S-BGP:
A Very Quick Overview

Dr. Stephen Kent

Chief Scientist - Information Security

BBN TECHNOLOGIES

BGP Security Goals

- Need to have realistic goals for BGP security:
  - We can’t make any AS do anything!
  - Traffic flow is dictated by forwarding tables, and ensuring that these tables match routing info and local policy is a LOCAL matter
  - But, if we don’t believe that routing significantly affects forwarding, let’s not bother trying to secure BGP
  - The good news: it takes two to ~~tango~~ forward
  - A reasonable goal is to enable each AS to determine if the advertisements it receives are authentic, so that an AS can make routing decisions based on authentic data, plus local policy inputs
  - In general, an AS cannot use BGP to impose its local policy on other ASes, at least not at a distance, although some do try …

BGP Security Solution Criteria

- Security architectures for BGP should not rely on “trust” among ISPs
  - On a global scale, some ISPs will never be trusted
  - People, even trusted people, make mistakes, and trusted people do “go bad”
  - Transitive trust in people or organizations allows errors and attacks to propagate (the domino effect)
- Elements of security solutions should exhibit the same dynamics as the aspects of BGP they protect
- The memory & processing requirements of a solution should scale consistent with BGP scaling
- Management controls must not be too complex!

A Basic BGP Security Requirement

- **For every UPDATE it receives, a BGP router should be able to verify that the holder of each prefix authorized the first AS to advertise the prefix and that each subsequent AS in the path has been authorized by the preceding AS to advertise a route to the prefix**

  This is oversimplified, e.g., it does not explicitly address some forms of aggregation, but the principle is sound

- This requirement, if achieved, allows a BGP router to detect and reject unauthorized routes, irrespective of what sort of attack resulted in the bad routes

Derived BGP Security Requirements

- Verify address space holder assertions
- Verify Autonomous System (AS) assignments
- Bind a BGP router to the AS(es) it represents
- Router verification of UPDATEs
- Route withdrawal authorization
- Integrity and authenticity of all BGP traffic on the wire (as a counter to active wiretapping attacks that could result in DoS)
- Timeliness of UPDATE propagation*

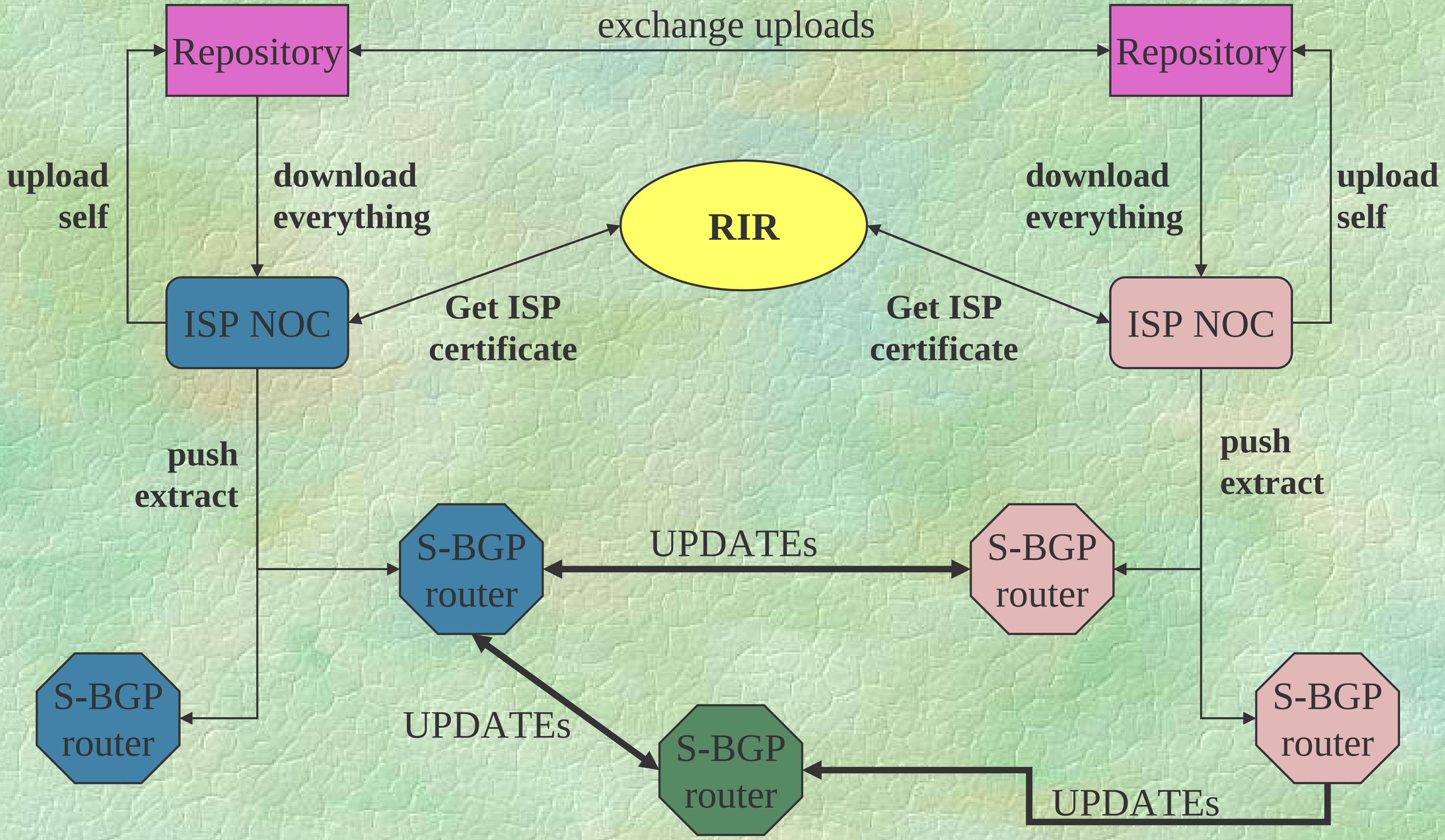
Secure BGP (S-BGP)

- S-BGP is one architectural solution to the BGP security problems described earlier
- S-BGP represents an extension of BGP
  - It uses a standard BGP extension facility to carry additional data about paths in UPDATE messages
  - It adds an additional set of checks to the BGP route selection algorithm
- S-BGP avoids the pitfalls of transitive trust that are common in today’s routing infrastructure
- S-BGP mechanisms exhibit the same dynamics as BGP, and they scale commensurately with BGP

S-BGP Design Overview

- S-BGP makes use of:
  - IPsec to secure point-to-point communication of BGP traffic
  - A PKI to provide an authorization framework for address space holders and AS number assignees
  - Attestations (digitally-signed data) to represent
    - Authorization for route origination
    - Authorization for route propagation
- S-BGP is incrementally deployable in the public Internet, and within a single AS
- Full deployment would require more memory than most routers can support, plus use of hardware crypto
  - Moore’s law can address this over time
  - Recent work at Dartmouth has lowered S-BGP memory requirements by ~60%, and significantly reduced convergence time for S-BGP (in simulations)

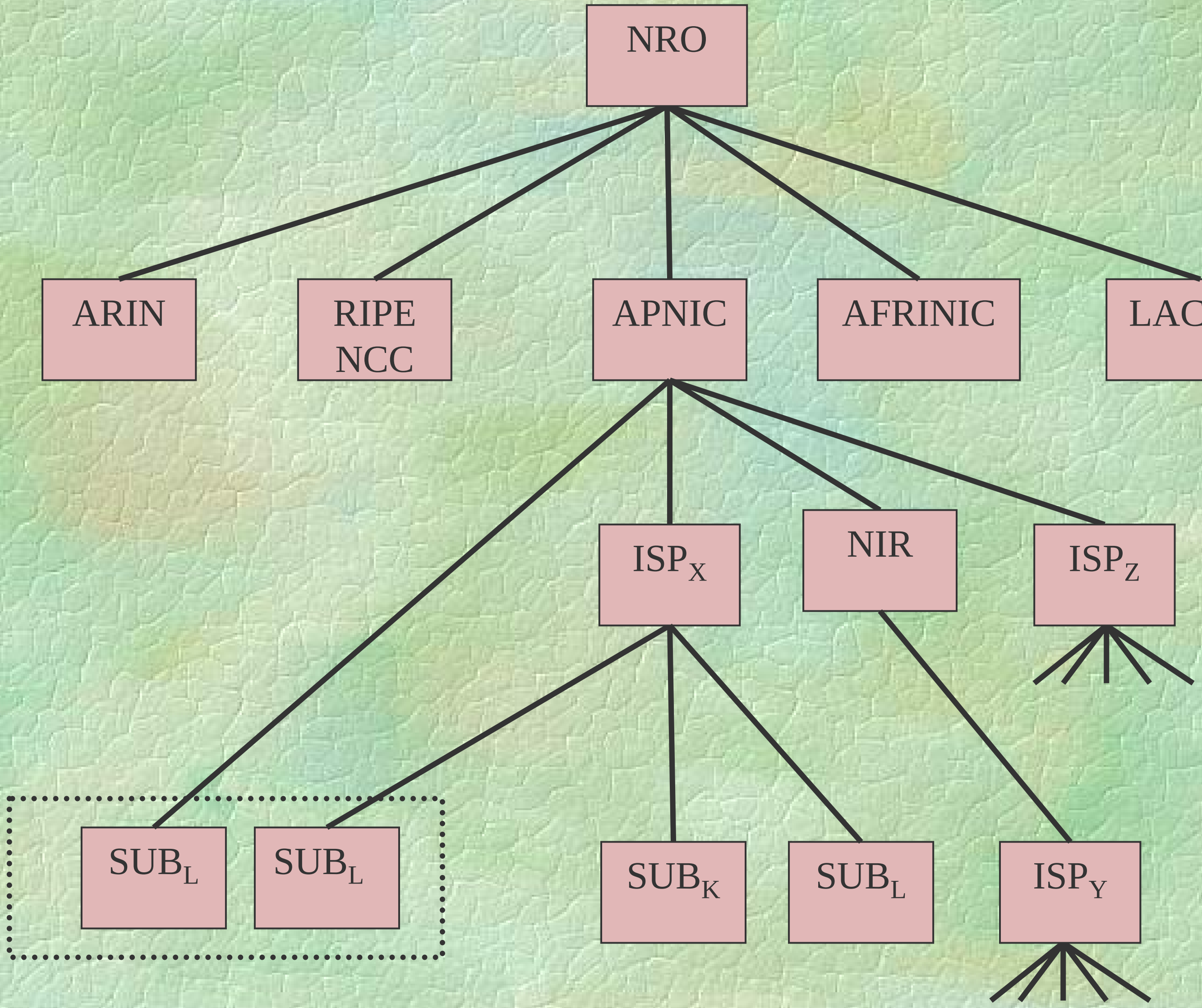
S-BGP System Interaction Example



A First Step

- Most of the BGP security proposals rely on some infrastructure prerequisites
  - Which organizational entities hold which prefixes and AS numbers?
  - Which ASes are authorized to originate routes for which prefixes?
- Both of these bindings are fairly static, and every ISP needs to know all of the data, suggesting out of band distribution via repositories
- A PKI that parallels address space and AS number allocation can securely represent these bindings
- Note that this does not imply a need for routers to process certificates, CRLs, etc.
- The PKI could be used to improve route filter generation prior to adoption of any scheme that calls for router enhancements

IP Address Space PKI



Hierarchic vs. Mesh PKIs

- If one constructs a hierarchic PKI, users of the PKI can choose (locally) to interpret it either as hierarchic or as a mesh PKI (“web of trust”)
- To interpret a hierarchic PKI as a mesh PKI, a user (e.g., ISP) configures other users as trust anchors, instead of recognizing only the root
- Thus both hierarchic and mesh interpretations are compatible with a hierarchic PKI deployment
- But, if one deploys only a mesh PKI, then all users are forced to a mesh model, because of the lack of a root, certificate subordination controls, etc.

Summary

- We need
  - Agreement on what are the goals for BGP security
  - Security criteria that are consistent with the autonomous nature of BGP operation in the public Internet
  - Objective solution evaluation criteria
- Solution approaches based on “trust” are worrisome, prone to domino effect failures
- A reasonable first step is creation of a hierarchic infrastructure (PKI) that
  - Issues credentials to address prefix and AS number holders
  - Allows prefix holders to authorize ASes to originate routes for prefixes
  - Allows local interpretation of the PKI as a “web of trust”

Questions?