An overview of current BGP security problems

Ralph Krimmel

July 3, 2012

1. Introduction
2. Security issues of BGP
3. Cryptographic techniques
4. BGP security today
5. Defensive Filtering
6. S-BGP

Routing in the Internet

The Internet

- Large, decentralized Network
- Intermediate hosts: Routers
- Internet protocol

Some definitions

IP Addresses

- IP Address: 32(v4)/128(v6) bit Numbers
- E.g.: Host: 134.76.80.1 Subnet: 134.76.80.0/24
- IP Prefix: Block of IP addresses

Some definitions #2

Autonomous Systems

- Collection of IP prefixes under control of one organisation
- Identified by *AS Number*
  - Public: 1-64511
  - Private: 64512-65535
- Exchange routing information with adjacent autonomous systemss

BGP

BGP Basics

- Incremental protocol
- 4 Message Types
  - Open: Session initiation
  - **Update**: Advertisement/withdrawal of routes
  - Notification: Session termination
  - Keepalive: Verification of reachability

BGP Update Message

Important attributes

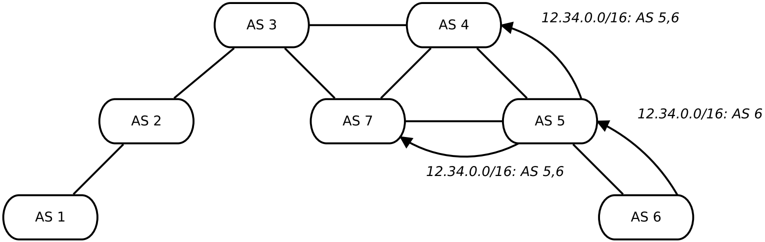
- Next hop: Destination of the next hop router
- AS-Path: Path with AS-Numbers leading to prefix
- Several attributes for path selection (MED, Origin, Local preference)

Path selection

Decision factors

1. Local preference
2. Shortest AS path length
3. Lowest origin value
4. Lowest MED value
5. ...

Example

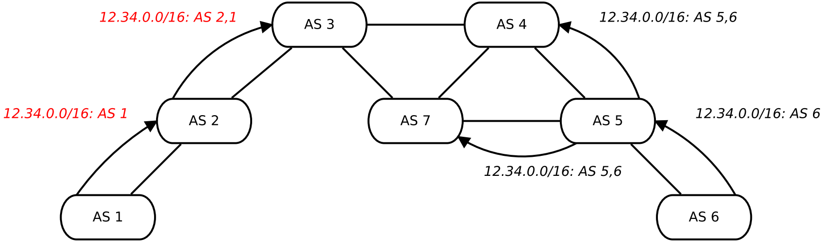

AS 3
AS 4
12.34.0.0/16: AS 5,6
AS 2
AS 7
AS 5
12.34.0.0/16: AS 6
12.34.0.0/16: AS 5,6
AS 1
AS 6

Prefix hijacking

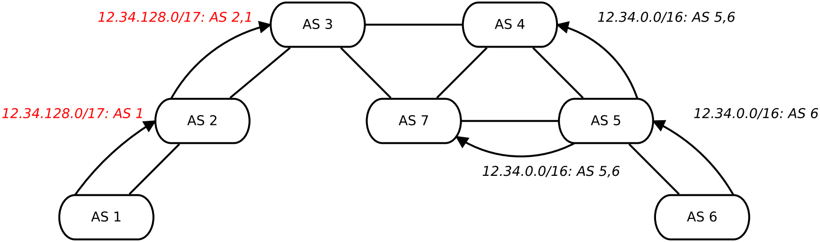
No verification of:

- Prefix ownership
- AS number ownership

Short AS pathes



Deaggregation



Attacks on TCP

Attacks on TCP

- Eavesdropping to learn routing information
- MITM: Insertion, modification and deletion of messages
- Replay attack
- DoS attacks (via RST, SYN-Flood)

Cryptographig techniques

Some techniques

- Pairwise keying
- Cryptographic hash functions (message digests)
  - Non-invertible
  - Collision resistant
- Message Authentication Code: digest(Shared key + Message)

BGP security today

Current approaches

- Protection of the BGP session between routers
- Defensive filtering

Protection of a BGP Session between routers

Two goals

- Protecting TCP
- BGP session itself

Proposed solutions

Countermeasures

- MD5 Integrity
- Session and Message Protection
- Generalized TTL Securiy Mechanism
- IPsec

MD5 Integrity

Idea

- TCP extension that uses a MAC based on MD5
- Carries MAC of TCP header and BGP data

⇒ Protects integrity and prevents replay attacks

Session and Message Protection

Proposed countermeasures

- Adding sequence numbers
- Encryption of all BGP data between peers
- Digital signatures of all UPDATE fields

Disadvantages: BGP needs to be altered, based on shared keys

Generalized TTL Security Mechanism

Idea

- IP header contains a TTL field
- TTL decreased with every hop
- Utilize IP TTL to discard every packet with TTL < 254.
- Cheap solution
- Weakly defends against remote attacker

IPsec

IPsec overview

- IP layer protocol
- Three protocols: IKE (Key Managment, AH and ESP (packet level security)
- Provides: authenticity, integrity, replay prevention, confidentality, DOS prevention
- Widely used for securing BGP sessions

Defensive Filtering

Goal: Filter bad and potential malicious announcements

Route policies

- Prefixes with special uses
- Bogons
- Private AS numbers
- Long AS-Pathes
- Routes to small networks (Deaggreation prevention)
- Limit of announcements by a neighbour (DoS and Deaggreation prevention)
- Rewrite of BGP attributes

S-BGP

S-BGP overview

- Full scale security architecture
- Installs PKI, parallel to existing allocation and delegation systems
- BGP data can be signed and verified
- IPsec to secure peer sessions
- Two kind of attestations: Address and route attestations

Address attestations

Address attestations

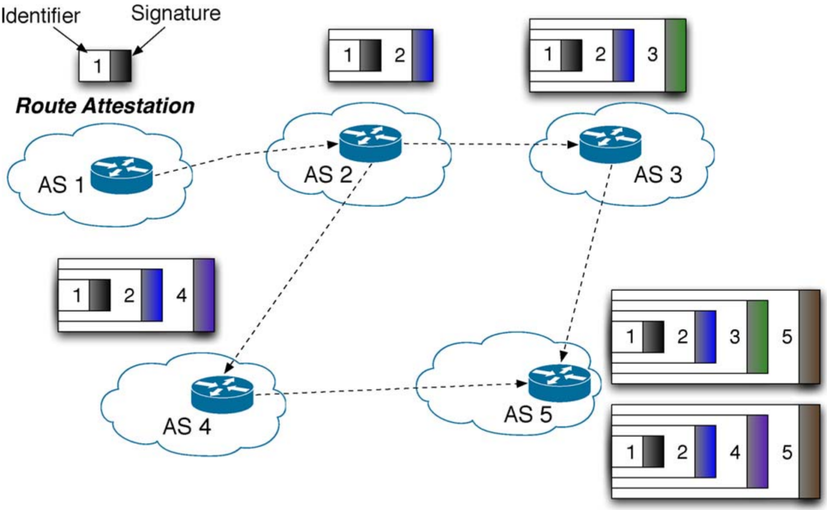
- Out-of-band mechanism
- Verification of the ownership of prefixes via certificates
- Delegation chain, similar to x.509 PKI

Route attestations

Route attestations

- Distributed via BGP
- Update messages can carry digital signatures
- Each AS in the path signes the path recursively

Route attestations



Deployment issues

- S-BGP needs more memory
- Alot of parties have to work together (IANA/ICANN)/ISPs/Router vendors

Summary

Summary

- BGP plays a large role in in internet routing
- BGP is vulnerable at many places
- Several existing practises to defend against threads
- Existing solutions are hard to deploy

Questions?