BGP
Security Vulnerabilities Analysis

INTERNET DRAFT - draft-ietf-idr-bgp-vuln-00.txt
GSO - FH - Nürnberg
Sicherheit im Internet

Andreas Lorisch

GEORG-SIMON-OHM FACHHOCHSCHULE NÜRNBERG

Agenda

Introduction

Introduction: History

- BGP 4 (RFC 1771) specified in March 95
- BGP 3 (RFC 1267) specified in October 91
- Based on EGP (RFC 904) of April 84

- BGP was created when the Internet was much more peaceful than nowadays
- It lacks protection against errors and authentication

Introduction

- BGP is a TCP/IP – protocol
  - Subject to TCP/IP attacks like IP Spoofing, Session stealing, etc.
  - Outsiders could inject bogus routing information or disrupt peer to peer communication
  - This new information would spread through peers
- Therefore at least authentication mechanism must be supported (TCP MD5 Signature)

Introduction

- Faulty routing information can be caused by misconfigured peers themselves
  - By masquerading as other legitimate BGP speakers
  - By distributing unauthorized routing information
- Whole portions of the network could become unreachable
- Packets could be forwarded by a suboptimal path or a path that will not forward the traffic
- Therefore traffic could be delayed or misleaded

Introduction

- The damage resulting from attacks might be:
  - Starvation
  - Network congestion
  - Blackhole
  - Delay
  - Looping
  - Eavesdrop
  - Partition
  - Cut
  - Churn
  - Instability
  - Overload
  - Resource exhaustion

Attacks

Attacks

- BGP is subject to the following attacks:
  - Eavesdropping:
    - Routing data is carried in cleartext (attacks confidentiality)
  - Replay:
    - BGP doesn‘t provide any protection against replay attacks
  - Message Insertion:
    - No protection against message insertion
    - However if TCP Session is fully established, prediction of the correct session number becomes necessary for the attacker

Attacks

- Further attacks might be:
  - Message deletion:
    - No protection inside BGP
    - Again difficult against mature TCP implementation
  - Message modification:
    - Modifications not altering the length of the payload can not be detected
  - Man-in-the-middle:
    - As BGP has no peer entity authentication, man-in-the-middle attacks are easy to accomplish

Attacks

- Another attack against BGP is the Denial of service attack:
  - Bogus routing data can represent a DoS attack to:
    - End systems trying to transmit data through the network
    - The network infrastructure itself
  - Certain bogus information can represent a DoS attack to the BGP protocol itself:
    - E.g.: advertising large numbers of more specific routes can cause BGP traffic and routing table size to explode

Attacks: Countermeasures

- The protection of BGP using the TCP MD5 signature option (RFC 2385) will counter most of the previously listed attacks from outsiders
- It will not protect against eavesdropping, but confidentiality of routing data is no goal of BGP
- Replay attacks will still be possible too, but with TCP sequence number processing it will be hard to accomplish
- Still no protection against misconfigured legitimate speakers

Vulnerabilities and Risks

Vulnerabilities and Risks

- There are three major vulnerabilties in BGP:
  - There is no mechanism to proof freshness, protection of integrity and peer authentication in the BGP protocol
  - There is no validation of the authority of an Autonomous System (AS) to announce Network Layer Reachability Information (NLRI)
  - There is no insurance of the authenticity of path attributes announced by an AS

Vulnerabilities and Risks

- The first of these vulnerabilties motivated the support of the TCP MD5 signature in the BGP specification
- If implemented correctly, it provides message integrity and peer authentication
- But in the spec. the MD5 algorithm is supposed to be secure (which is not true), and that the shared secret is protected and difficult to guess

Vulnerabilities and Risks

- There are four diffrent types of BGP messages:
  - OPEN
  - KEEP ALIVE
  - NOTIFICATION
  - UPDATE
- Each of them has ist own vulnerabilties, which will be, besides other vulnerabilties, discussed in the following

Vulnerabilities and Risks

- Message Header:
  - Each BGP message starts with a standard header
  - Sytactic errors within the header will cause the connection to be closed, newly learned routes will be deleted and a new decision process about routes will be started

Vulnerabilities and Risks

- OPEN message:
  - Receipt of an OPEN message in state Connect, Active or Estabished, or receipt of erroneous OPEN messages will cause:
    - Closing of connection
    - Deletion of all associated routes
    - Starting of decision process
    - Return state to idle
  - Receipt of an OPEN message in state OpenSent (spoofing) will cause transition to OpenConfirmed state and the following legitimate OPEN message will be dropped

Vulnerabilities and Risks

- KEEPALIVE message:
  - Receipt of a KEEPALIVE message when the peering connection is in the Connect, Active or OpenSent state would cause a transition to the Idle state, and the failing of the connection to be established
  - To exploit this vulnerability, the KEEPALIVE message must be timed carefully within the exchanged messages

Vulnerabilities and Risks

- Receipt of a NOTIFICATION message in any state will cause the previosly described effects:
  - Closing of connection
  - Deletion of all associated routes
  - Starting of decision process
  - Return state to idle

Vulnerabilities and Risks

- UPDATE message:
  - In general, the UPDATE message carries the routing information, therefore the ability to spoof any part of this message will alter the routing tables
  - Withdrawn Routes field inside an UPDATE message:
    - By modifying this field an attacker could cause the elimination of existing legitimate routes
    - Reestablished routes could be deleted via replaying a previously recorded withdrawal
  - But the withdrawal of routes can only be performed by the BGP speaker having formerly announced these routes

Vulnerabilities and Risks

- UPDATE message continued:
  - The Path Attributes within the UPDATE message present various vulnerabilities and risks:
    - Altering of the AS_PATH attribute could be used to affect routing decisions, and thus mislead traffic to suboptimal routes, to create loops or to gain access to traffic
    - The NEXT_HOP attribute could be modified to disrupt forwarding of traffic between to AS‘s, or to force another AS to carry traffic it would otherwise not have to

Vulnerabilities and Risks

- UPDATE message continued:
  - Modifying or forging the NLRI field in the UPDATE message could cause :
    - Disruption of routing to the announced network
    - Overwhelming of a router along the announced route
    - Data loss if the announced route will not forward traffic to the announced network
    - Routing of traffic by a suboptimal route, etc.
  - In general, syntactic malformed UPDATE messages will cause the connection to be closed, associated routes will be deleted, etc. , with the previosly described effects

Vulnerabilities and Risks

- Other vulnerabilities arise through the use of the TCP protocol:
  - TCP SYN attack:
    - BGP is vulnerable to SYN flooding as other protocols using TCP
    - An attacker could send a SYN, and a sequence of BGP packets to establish a BGP session, letting the legitimate connection appear as a collision which would be destroyed
  - TCP SYN ACK:
    - If an attacker could answer to a SYN before the legitimate peer, which would receive an empty ACK reply this would finally result in a RST that would break the connection

Vulnerabilities and Risks

  - Further spoofed RST or FIN messages would also cause the connection to be broken
- All these TCP attacks can be countered by the use of BGP session protection via the TCP MD5 signature option

- DoS and DDoS attacks against BGP are easy to accomplish, because packets directed to port 179 are passed to the BGP process, normally residing on a slower processor

GEORG-SIMON-OHM
FACHHOCHSCHULE
NÜRNBERG

Security Considerations

Security Considerations

- The use of the ‚Protection of BGP Sessions via the TCP MD5 Signature Option‘ (RFC2385) counters message insertion, message deletion, modification and man-in-the-middle attacks from outsiders and therefore should be used
- If routing data confidentiality is desired, this could be accomplished using IPSec ESP
- Both provide security, assuming the algorithms are secure, the used secrets are protected from exposure and not guessable, the platforms are secure, etc.

Security Considerations Residual Risks

- Protection against attacks arising from legitimate peers could be accomplished through:
  - Origination Protection: sign the originating AS
  - Origination and Adjacency Protection: sign the originating AS and predecessor information
  - Origination and Route Protection: sign the originating AS and remove AS_PATHs of ‚bad routers' (Secure-BGP)
  - Filtering: verify AS_PATH and NLRI originating AS via a registry (RFC2725)
- Except of Filtering, which is limited to the ‚outscirts' of the internet, none of these is in common use

Security Considerations Operational Protections

- BGP is used by all major ISPs, to distribute global routing information, internally and between each other
- Therefore BGP implementations are confronted with huge amounts of traffic, making use of cryptography nearly impossible
- Protection against DoS attacks can only be achieved using port based packet filtering

Security Considerations Operational Protections

- Current practice of the ISPs is the usage of filtering techniques at their borders, reducing exposure to attacks from outside
- These filters remove the BGP Port Number (179) from traffic destined to the inside, preventing internal peers to be flooded
- Prevented from injecting sufficent traffic from the outside, attackers have to gain physical access

References

-BGP Security Vulnerable Analysis

‚draft-ietf-idr-bgp-vuln-00.txt'

Sandra Murphy – NAI Labs

-A Border Gateway Protocol 4 (BGP-4)

‚draft-ietf-idr-bgp4-20.txt' and RFC1771

Y. Rekhter, T. Li, S. Hares

-Internetworking Technology Handbook - Cisco Systems

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/

-Protection of BGP Sessions via the TCP MD5 Signature Option

RFC2385

A. Heffernan

Thank You!