BGP Security

APNIC Open Policy Meeting
Routing SIG
23 February 2005
Kyoto, Japan

Russ Housley
housley@vigilsec.com

Outline

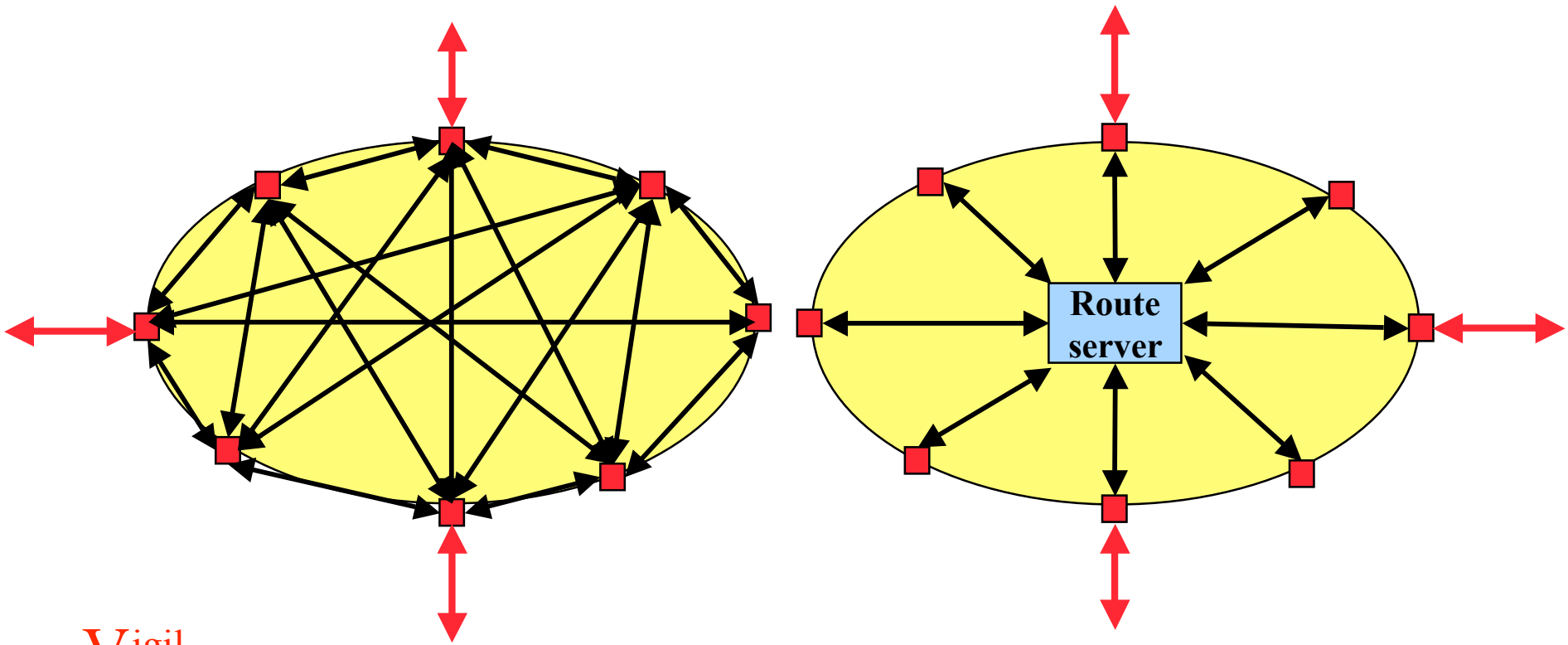
- Introduction
- BGP Security
- IETF Activities

The Problem

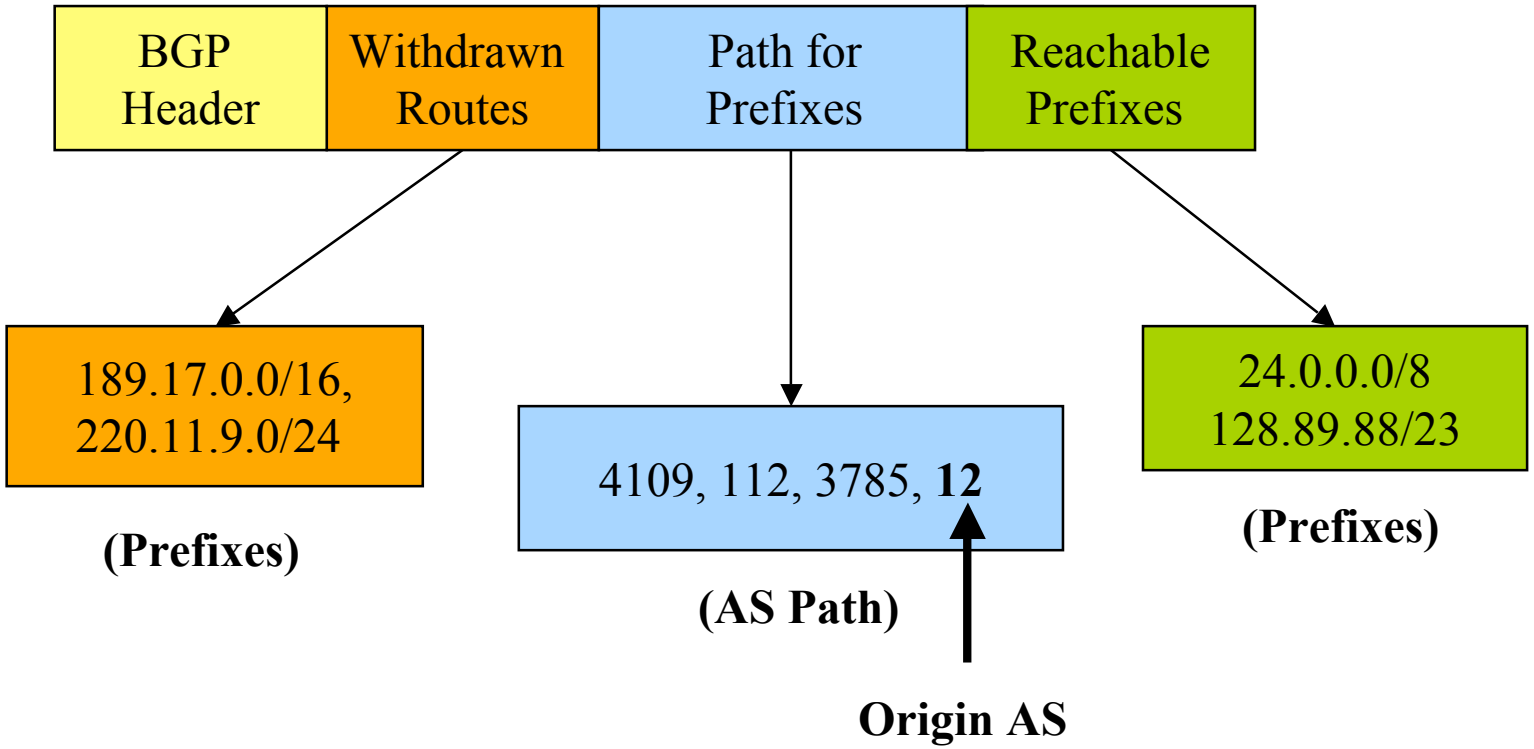
- BGP provides critical routing infrastructure for the Internet; BGP is the basis for all inter-ISP routing
- The current system is highly vulnerable to human errors, as well as a wide range of malicious attacks
- Configuration errors are commonplace
- BGP has been attacked; more attacks seem likely
- BGP needs a comprehensive security solution
- Security solutions will require buy-in from vendors, ISPs, and subscribers
- Deployment will probably to take many years

External vs. Internal use of BGP

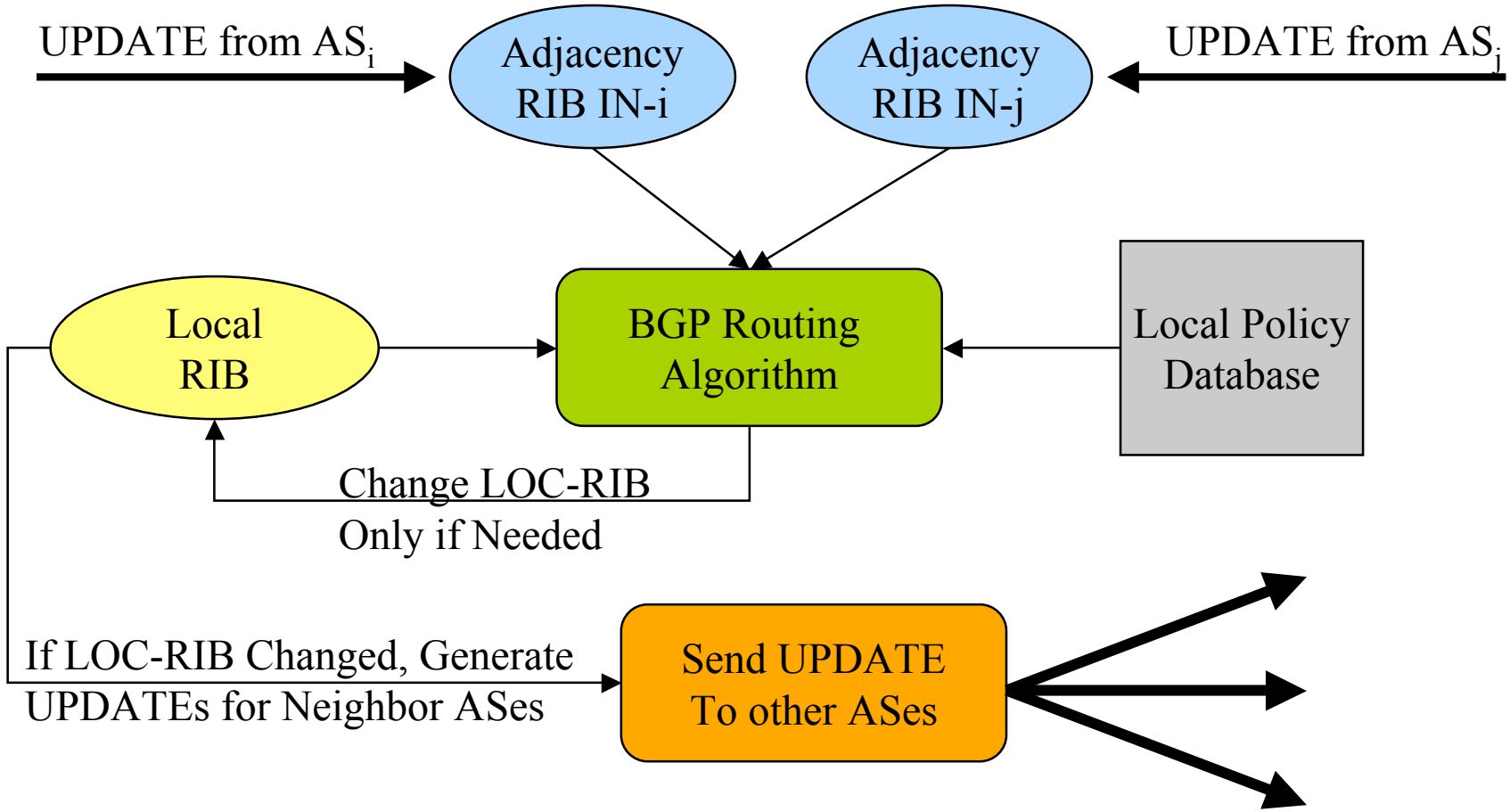
Routes acquired externally from other ASes via eBGP are propagated to other border routers in an AS using iBGP, either directly or via a route server.



A Simplified UPDATE Message



Processing an UPDATE



Assumption Underlying UPDATEs

- Each AS along the path is assumed to have been authorized by the preceding AS to advertise the prefixes contained in the UPDATE message
- The first AS in the path is assumed to have been authorized to advertise the prefixes by the "holder" of the prefixes
- A route may be withdrawn only by the neighbor AS that advertised it (ADJ-RIB-IN locality)
- **If <u>any</u> of these assumptions are violated, BGP becomes vulnerable to many forms of attack, with a variety of adverse consequences**

Some BGP Subtleties

- The “best” route is greatly influenced by local policies, which represent business arrangements between ISPs and internal ISP traffic engineering decisions
- An AS may report different routes to different neighbors because of local policies, making asymmetric routes common
- Not all connections between ASes are visible to the Internet at large, e.g., private peering links
- Withdrawal of a route for a prefix by one AS may not result in a neighbor withdrawing the route for that prefix, since the neighbor may have an alternative route available from another source

BGP Security

Vigil Security LLC

Adversary Goals for BGP Attacks

- Degrade service (locally or globally) by effecting a denial-of-service (DoS) attack against a router's BGP implementation
- Reroute subscriber traffic to subject that traffic to passive or active wiretapping
  - Examine subscriber traffic and pass it on to the destination
  - Modify subscriber traffic and pass it on to the destination
  - Delete selected subscriber traffic
  - Masquerade as subscribers by consuming traffic directed to them and responding on their behalf

BGP Security Problems

- The BGP architecture makes it highly vulnerable to human errors and malicious attacks
  - Against links between routers
  - Against routers
  - Against management stations that control routers
- Most BGP implementations are susceptible to various DoS attacks, which crash the router or severely degrade performance
- Many ISPs rely on local policy filters to protect against configuration errors and some attacks, but creating and maintaining these filters is difficult, time consuming, and error prone

Is BGP Under Attack?

- DARPA-sponsored research has discovered that configuration errors affect about 1% of all routing table entries at any time
- BGP attack tools have been developed and demonstrated at hacker conferences
- Attacks against ISP routers do occur, which permits BGP attacks to be launched from the compromised routers
- Spammers are mounting BGP attacks to use unassigned address space
- BGP-based attacks have been used by hackers as part of an effort to masquerade as root DNS servers

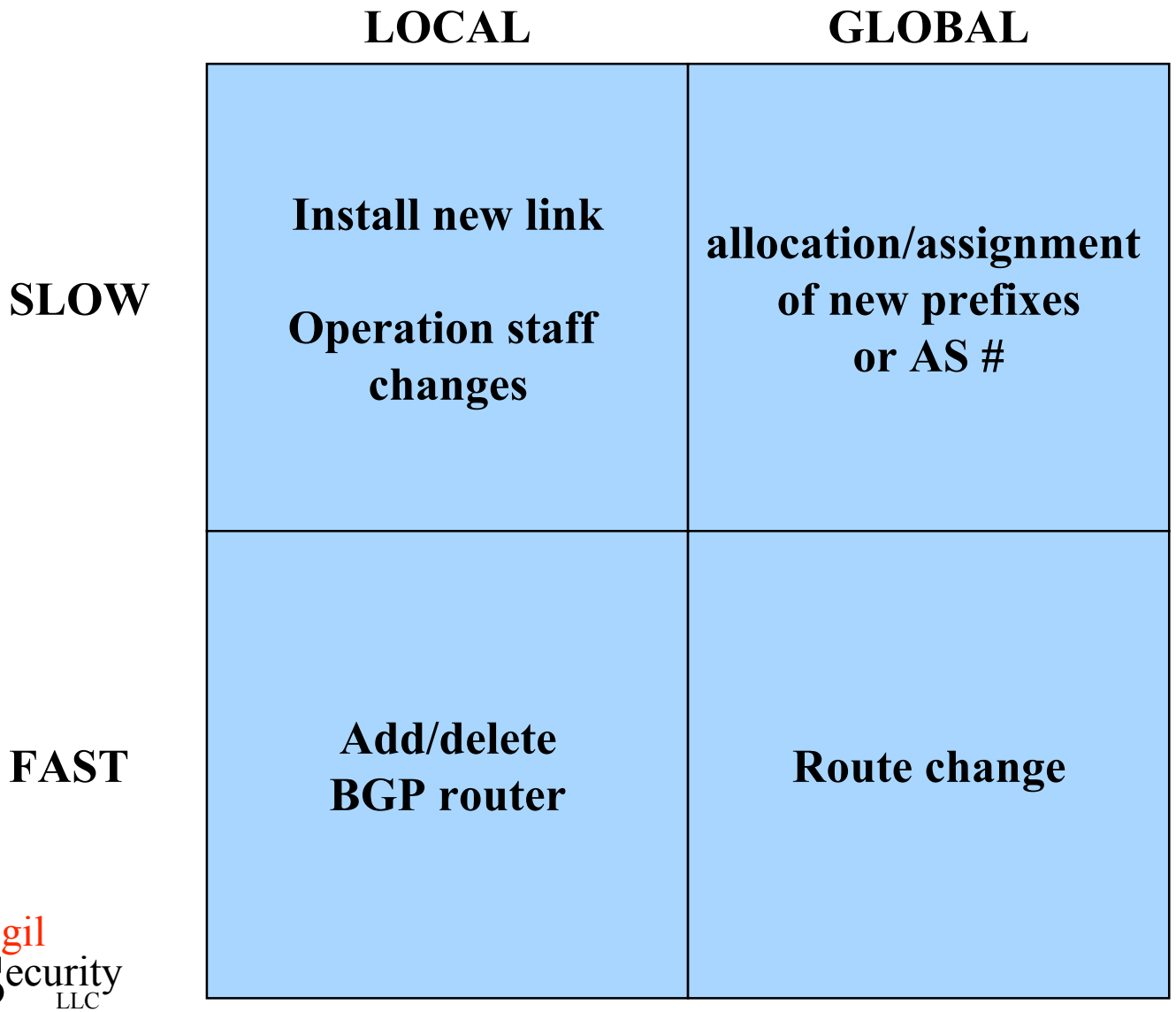
BGP Security Solution Requirements

- Security architectures for BGP should not rely on "trust" among ISPs or subscribers
  - On a global scale, some ISPs will be untrustworthy
  - People, even trusted people, make mistakes
    - Trusted people do "go bad"
  - Transitive trust in people or organizations causes mistakes to propagate (the domino effect)
- Elements of security solutions must exhibit the same dynamics as the parts of BGP they protect
- The memory and processing requirements of a solution should scale consistent with BGP scaling

Principle of Least Privilege

- Each system element should be granted the permissions necessary to perform its functions, but no more
- Applying this cornerstone information assurance principle to BGP:
  - A security failure (or benign error) by an ISP or subscriber should not propagate to other ISPs
  - Any security strategy for BGP should incorporate this “fire break” approach to containing (Byzantine) security failures or errors

Scope and Dynamics of BGP Data



Vigil Security LLC

Architecture and Implementation

- Improve quality of BGP router implementations
  - Reduce the likelihood that an individual router can be crashed, thwarting DoS attacks on itself
  - Reduce the likelihood that BGP software can be subverted as a result of router compromise, thwarting DoS attacks on neighbors
- Yet, improvements in BGP implementations will not secure the routing system – architectural changes to address BGP security are needed too
- **Architectural and implementation security improvements are required to make BGP secure and robust**

BGP and Router DoS Issues

- Generally, routers are unable to process management data (like BGP and SNMP) at line rates, which is normally not a problem
- DoS vulnerability for the processor that deals with management traffic
- This implementation vulnerability may merit an architectural solution, given its severity and pervasiveness – it is not just a BGP issue
- BGP has two classes of traffic:
  - Point-to-point – various solutions possible
  - End-to-end – requires more sophisticated solutions

The Basic BGP Security Requirement

- **For every UPDATE it receives, a BGP router can verify that the "holder" of each prefix authorized the origin 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 requirement, if achieved, allows a BGP router to detect and reject unauthorized routes, irrespective of the attack resulted in the bad routes
- Failing to achieve this requirement, a BGP router will be vulnerable to attacks that result in misrouting of traffic in some fashion

Derived BGP Security Requirements

- Verification of AS ownership and prefix holders
- Binding a BGP router to the AS(es) it represents
- Router authentication of UPDATEs
- Route withdrawal authorization
- Integrity and authenticity of all BGP traffic, countering active wiretap attacks that could result in DoS
- Timeliness of UPDATE propagation

Incremental Deployment

- Cannot afford a flag day
- Provide improved security to routers that implement the security solution, without harming routers that are ignorant of the security solution
- Reality: the Internet routing system is vulnerable until all routers implement the security solution

IETF Activities

IETF RPSEC WG

- Routing Protocol Security Requirements
- Generic Threats to Routing Protocols (in RFC Editor Queue)
- Three other draft documents:
  - OSPF Security Vulnerabilities Analysis
  - Generic Security Requirements for Routing Protocols
  - BGP Security Requirements
- No protocol development has begun …

IETF PKIX WG

- RFC 3779: X.509 Extensions for IP Addresses and AS Identifiers
- Need a protocol to go with it …
- Yet, it can be the cornerstone to a solution that will prevent misconfiguration errors from propagating
- Can we get started?

Personal Opinion

- The time is right …
- Use the pieces that exist
  - We know that incremental deployment is the only way forward
- Ask for the missing pieces
  - The IETF needs to know that there is a constituency waiting for standards

Questions?

Russ Housley
+1 703-435-1775 (voice)
+1 703-435-1274 (fax)
housley@vigilsec.com

Vigil Security LLC