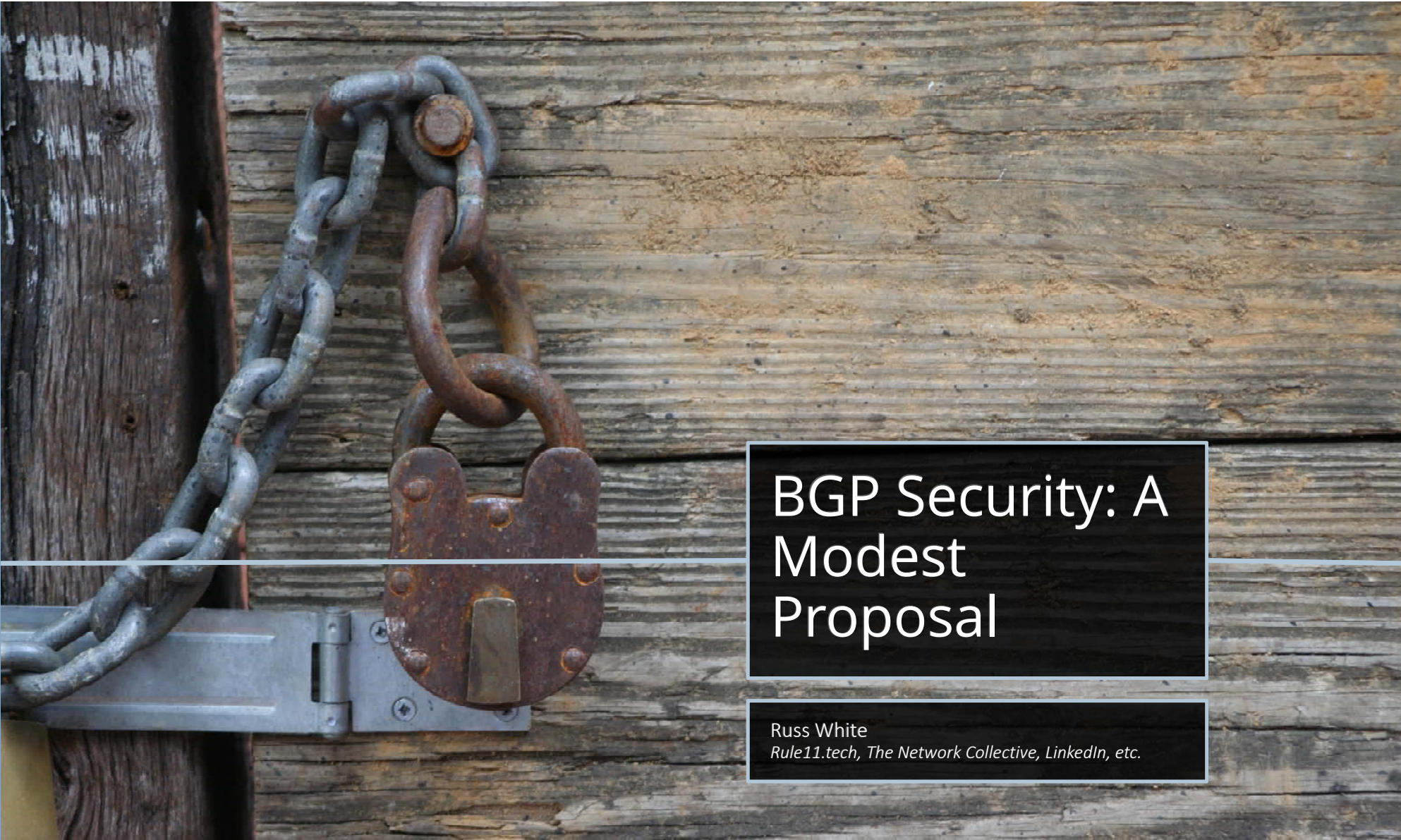


A photograph of a heavy metal padlock and chain on a wooden door. The padlock is dark, rusted metal with a silver-colored metal plate on the front. It is attached to a thick metal chain. The chain is made of large, dark metal links. The background is a wooden door with horizontal planks. The lighting is natural, highlighting the textures of the wood and metal.

BGP Security: A Modest Proposal

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

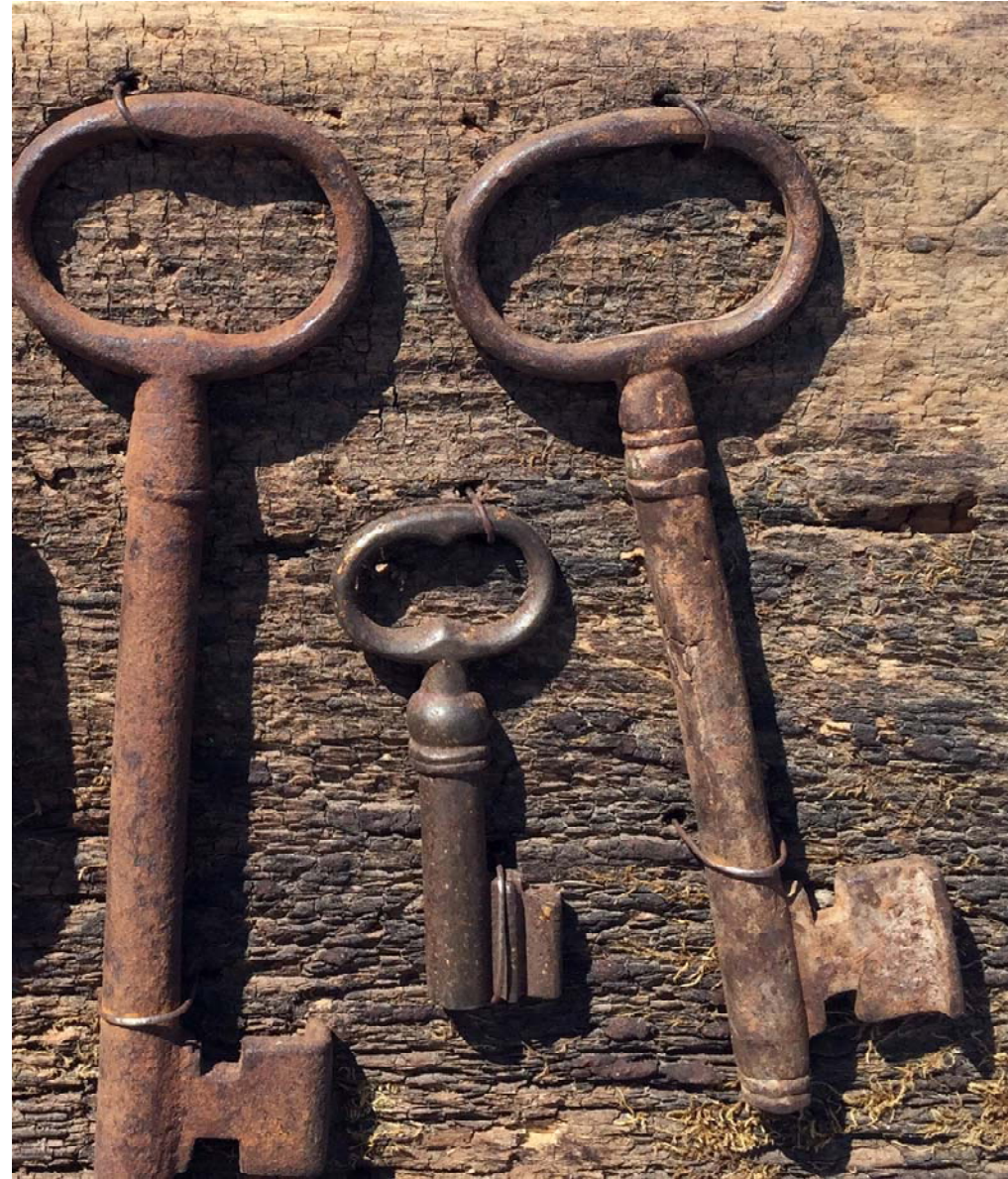
Operational Requirements

- 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

ROA

+ first hop

- RIR/Public IRRs
- Authoritative maintenance

RPSL

+ signature

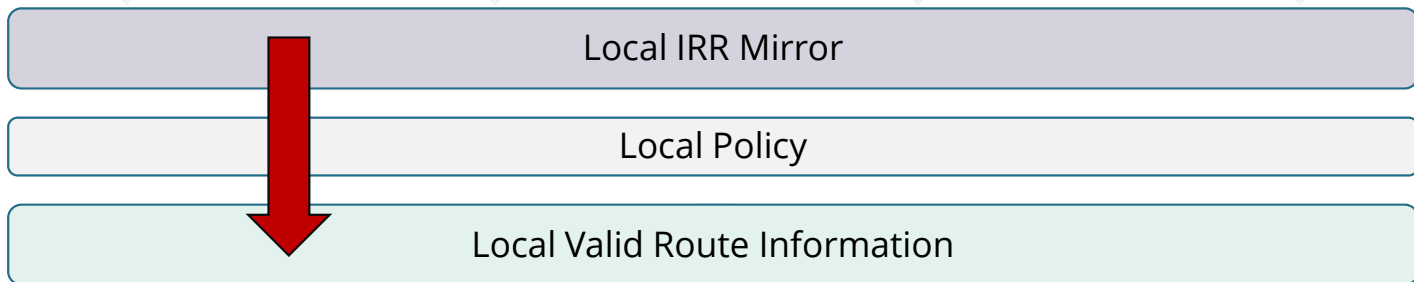
- Private IRRs
- Provider maintenance

RPSL

+ signature

- Table Analysis
- RIPE ATLAS, openbmp, etc.

Table Info



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