial and partial deployment is critical
- Ease of use for operators is key