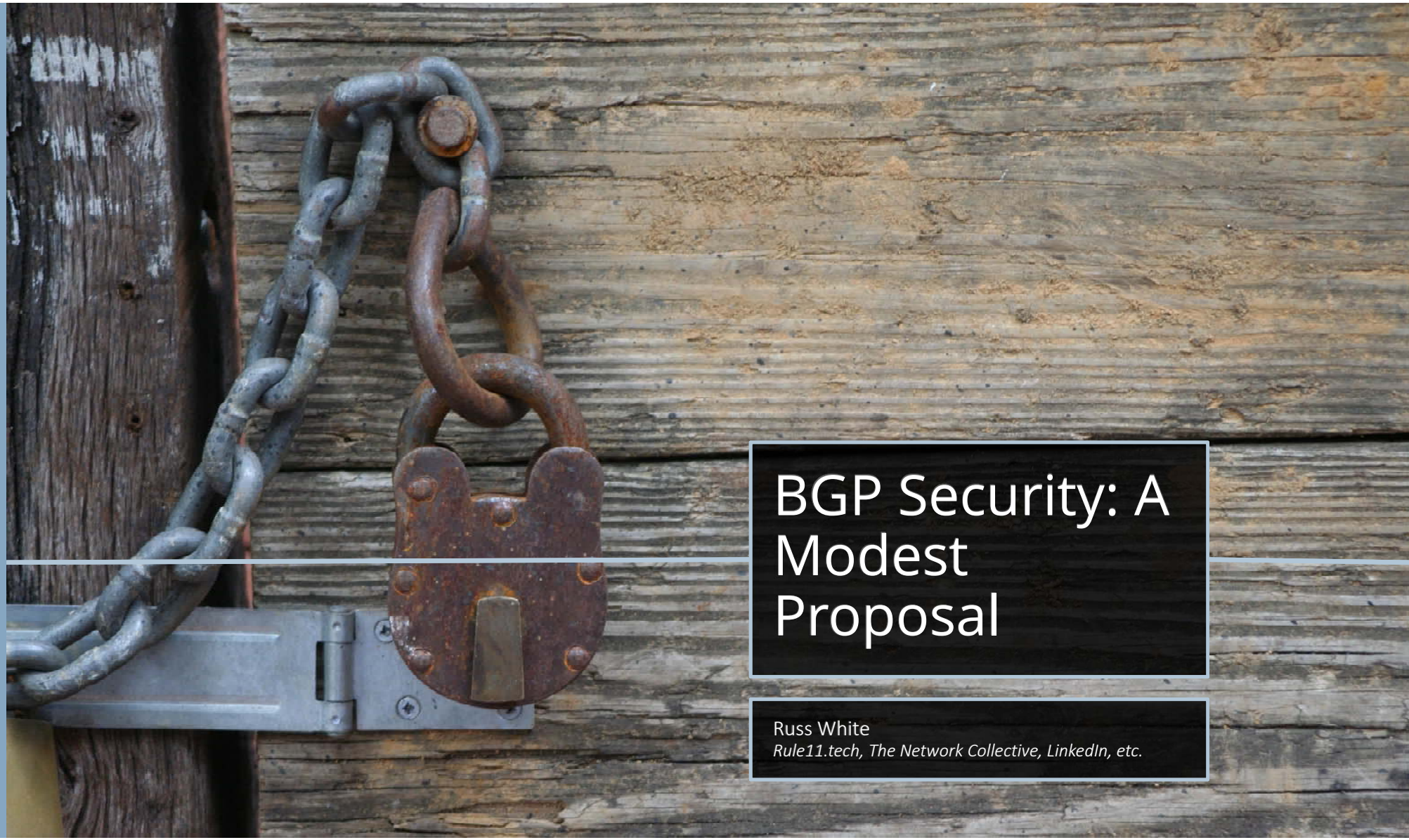


BGP Security: A Modest Proposal

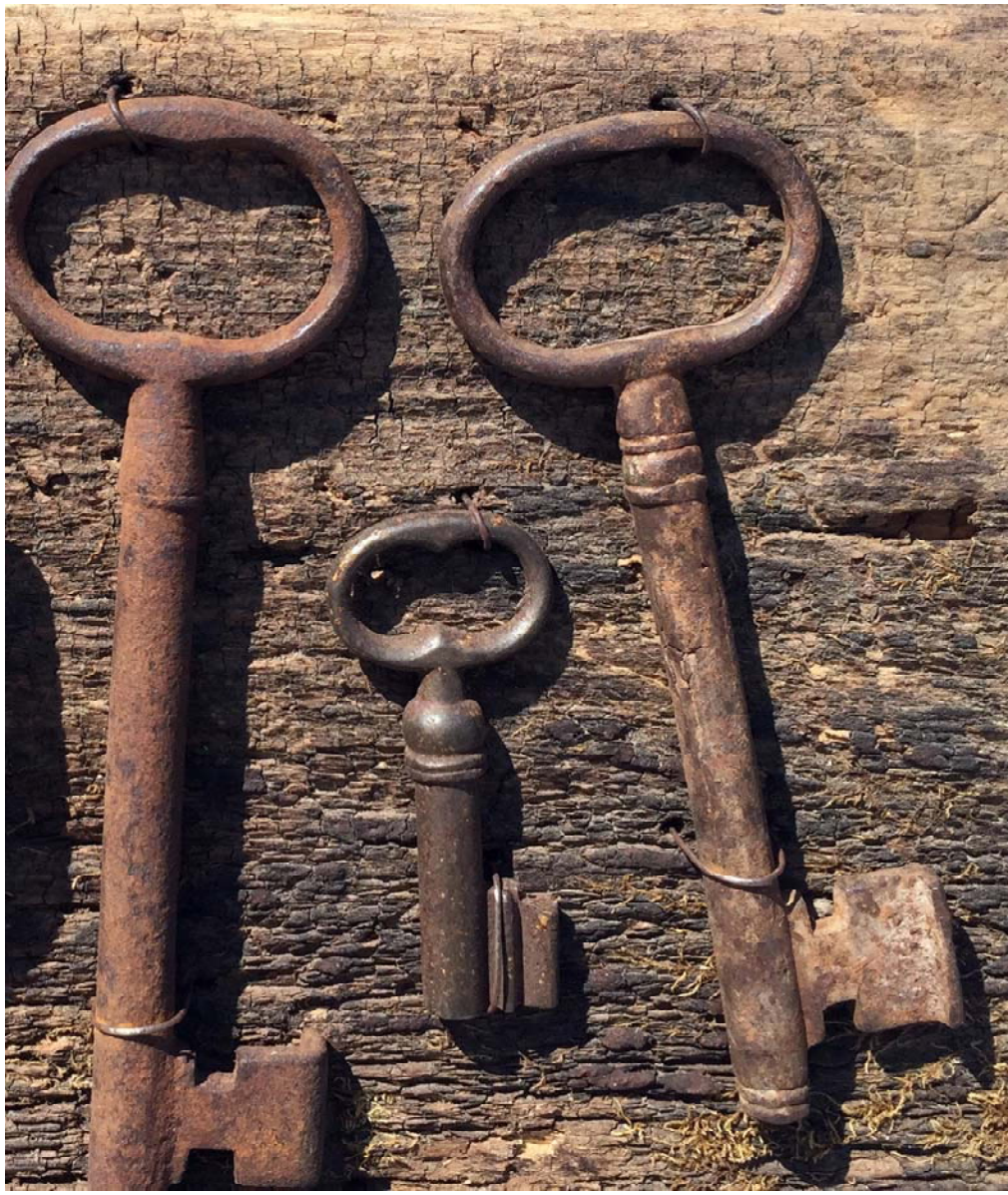
Russ White
Rule11.tech, The Network Collective, LinkedIn, etc.

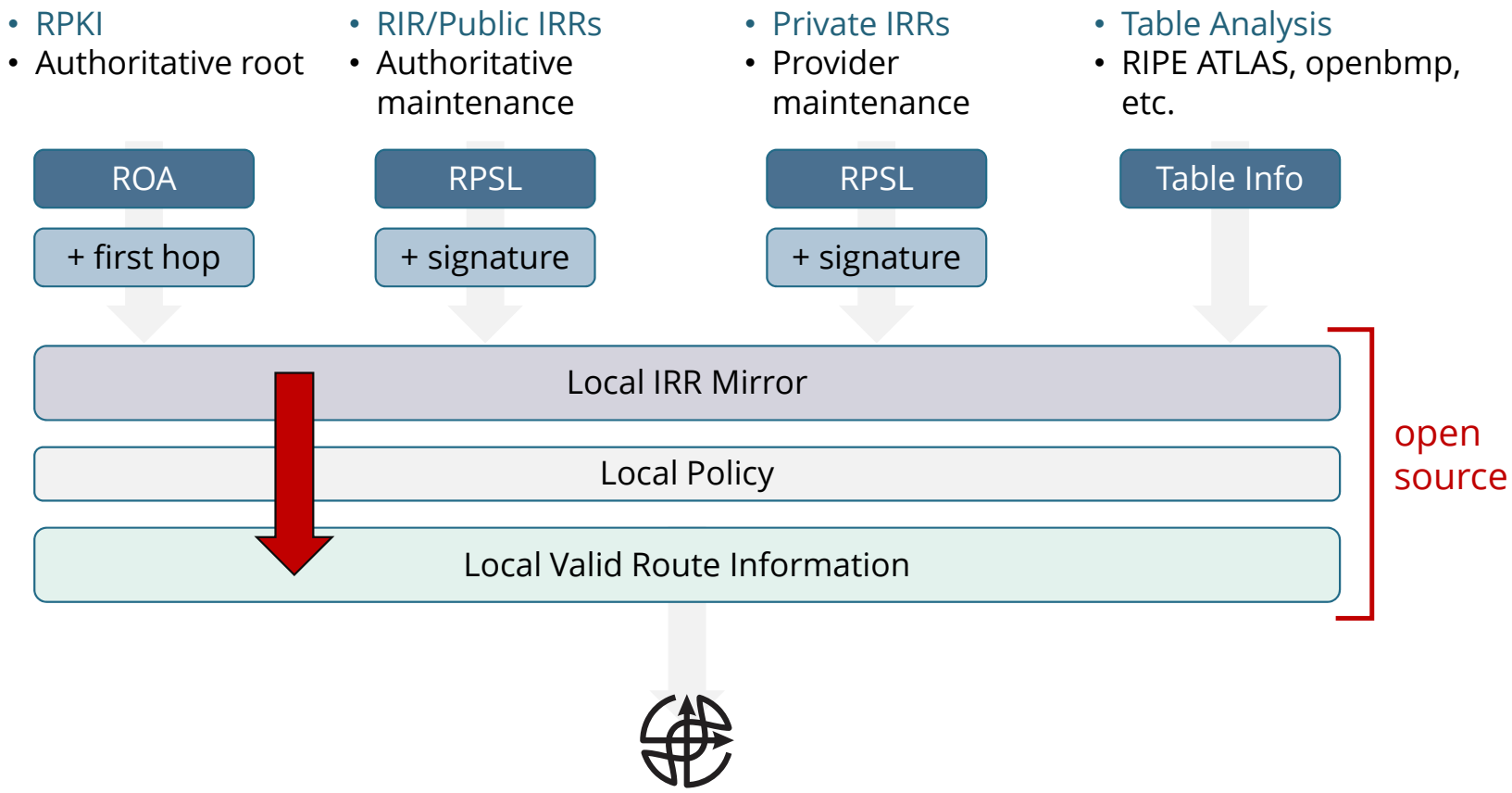
Operational Requirements

- 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

Reality

- RPKI
  - General worries about scale
  - May suffer from information rot
  - Probably will not be *universally* deployed
  - Does not solve path validation
- Graph Overlays
  - Killed by the community
- BGPSEC
  - Undeployable
  - Not (really) quiet
  - Doesn’t solve the problem at hand
  - Too much pain for too little gain
- Is there a solution here?
  - Can we solve 80% of the problem?




• RPKI
• Authoritative root
• RIR/Public IRRs
• Authoritative maintenance
• Private IRRs
• Provider maintenance
• Table Analysis
• RIPE ATLAS, openbmp, etc.
ROA
+ first hop
RPSL
+ signature
RPSL
+ signature
Table Info
Local IRR Mirror
Local Policy
Local Valid Route Information
open source

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 control
  - Receiver focused trust model
- No single point of failure
- 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