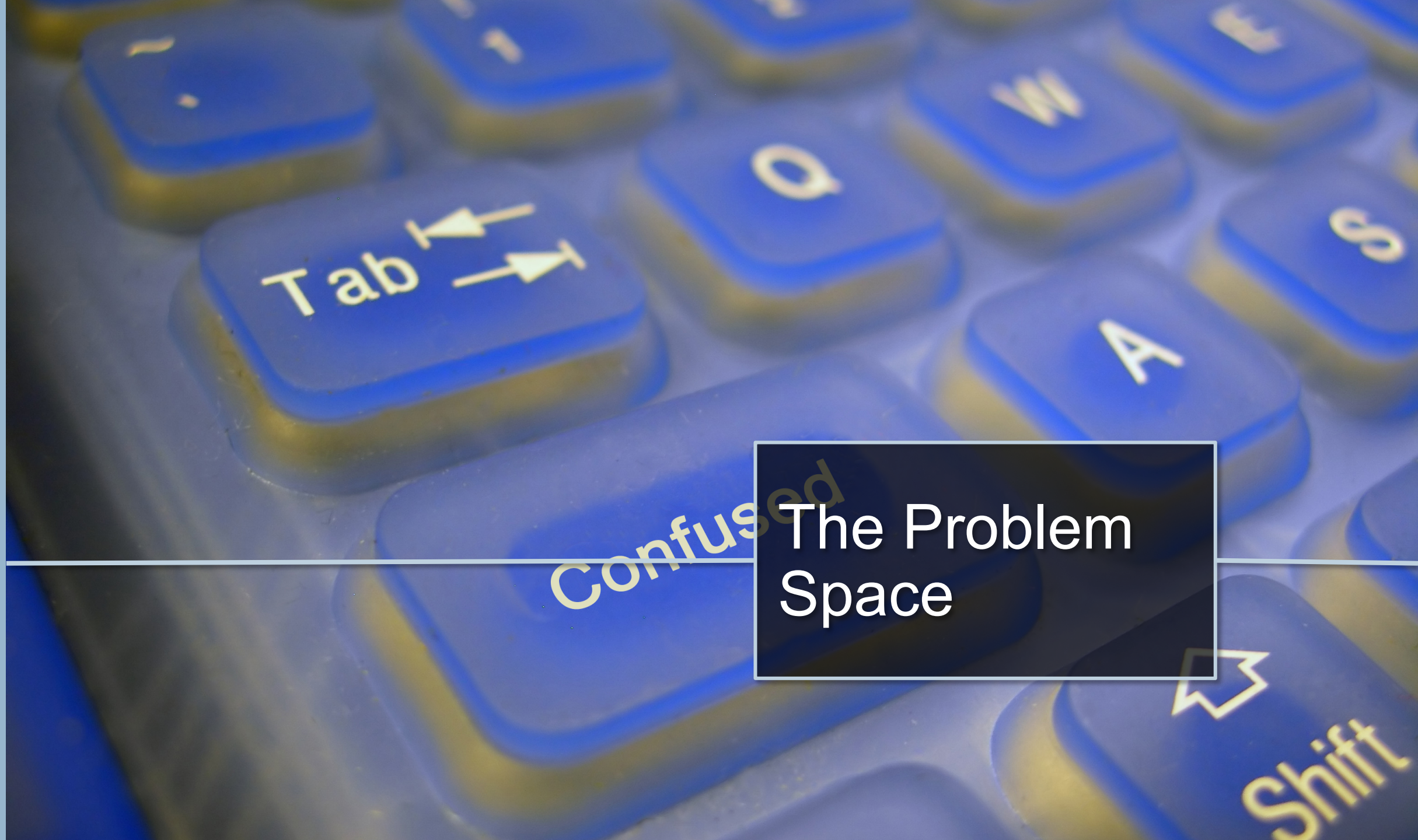
# BGP Security

Where we are, what we're trying to do next

*Russ White*
*russ@linkedin.com*
*Rule11.us*

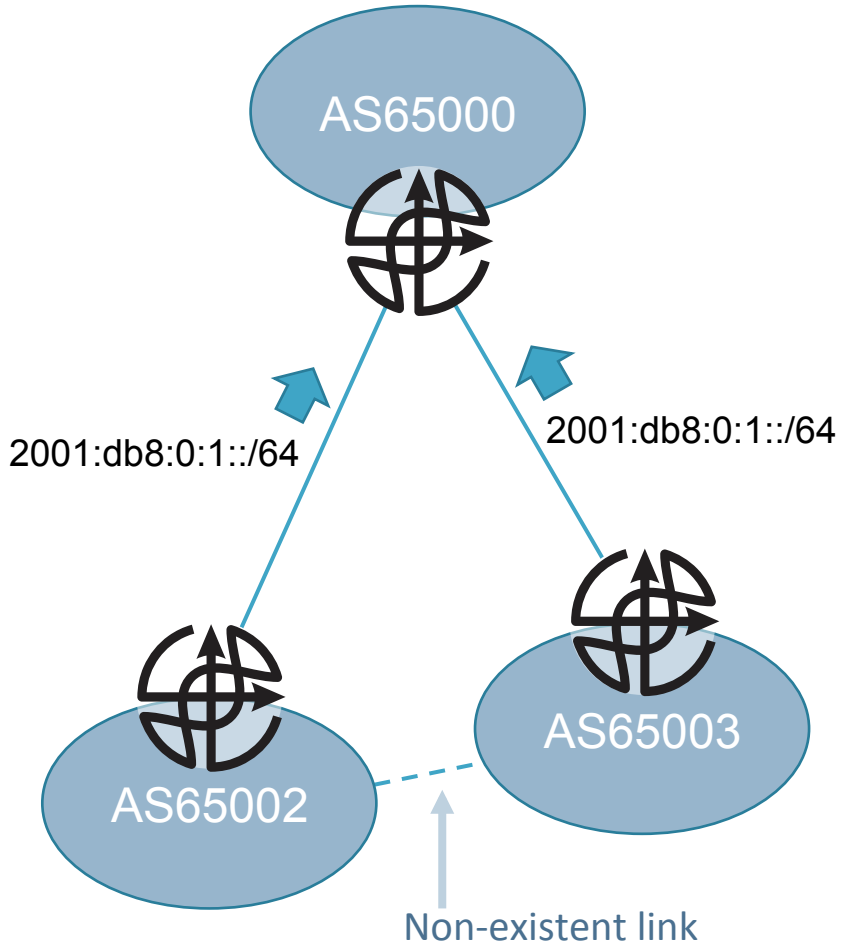
LinkedIn




# The Problem Space

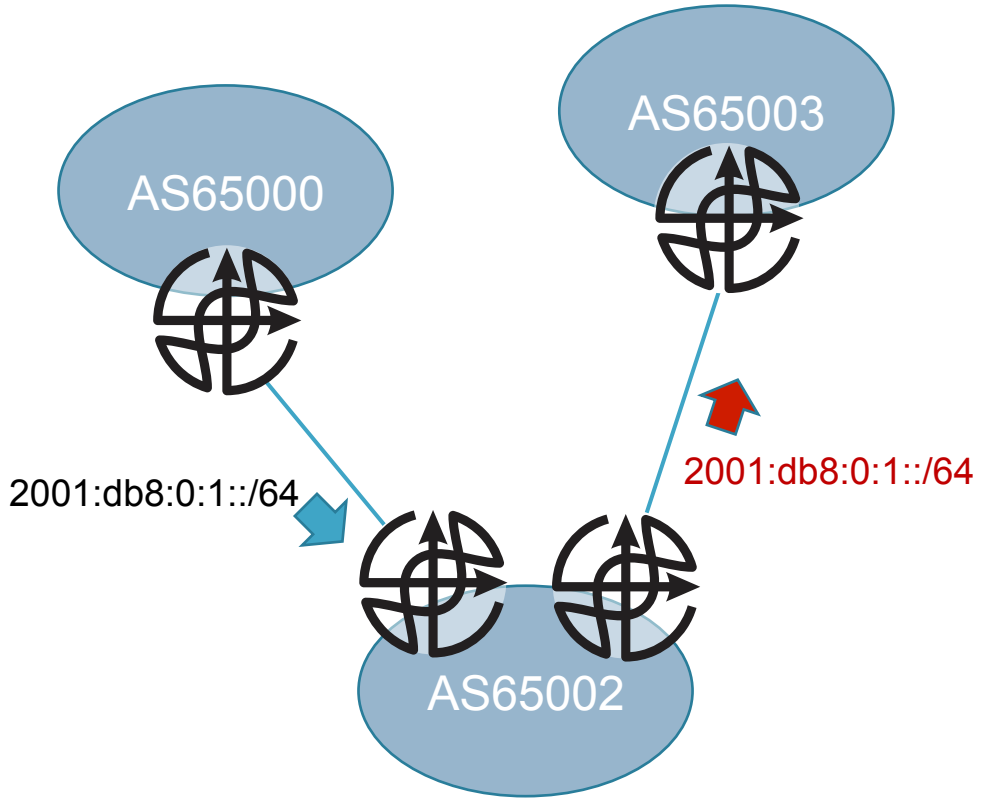
# Origin & Path Validation

- Who really owns 2001:db8:0:1::/64?
  - How can hijacking or spoofing attacks be resolved?
- What if we had some way for AS65000 to *know* AS65002 is the correct originator?
  - AS65003 can simply advertise 2001:db8:0:1::/64 with the AS Path [65002,65003]
  - To resolve this, *path validation* of some sort is needed



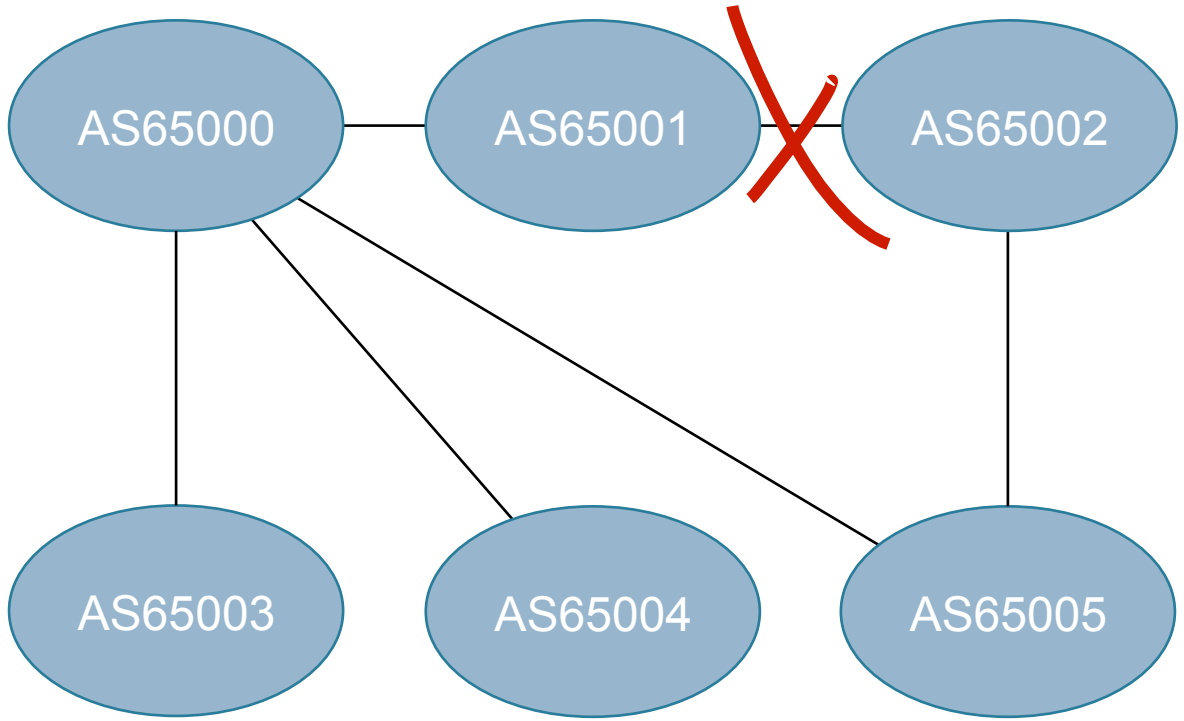
# Valley Free Routing

- AS65002 is a customer of AS65000 and 65003
- AS65000 advertises 2001:db8:0:1::/64 to AS65002
- AS65002 is not a transit AS, so it should not advertise 2001:db8:0:1::/64 towards AS65003
- AS65000 needs some way to signal AS65003 that AS65002 is not a transit, so it can reject this advertisement



# Controlling Information Distribution

- AS65000 doesn't want to advertise it's connection to AS65003 unless the routes are being advertised
  - Backup routes, etc.
- AS65000 only wants its connection to AS65004 advertised to its peers, and not to their peers
  - Regional routing information, partnering relationships, etc.



# Operational Requirements

- No single point of failure
- Don’t replace the edge
- Don’t tell operators how to run their networks
- Don’t slow down convergence
- Be quiet

# Notes

- No single point of failure
  - No single trust anchor
  - No single copy of a database
  - No single source of information
- Don’t replace the edge
  - Edge routers can’t do encryption
- Don’t tell operators how to run their network
  - Provide information on which to form policy, rather than policy
- Don’t slow down
  - Should converge in near to BGP time
  - DDoS protection services and the like are a consideration
- Be quiet
  - Don’t tell anyone anything that can’t already be inferred from publicly available information
  - Allow filtering of information to protect relationships

# Current Solutions

# RPKI Analysis

*Positive*

- Validation/data is out of band
- Very low/no information leakage
- Incremental deployment
- No edge replacement
- Leaves BGP alone

*Negative*

- Does not protect against
  - One-off attacks
  - Any sort of “man in the middle”
- Difficult to justify for transit operators
- Concerns around business control over operators by RIRs

# BGPSEC Analysis

*Positive*

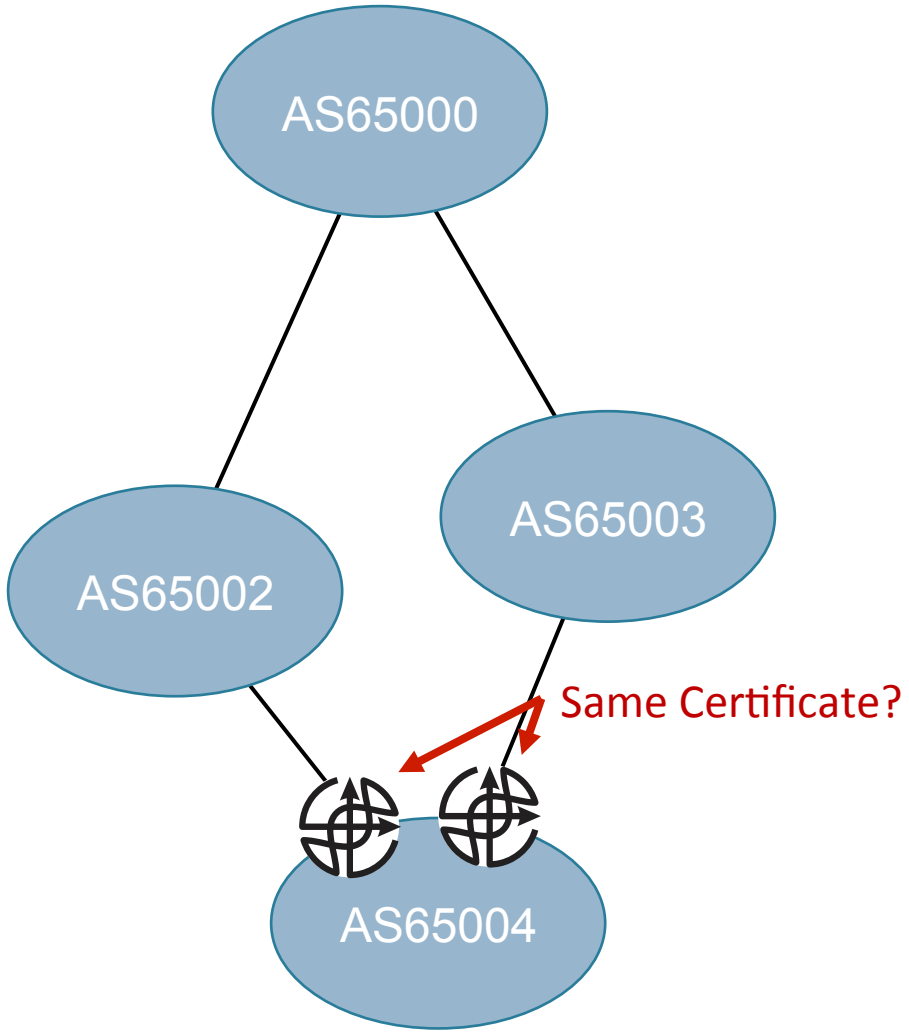
- 100% positive attribution of AS Path
- Validation advertised in band
  - Validation follows routing information
  - Validation converges at the speed of the control plane
- Defeats specific classes of man in the middle attacks
- Protects against one off attacks

*Negative*

- Performance
  - 15x table size
  - Precludes packing and other optimizations
  - Signature processed per AS hop
- Replay attacks are possible
- Attacks against time can impact entire routing system

# BGPSEC Analysis

- Every eBGP speaker uses the same certificate == security hole
- Resolved by every eBGP speaker using a different certificate
- This exposes peering information for each eBGP speaker



# DAG Overlay Analysis

*Positive*

- Validation of AS Path
- Validation advertised in overlay
- Defeats specific classes of man in the middle attacks
- Protects against one off attacks
- Uses BGP
  - Well known tools and analysis

*Negative*

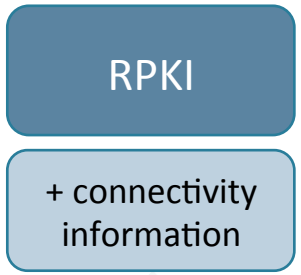
- Uses BGP
  - Requires modification to BGP
- Doesn’t provide the strongest level of path protection
- Providers cannot advertise customers

# Nothing we have today will Deploy 100%

- Some won’t deploy at all
- What we need is
  - Something to make multiple systems work together
  - Something to get to “good enough”
- Hence—a modest proposal…

# A (Modest) Proposal

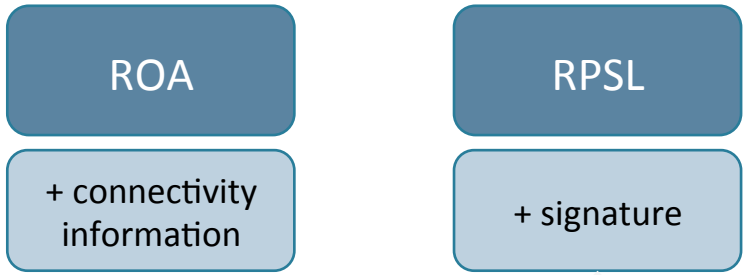
- RPKI
- Authoritative root
- Slow'ish convergence




- Find some way to add connectivity information to the existing RPKI
- This would be optional information, but helpful in validating the AS Path

- RPKI
- Authoritative root
- Slow'ish convergence

- RIR/Public IRR
- Authoritative maintenance
- Fast'ish convergence

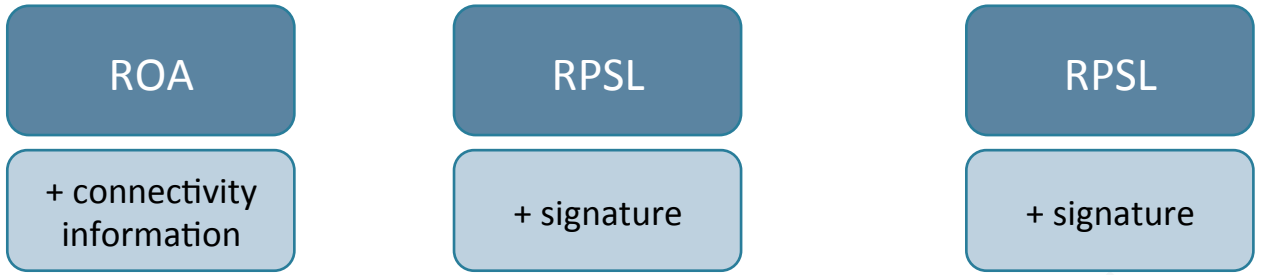



- IRR maintained by RIR's and "public entities" (such as a foundation/trust/ company set up for this purpose)
- Need to determine how to sign/what to sign with/etc.
- Origin information provided by party inserting data in the IRR
- Connectivity and policy information optionally provided by party inserting data in the IRR

- RPKI
- Authoritative root
- Slow'ish convergence

- RIR/Public IRR
- Authoritative maintenance
- Fast'ish convergence

- Private IRR
- Provider maintenance
- Fast'ish convergence




- IRR maintained by tier 1 and other providers
- Need to determine how to sign/what to sign with/etc.
- Origin information provided by party inserting data in the IRR, validated by the providers
- *Assuming this information would mostly be provider's customers*
- Connectivity and policy information optionally provided

- RPKI
- Authoritative root
- Slow'ish convergence

ROA

+ connectivity information

- RIR/Public IRRs
- Authoritative maintenance
- Fast'ish convergence

RPSL

+ signature

- Private IRRs
- Provider maintenance
- Fast'ish convergence

RPSL

+ signature

- Table Analysis
- Open source tooling
- Locally maintained/processed

Table Info

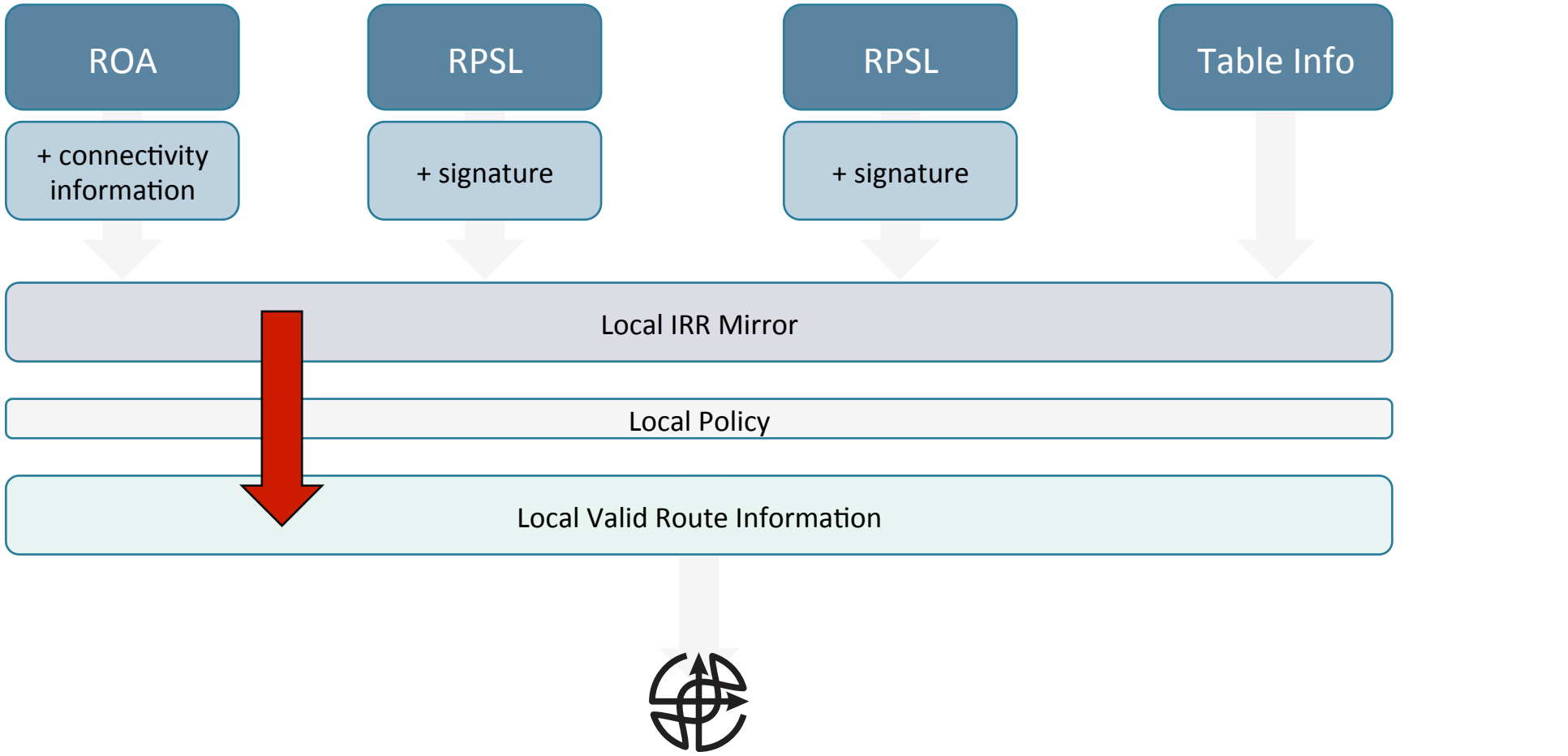
- Mines route views and other sources
  - Stable origin information
  - Stable AS connectivity information
- Feeds into a local system
- Open source tool set

- RPKI
- Authoritative root
- Slow'ish convergence

- RIR/Public IRRs
- Authoritative maintenance
- Fast'ish convergence

- Private IRRs
- Provider maintenance
- Fast'ish convergence

- Route Views Analysis
- Open source tooling
- Locally maintained/processed



# Analysis

*Positive*

- Validation of origin and path
  - Validation level depends on amount of information available
- Validation information carried outside the routing system
- No single point of failure or control
- Local policy shaped from multiple sources

*Negative*

- Lots of moving parts
  - But any particular AS can use the tool set they trust
- No single point of control
  - Receiver focused trust model, rather than third party/ authoritative focused trust model
- Current IRR model is “broken”
  - Offset by RPKI + private IRRs
  - Public IRRs still need to be cleaned up

# Problems to Resolve

- RPSL needs some way to restrict propagation
  - Communities or the like to filter what is mirrored where
- Signing semantics/key sources for RPSL objects
- Need to be able to access all sources of information from a single API
  - The IRR interface is probably the natural candidate
  - IRR to RPKI API
  - Route Views information to IRR system/API
- Local policy store
  - Open source/commercial tools
  - Consistent interface across all routers to express policy

# Questions?

*Russ White*
*russ@linkedin.com*
*Rule11.us*

LinkedIn