Routing and Forwarding Integrity: Defenses to Common Challenges

John Kristoff
jtk@cymru.com
Systems and policy

• Sane and secure defaults
• Automated configuration management, connected to
• Automated monitoring and measurement capabilities
• Policy, type and consistency checking
• Control plane isolation and protection
• Authentication and cryptography
• Neighbor collaboration and cooperation
Goodput

- Peer/IX transit/forwarding theft mitigation
- Minimizing CPU punts and packet processing
- BCP 38/84, uRPF, SAVI
  - WARNING: all spoofing-related discussion is tabled
- RTBH, flow-spec, rate limiting, filters
- Queuing and active traffic management (RED, CoS)
- Darknets, quarantines and sinkholes
- Redirects (e.g. fabricated GFW DNS answers)
Route Integrity

- RPKI-Based Origin Validation / BGPsec
- IRR-Based ACLs
- Route history monitoring and alerting
- Route flap dampening
- Prefix allocation boundary filtering
- Prefix announcement count limits
- “Golden Routes” protection
Thank you

- John Kristoff
- <jtk@cymru.com> - https://www.cymru.com/jtk/