BGP Security

RIPE 52 Meeting
Istanbul, Turkey
26 April 2006

Russ Housley
housley@vigilsec.com

Vigil Security LLC

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

A Few Well Known Incidents

- **Apr 1997**: AS 7007 announced direct connections to all the Internet
- **Dec 1999**: AT&T's server network announced by another ISP, misdirecting their traffic
- **Dec 24, 2004**: Thousands of networks misdirected to Turkey, including parts of CitiCorp, MetLife, Blue Cross Blue Shield (See http://www.nanog.org/mtg0505/pdf/underwood.pdf)
- **Sep 2005**: AT&T, XO, and Bell South misdirected to Bolivia
- **Jan 2006**: Many networks, including PANIX and Walrus Internet, misdirected to New York ISP

- **These are human mistakes, not attacks**
- **But, anything possible through human error can also be done by human intent**

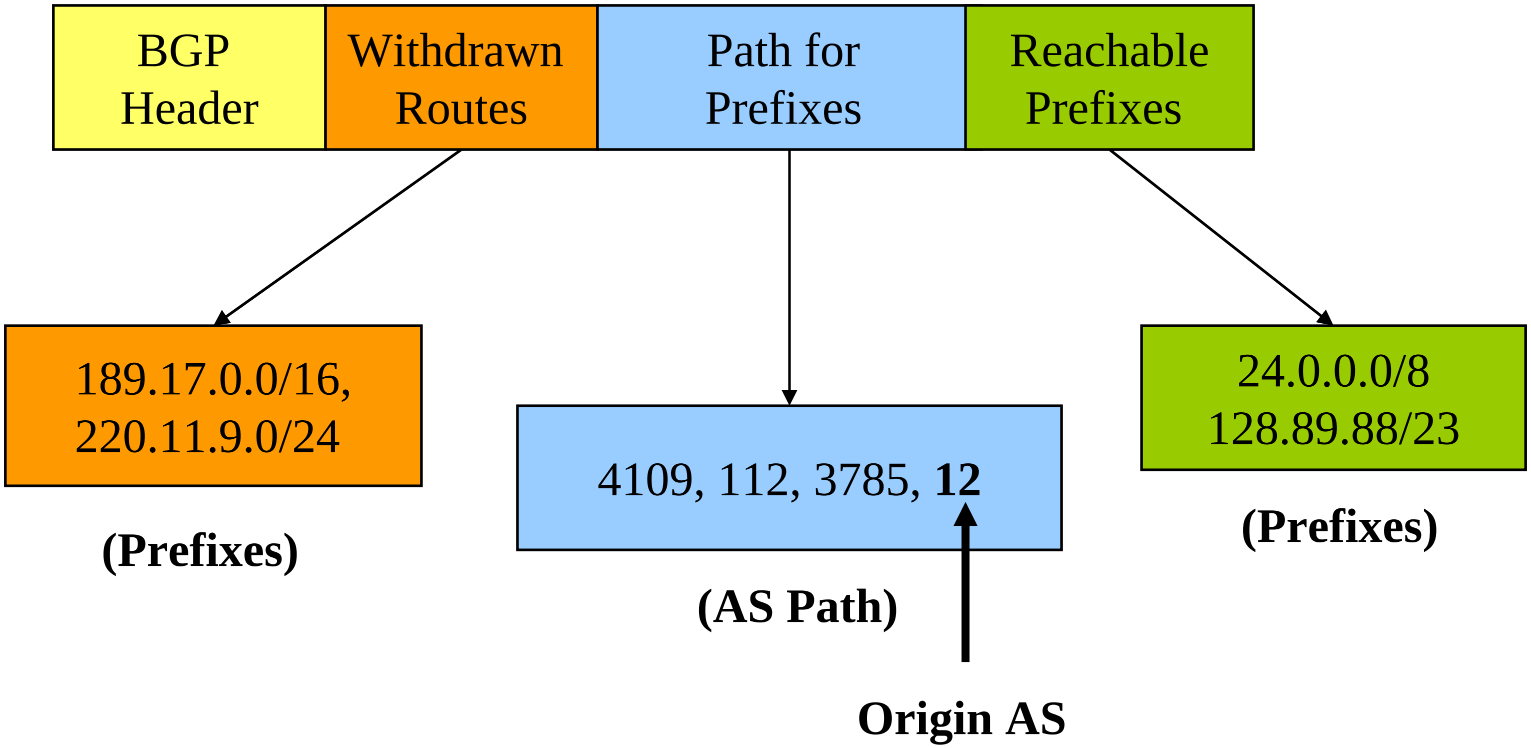
Is BGP Under Attack?

- 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 send Spam messages from unused address space
- BGP-based attacks have been used by hackers as part of an effort to masquerade as root DNS servers

External vs. Internal use of BGP

- BGP is used between ISPs
- BGP vulnerabilities impact the whole routing infrastructure
  - Routes acquired from other ASes via eBGP are propagated to other border routers within an AS using iBGP

A Simplified UPDATE Message



BGP Header

Withdrawn Routes

Path for Prefixes

Reachable Prefixes

189.17.0.0/16,
220.11.9.0/24

(Prefixes)

4109, 112, 3785, **12**

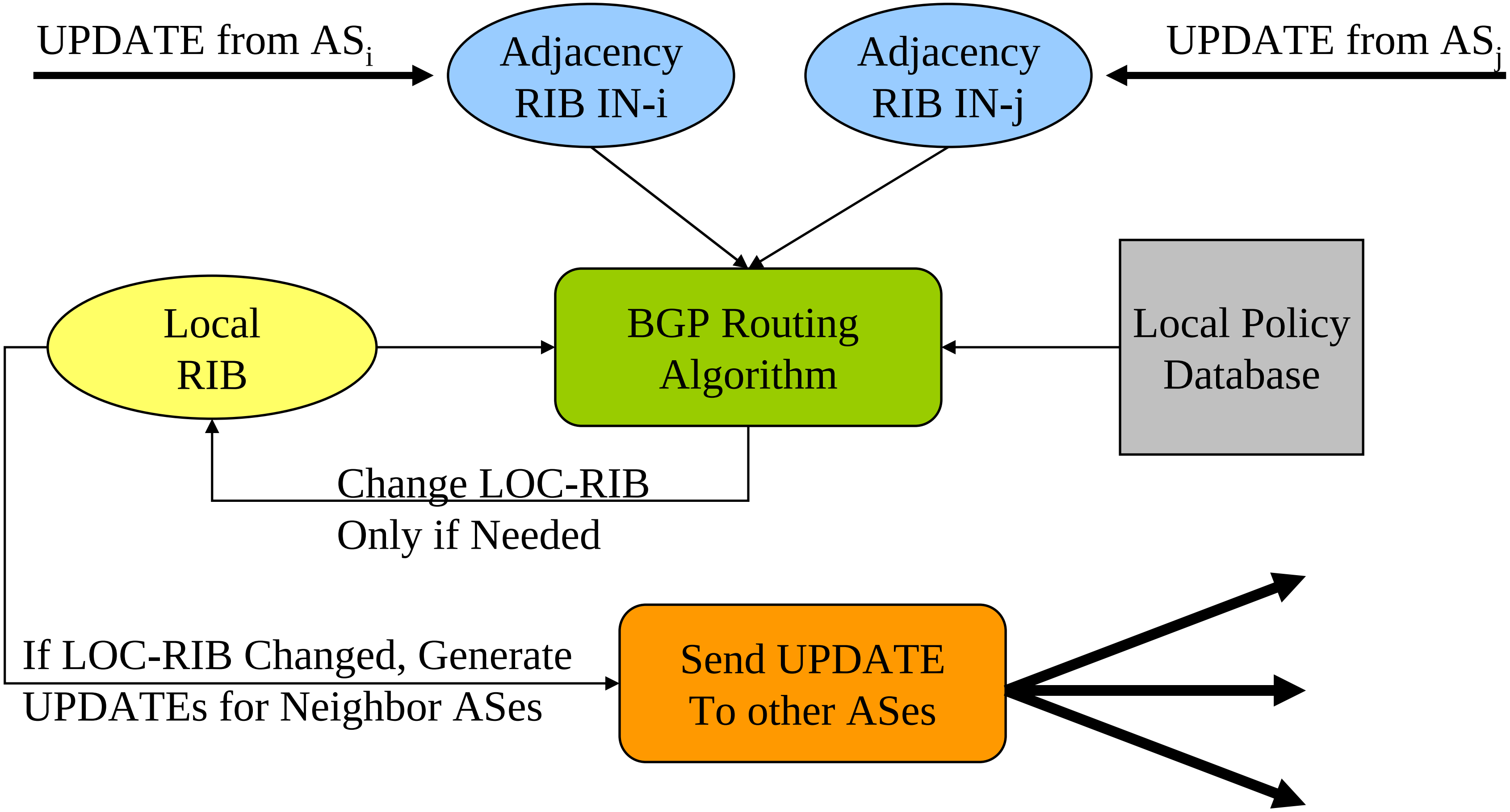
(AS Path)

Origin AS

24.0.0.0/8
128.89.88/23

(Prefixes)

Processing an UPDATE



Vigil Security LLC

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, then 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
- Multiple paths between two ASes is a common cause of asymmetric routes
  - Also, due to local policy an AS may report different routes to different neighbors
- Not all connections between ASes are visible to the whole Internet – peering near the edge
- 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 be using a “better” route available from another source

BGP Security

Adversary Goals for BGP Attacks

- Degrade service (locally or globally) by mounting a denial-of-service (DoS) attack against a router’s BGP implementation
- Reroute subscriber traffic to enable 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

BGP Security Solution Requirements

- Security architectures for BGP should not rely on “trust” among ISPs or subscribers (or any router)
  - On a global scale, some ISPs will be untrustworthy
  - People, even trusted people, make mistakes
  - 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 no worse than BGP itself
- Solutions must accommodate incremental deployment

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

	LOCAL	GLOBAL
SLOW	Add/delete BGP router Operation staff changes	Allocation of new prefixes or AS Numbers Add/delete peer
FAST	Install new link	Route change

Vigil Security LLC

The Basic BGP Security Requirement

- **For every announcement 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**
- **For every withdrawal it receives, a BGP router can confirm the source of the message**
- This requirement, if achieved, allows a BGP router to detect and reject unauthorized routes
- Failing to achieve this requirement, a BGP router will be vulnerable to attacks that result in misrouting in some fashion

Derived BGP Security Requirements

- Verification of AS and prefix holders
- Binding a BGP router to the AS(es) it represents
- Router authentication of announcement messages
- Route withdrawal authentication
- Integrity and authenticity of all BGP traffic to thwart active wiretap attacks
- Timeliness of UPDATE message propagation

Incremental Deployment

- *NO* 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
- Adjacent ASes can provide a “secure” portion of the Internet routing system, and then expand outwards

Several Long Lead Items

- Develop infrastructure to provide authentic IP address prefix and AS number holders
  - Clean up the registry data
  - Repository
- Develop standards to transfer the authentic announcement and withdrawal messages

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
- Protocol work will be done elsewhere …

IETF PKIX WG

- Public Key Infrastructure using X.509
- RFC 3779: X.509 Extensions for IP Addresses and AS Identifiers
- Need two companion parts:
  - Prefix “holder” to authorize one or more ASes to originate routes
  - a distribution mechanism
- Can be a significant portion of a solution that will prevent misconfiguration errors from propagating

IETF SIDR WG

- Secure Inter-Domain Routing
- Chartered April 2006
- SIDR WG will
  - document an extensible inter-domain routing security architecture
  - document the use of certification objects within this secure routing architecture
  - document specific routing functionality modules within this architecture that are designed to address specific secure routing requirements as they are determined by the RPSEC WG

Personal Opinion

- The time is right …
- Registry cleanup effort are under way
- 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