Routing Protocol Security
Requirements (rpsec)
Internet-Draft
Expires: March 17, 2004

S. Convery
D. Cook
M. Franz
Cisco

September 17, 2003

An Attack Tree for the Border Gateway Protocol
draft-convery-bgpattack-01

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on March 17, 2004.

Copyright Notice

Abstract

This I-D presents all known attack vectors into or using BGP. The data is presented in "Attack Tree" format as published by Schneier [ATTACKTREE] and detailed by the CERT in "Attack Modeling for Information Security and Survivability" [MODELING]. Future security improvements to BGP (whether best practices or enhancements to the protocol) should consider the attacks outlined here when determining the relative security improvements such changes provide.

Table of Contents

1. Introduction

BGP and other infrastructure protocols such as DNS have received significant critical attention as the overall awareness of Internet security has increased. Although BGP threat models have been published [BGPVULN] that identify inherent vulnerabilities in the protocol, none have considered the full range of options available to the adversary or their relative difficulty.

The use of attack trees focuses analysis on measurable goals that can ultimately be translated into specific tests against popular implementations. This analysis technique also encourages a structured elaboration of events that must occur for a successful intrusion. Since each node (an attacker goal) may be decomposed into subordinate nodes (sub-goals, or means of achieving the parent goal), attack trees allow security analysis to be conducted at multiple layers of abstraction. This allows common attacks to be referenced as reusable modules that apply to common network scenarios.

Although a comprehensive discussion of attack trees is outside the scope of this I-D, it is useful to provide a general overview of their function and value. The clearest way to demonstrate this is through examples, as illustrated in [ATTACKTREE]. Consider an individual trying to gain unauthorized physical access to a building. An attack tree for such an act might look like this:

Goal: Gain unauthorized physical access to building

Attack:
OR 1. Unlock door with key
2. Pick lock
3. Break window
4. Follow authorized individual into building

This simple tree should be read as follows: to gain unauthorized physical access to a building, the adversary must unlock the door with a key, pick the lock, break a window, or follow an authorized individual into the building. The "OR" operator defines that only one is required. In the same tree, replacing the "OR" with "AND" would require that all subordinate goals be achieved to realize the parent goal. Attack trees at this level of detail are of limited use. Their true value comes in understanding how an adversary can execute one of the listed subordinate goals. This requires the following, more detailed, attack tree:

Goal: Gain unauthorized physical access to building

Attack:

```
OR  1. Unlock door with key
    OR  1. Steal Key
        2. Social Engineering
        OR  1. Borrow key
            2. Convince locksmith to unlock door
    2. Pick lock
    3. Break window
    4. Follow authorized individual into building
    OR  1. Act like you belong and follow someone else
        2. Befriend someone authorized outside a building
        3. Appear in need of assistance (such as carrying a large box)
    AND 4. Wear appropriate clothing for the location
```

Now the various sub nodes of the tree are better defined. In order to "unlock door with key" you need to either steal the key or perform some type of social engineering. Sub goal 4 (Follow authorized individual into building) illustrates the use of "OR" and "AND" at the same level of the tree. This should be read as follows: In order to follow an individual into the building the adversary needs to do one of the first 3 listed items, and wear appropriate clothing for the location.

The use of attack trees also allows comparison between technical and non-technical means of attack, and leads to a more comprehensive analysis of threats and vulnerabilities. Even without extensive elaboration, we learn in this tree that following someone into a building is probably the easiest way of gaining entrance with the lowest amount of cost or risk to the adversary. This class of attacks collectively known as "social engineering" is listed but not elaborated throughout this I-D. In many cases social engineering is the easiest form of attack and could result in the greatest damage.

This I-D illustrates a simple BGP attack tree: subsequent analysis could assign attributes (and possibly values) to each node of the tree. This allows more quantitative methods to be used in analyzing the attack tree data. These attributes could include:

- Impact of the attack
- Ease of attack execution
- Cost of the attack
- Presence of countermeasures (such as best practices)
- Access/trust requirements to conduct attack

Analysis of this data will yield the subset of attacks that result in

the most damage, are the easiest to launch, the least costly, have the least access requirements, and are unlikely to be mitigated by current best practices. Addressing these attacks should be the initial focus of any improvements to BGP or relevant best practices.

Computer security terms used in this I-D are in accordance with RFC 2828 [GLOSSARY].

2. BGP Attack Tree

This I-D divides the attack tree into three main sections to reduce redundancy and provide greater portability into subsequent trees defined in other I-Ds. When another section of this I-D is referenced within a specific tree, the tree located at the referenced section should be attached at the point the reference is made.

The first section details BGP Atomic Goals of an adversary and is detailed in Section 2.1. BGP Atomic Goals are defined in this I-D as the narrowest form of attack by an adversary specifically directed against BGP. BGP Atomic Goals consist of unique attack techniques and Supporting Atomic Goals as detailed in Appendix A. Supporting Atomic Goals are common network attack methods used in more than one BGP Atomic Goal. The third main section of the document details higher level adversary goals that make use of BGP Atomic Goals (and therefore supporting atomic goals as well). These goals are referred to as Attack Scenarios and are detailed in Section 2.2.

It is worth noting that the inclusion of an attack in this attack tree says nothing with regard to the likelihood such an attack will occur or even the reasonable possibility it could occur. Future testing and analysis, as mentioned earlier, is required to accurately interpret the data in this tree. Some of this analysis has been done in [VULNTEST] but further testing is warranted. Some of the results from this testing have been incorporated into this I-D.

2.1 BGP Atomic Goals

The following atomic goals are defined and used throughout the attack tree:

- Compromise MD5 authentication
- Establish unauthorized BGP session with peer
- Originate unauthorized prefix into peer route table
- Change path preference of a prefix
- Conduct denial/degradation of service against BGP process
- Reset single BGP session
- Spoof a BGP message

2.1.1 Compromise MD5 Authentication

The common-sense view is that most adversaries will choose the path of least resistance, so that all but the most sophisticated threats would target a BGP speaker whose sessions are not protected by RFC 2385 [BGPMD5] authentication. Nevertheless, attempting a compromise of MD5 authenticated BGP messages could be done as follows:

```
Attack:
OR  1. Use social engineering to obtain MD5 password
    2. Capture Password
    OR  1. Keystroke logger
        AND  1. Compromise/gain access to administrative host
             2. Install hostile application on administrative host
             3. Observe MD5 password as it is typed/viewed on screen
        2. Sniff MD5 password from management traffic (Appendix A.4)
        3. Capture password from router configuration
        OR   1. Compromise network management server
             OR  1. View unencrypted router configuration
                 2. Decrypt encrypted router configuration
             2. Compromise router (Appendix A.1)
    3. Brute-Force MD5 password
    OR  1. Active attack - Send signed message to peer eliciting signed
response
        AND  1. Send segment with RFC 2385 option to router
             2. Observe response from router to determine if your hash
             was valid
             3. Gain physical/local access to link between peers
        2. Passive Attack
        AND 1. Obtain hashed packet (to facilitate offline attack)
            2. Use RFC 2385 cracking tool to discover password
    5. Discover implementation flaw in RFC 2385
    6. Discover new attack against MD5
    7. Exploit hash collision attack against MD5
```

To validate our assumptions about the relative difficulty of attacking RFC2385 authentication, we must have test data that measures the relative ease/difficulty of such attacks (or the side effects of unsuccessful attacks) against popular BGP/TCP implementations. When observing the response from an RFC 2385 authenticated session, sniffing will be necessary if using a spoofed SYN. Findings from [VULNTEST] indicate that an inline adversary is easily able to determine the MD5 key if weak passwords are chosen but that a sufficiently strong password is as difficult to attack as any other strong password using in modern computing today. Preliminary tool development indicates that an offline attack is far more viable

than an online attack.

2.1.2 Establish Unauthorized BGP Session with Peer

Establishing an unauthorized BGP session with a peer is defined by achieving a peering arrangement without the knowledge or permission of both sides of the session. This includes peering sessions established by routers and/or any other device capable of being a BGP speaker. In this this attack, "permissive router" is meant to mean a router which will allow BGP peering without explicit neighbor IP / AS configuration.

```
Attack:
OR  1. Establish session with permissive router
    OR  1. Find available local BGP speaker
        OR  1. Port Scan
            2. Social Engineering
        2. Find available remote (EBGP-multi) speaker
        OR  1. Port Scan
            2. Social Engineering
    AND 3. Establish peering relationship with discovered router
    2. Compromise router and reconfigure to allow peering session
    AND 1. Compromise Router (Appendix A.1)
        2. Configure router to allow peering from attacking router
    3. Simulate BGP Session from non-router
```

Once a peering session has been established, the adversary can much more easily launch attacks that not only effect the peer, but the entire network. Internet scanning performed in [VULNTEST] indicates that "permissive routers" are a very small percentage of deployed routers and that with basic BCPs a router can be sufficiently masked so as to make blind attacks impossible. When the adversary is inline, much more damage is possible.

2.1.3 Originate Unauthorized Prefix/Attribute into Peer Route Table

To accomplish this goal, an adversary must insert a new prefix into a peer's routing table. This attack can be used to change traffic patterns in a network in the case that the prefix is more specific than the route previously used to direct traffic. This can lead to stolen or blackholed traffic across the network. This introduced prefix/attribute could be used for all sorts of malicious goals some of which are detailed in Section 2.2.

```
Attack:
OR  1. Send from valid Router
    OR  1. Misconfigured
        2. Compromise router (Appendix A.1)
    2. Send from Invalid Router
    AND 1. Gag valid router
```

```
          OR  1. Kill Router
              OR  1. Power Off/Physical Layer
                  2. Crash and prevent reboot
                  3. Conduct denial of service against router (Appendix A.2)
              2. Steal IP Addr
              OR  1. ARP Spoof
                  2. Steal MAC
          2. Introduce rogue router (Assume IP)
          OR  1. Steal IP Addr (section 2.1.3.1.2)
              2. More Specific Route Introduction
              3. Establish unauthorized BGP session w/peer (Section 2.1.2)
      3. Send spoofed BGP Update from Non-Router
      OR  1. Conduct TCP Sequence Number Attack (Appendix A.4)
          2. Conduct Man-in-the-Middle (Appendix A.3)
  AND 4. Craft BGP Message
```

This is one of several attacks that can be caused by misconfiguration as opposed to a deliberate attack. Launching this attack from a compromised / misconfigured router is by far the easiest with findings from [VULNTEST] indicating that sending spoofed updates as a blind adversary is more difficult than previously posited.

2.1.4 Change Path Preference of a Prefix

Changing the path preference of a prefix can lead to the same types of attacks that occur by inserting a new prefix into a peer's routing table. This atomic goal is defined by altering the attributes of a prefix so that the BGP decision process is affected. This goal is different from originating an unauthorized prefix in that altering the attributes implies that the prefix already exists in the BGP table. There are different methods that can be used to accomplish each of these goals so they will be analyzed separately.

```
Attack:
OR  1. Modify (AS-PATH, Next-Hop, MED, local-pref, communites)
    OR  1. Valid BGP Speaker
        OR  1. rogue transit implementation
            2. compromise edge (origin/recipient) router
        2. Man-in-the-middle attack (Appendix A.3)
        3. Compromise router (Appendix A.1)
```

In reality, any attribute could be altered to change the path preference. The five listed are the most common.

2.1.5 Conduct Denial/Degradation of Service Attack Against BGP Process

BGP routing processes are susceptible to a variety of attacks which can prevent establishment of new sessions, exchange of routing updates, or cause the router itself to become inoperable.

```
Attack:
OR  1. Denial of service against router (Appendix A.2)
    2. TCP Resource Exhaustion against Port 179
    OR  1. SYN Flood - exhaust SYN_RCVD state in TCP stack
        2. Connect() - repeated full (3-way handshake) connections
        3. LAST_ACK - complete 3-way handshake, then FIN-ACK
    3. Invalid BGP Messages
    OR  1. OPEN
        2. UPDATE
        3. KEEPALIVE
        4. NOTIFICATION
    4. Valid BGP Messages
    OR  1. Update Flooding
        OR  1. Flood routes (/32, etc.)
            2. Excessively long path attributes
        2. Update/Withdraw Flooding
        3. MD5 Resource Exhaustion
```

Given the nearly infinite number of attacks and operational conditions that could cause a routing process to stop performing as expected, a significant testing effort will be needed to increase the level of assurance in popular BGP implementations. Findings from [VULNTEST] indicate that basic TCP resource exhaustion attacks are difficult against current popular BGP implementations particularly if the peer has been already established. MD5 resource exhaustion attacks are similarly difficult. The easiest DoS against the BGP process itself is update flooding from a compromised router or inline adversary.

2.1.6 Reset a Single BGP Session

In this attack, the adversary is trying to cause a current BGP session in the established state to reset. Such an attack could be launched over and over again to prevent two peers from reliably exchanging routing information.

```
Attack:
OR  1. Send message to router causing reset
    OR  1. Send RST message to TCP stack
        2. Send BGP Message
        OR  1. Notify
```

2. Open
3. Keepalive
AND 3. TCP Sequence number Attack (Appendix A.4)
2. Alter configuration via compromised router (Appendix A.1)

It is unknown why an adversary would choose to reset a session via Section 2.1.6.1.2. Since the preconditions of attack Section 2.1.6.1.1 are required in order to be successful. Also, it should be noted that the sequence number attack detailed in Appendix A.4 is far from trivial to properly execute. Findings from [VULNTEST] indicate the attack can easily be rendered impossible for blind attackers with basic BCPs and even without BCPs determining the proper TCP packet to cause the reset without inline access to the routers is very difficult.

2.1.7 Send Spoofed BGP Message

An adversary could send a BGP message to a BGP speaker and potentially alter the behavior of the routing process. This attack is mainly designed to insert false information into a BGP session, or to reset a session.

Attack:

OR 1. TCP Sequence number Attack (Appendix A.4)
2. Intercept or Modify Data Through Man-in-the-Middle (MITM) Attack (Appendix A.3)
AND 3. Build a valid BGP packet

This attack assumes that the adversary is able to cause the BGP speaker to accept a message without establishing a peering relationship. Spoofing the message is the primary mechanism to accomplish this. Because of the requirement for the TCP sequence number attack, this attack is quite difficult and findings in [VULNTEST] indicate that after the spoofed update is sent, the legitimate TCP session will begin to ACK storm resulting in a session reset in several minutes.

2.2 Attack Scenarios

The attack scenarios represent larger goals an adversary may have which use BGP as a means to accomplish them. These attacks use the atomic goals discussed in Section 2.1 as a mechanism to reduce the duplication of information within each tree.

The following attack scenarios are defined:

o Disable critical portions of the Internet by disrupting Internet

routing tables

- Force a multi-homed AS to use an alternate path to/from an outside network instead of the preferred path
- Disable a single-homed AS
- Disable a multi-homed AS
- Blackhole traffic

2.2.1 Disable Critical Portions of the Internet by Disrupting Internet Routing Tables

Common concerns regarding BGP have described scenarios where large section of the Internet become unreachable due to the lack of security features in BGP. In theory, the attack can be done in one of three main ways: physical destruction, social engineering, or routing attacks.

```
Attack:
OR  1. Physical Destruction
    OR  1. Destroy Peering Points
        2. Strategic Link Destruction (backhoe)
    2. Social Engineering
    3. Routing Attacks
    OR  1. Alter global Internet routing table
        OR  1. Insert unauth prefix into route table (Section 2.1.3)
            2. Establish unauthorized BGP session with peer (Section 2.1.2)
        AND 3. Ensure propagation in spite of prefix filtering
            4. Repeat for ASs at multiple ISP
        2. Disable critical core routers
        OR  1. Router overload leading to crash
            OR  1. DDoS
                2. Worm
                3. Loops
                4. Change prefix paths (Section 2.1.4)
            2. Exploit pervasive implementation flaw on router
            OR  1. Memory exhaustion
                2. CPU exhaustion
                3. Magic packet (buffer overflow, etc.)
            3. DoS BGP Process (Section 2.1.5)
            4. Exploit routing table memory limitations
            AND 1. Find unfiltered routing distribution point
                2. Send the most specific routes that will be accepted and
                propagated upstream
```

Since this I-D is focused on BGP, this tree elaborates on the routing related portion of the tree. Any of the above listed attack goals are non-trivial and would require extensive coordination and potentially insider involvement.

2.2.2 Force a Multi-homed AS to use an Alternate Path to/from an Outside Network Instead of the Preferred Path

Another way that BGP can be compromised is by forcing a multihomed AS to change the normal path preference. This can result in the entire AS using a suboptimal path, or using links that cost the AS more money. In the extreme case, changing the path preference could cause a link to become oversubscribed and result in the loss of data or control traffic.

Attack:
OR 1. Force traffic from outside network to use alternate path
OR 1. Lower preference of preferred path
OR 1. Change path preference of a prefix (Section 2.1.4)
2. DoS BGP Process (Section 2.1.5)
3. Reset BGP Session (Section 2.1.6)
4. Compromise Router (Appendix A.1)
2. Raise preference of alternate path (Section 2.1.4)
2. Force traffic going to outside network to use alternate path
OR 1. Lower preference of preferred path
OR 1. Change path preference of a prefix (Section 2.1.4)
2. DoS BGP Process (Section 2.1.5)
3. Reset BGP Session (Section 2.1.6)
4. Compromise Router (Appendix A.1)
2. Raise preference of alternate path (Section 2.1.4)

2.2.3 Disable a Single-homed AS

This attack is a smaller scale version of the attack described in Section 2.2.1. Here the adversary need only prevent a single-homed AS from communicating with the rest of the Internet.

Attack:
OR 1. Disable provider link
OR 1. Physical link destruction
2. Social engineering
3. Turn off the link by compromising the upstream router (Appendix A.1)
2. Disable AS via routing protocol attack
OR 1. DoS BGP Process (Section 2.1.5)
2. Reset BGP Session (Section 2.1.6)
3. Compromise router (Appendix A.1)

Any crashes or resets initiated by the adversary in Section 2.2.3.2.1 or .2.2 would usually require the attack be generated continually to prevent the router from reestablishing proper communications with its peer.

2.2.4 Disable a Multi-homed AS

This attack is a combination of Section 2.2.3 and Section 2.2.1. The number of links the AS under attack has with other ASs will dictate the type of attack necessary to most efficiently achieve the adversary's objectives. This attack sequence, in particular, would benefit from further testing through lab simulation and the association of attributes to each of the leaf nodes.

```
Attack:
OR  1. Disable links 1...N (Section 2.2.3)
    2. Disable critical portions of the ASs network (Section 2.2.1)
```

To summarize, the adversary can either consider the attack like disabling several individually connected single-homed ASs, or as a smaller version of the Internet as a whole.

2.2.5 Blackhole Traffic

BGP can be used to blackhole traffic. If an adversary has access to the forwarding path of the target system, he can quietly discard the traffic while continuing to function as a BGP speaker. The adversary could also affect the BGP tables of his neighbors using BGP advertisements so that they would send traffic to the incorrect destination. One way this could be accomplished is through the unauthorized origination of a prefix.

```
Attack:
OR  1. Drop traffic on the wire itself (Section 2.1.4.1.2)
    2. Drop traffic on a router (without using BGP)
    OR  1. Policy route to null
        2. Static route to null
    AND 3. Gain administrative access to the router
        OR  1. Rouge router
            2. Misconfigured router
            3. Compromise router (Appendix A.1)
    3. Drop traffic using bogus BGP messages
    OR  1. Establish unauthorized BGP session with peer (Section 2.1.2)
        2. Originate unauthorized prefix/attribute (Section 2.1.3)
        3. Compromise router (Appendix A.1)
```

3. Testing Considerations

BGP design decisions (such as the selection of TCP as the transport protocol) certainly impact the security of the Internet routing infrastructure. However, operational considerations and the quality of the BGP implementations may have a greater impact on Internet security. Testing (as the ultimate determination of relative difficulty of an attack) is especially critical for threat/ vulnerability analyses that use attack trees. This is because the likelihood, criticality, and access requirements of leaf nodes determine which are the most likely paths through the tree.

As discussed earlier, test procedures and results could be released in a subsequent I-D. Such analysis should be environment specific. For example, the analysis of this attack tree will be fundamentally different for Internet service provider networks and enterprise networks. The same can also be said of the differences in attack methods between a remote blind adversary and a trusted insider. Early findings in this area are available in [VULNTEST].

References

[ATTACKTREE]
Schneier, B., "Attack Trees", December 1999.

[MODELING]
Moore, A., Ellison, R. and R. Linger, "Attack Modeling for Information Security and Survivability", March 2001.

[BGPVULN] Murphy, S., "BGP Security Vulnerabilities Analysis", February 2002.

[GLOSSARY]
Shirey, R., "Internet Security Glossary, RFC 2828", December 1999.

[BGPMD5] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option, RFC 2385", August 1998.

[SEQATTACKS]
Bellovin, S., "Defending Against Sequence Number Attacks, RFC 1948", May 1996.

[RANDOMINC]
SEQATTACKS, T., "The Problem With Random Increments", March 2001.

[BGP] BGP, Y. and T. Li, "A Border Gateway Protocol 4 (BGP-4), RFC 1771", March 1995.

[VULNTEST]
Convery, S. and M. Franz, "BGP Vulnerability Testing: Separating Fact from FUD", June 2003.

Authors' Addresses

Sean Convery
Cisco Systems, Inc.
170 W. Tasman Dr.
San Jose, CA 95134
US

Phone: +1 408 853 8753
EMail: sean@cisco.com

David Cook
Cisco Systems, Inc.
7025 Kit Creek Rd.
Research Triangle Park, NC 27709
US

Phone: +1 919 392-8772
EMail: dacook@cisco.com

Matthew Franz
Cisco Systems, Inc.
12515 Research Blvd.
Austin, TX 78759
US

Phone: +1 512 378 1648
EMail: mfranz@cisco.com

Appendix A. Supporting Atomic Goals

A.1 Compromise Router

Although outside the scope of routing protocol security, if the routers themselves can be compromised the routing infrastructure can be subverted.

```
Attack:
OR  1. Gain physical access to router
    AND 1. Gain physical access to data center
        2. Guess passwords
    OR  3. Perform password recovery
    2. Gain logical access to router
    OR  1. Compromise network manager system
        OR  1. Exploit application layer vulnerability in server
            2. Hijack management traffic
        2. Login to router
        OR  1. Guess password
            2. Sniff password
            3. Hijack management session
            OR 1. Telnet
               2. SSH
               3. SNMP
            4. Social engineering
        3. Exploit implementation flaw in protocol/application in router
        OR  1. Telnet
            2. SSH
            3. SNMP
            4. Proprietary management protocol
```

The ability of an adversary to compromise a BGP speaker is largely dependent on operational best practices: use of secure management protocols and authentication mechanisms, use of intrusion detection systems, etc.

A.2 Denial of Service (DoS) Router

Denial/degradation of service attacks can be conducted against network devices using a variety of well-known techniques.

```
Attack:
OR  1. Physical destruction of router
    2. Link layer attacks
    OR  1. Protocol attack using link layer protocol
        2. Physical link attack
```

```
    3. ARP attacks
    4. IP attacks
    OR  1. ICMP Message
        OR 1. Flooding
           2. Malformed
        2. IP Fragmentation Attack
    5. UDP attacks
    6. TCP attacks
    OR  1. SYN Flood
        2. Connect()
        3. LAST_ACK
        4. New/undiscovered DoS against TCP
    7. Application-Layer DoS
    OR  1. Telnet
        2. SSH
        3. SNMP
        4. Other aplication layer protocol
```

All of these attacks are outside the scope of BGP design or implementation and ultimately depend on the survivability of the routing device itself, its ability withstand attack, and the proper configuration of the device based on published best-practices.

A.3 Intercept or Modify Data Through Man-in-the-Middle (MITM) Attack

Man in the middle attacks against cryptographic protocols or application layer protocols allow an adversary to effectively proxy communication between two parties allowing any data to either be read or altered. Although not impossible to conduct after a session has been established, the attack is easier done prior to session initiation.

```
Attack:
AND 1. Gain write access to network segment of one or more peers
    2. Subvert address infrastructure
    OR  1. ARP/MAC spoofing
        2. DNS spoofing
    3. Proxy BGP sessions between BGP speakers
```

The goals of a MITM attack against BGP are almost identical to a TCP Sequence Number Attack (Appendix A.4) against a BGP session. DNS Spoofing may be unlikely because many implementations/configurations are unlikely to use hostnames in router configurations.

A.4 TCP Sequence Number Attack

TCP suffers from well-known design flaws which make it possible to hijack or terminate applications that use it as their transport protocol. As a blind adversary, these attacks are quite difficult to execute, particularly as they apply to BGP.

```
Attack:
OR  1. Blind Spoofing Attack
    AND  1. Guess sequence number use by a BGP speaker
         2. Inject valid BGP message
    2. Non-Blind Spoofing attack
    AND  1. Sniff Traffic (Appendix A.5)
         2. Inject valid BGP message based on sequence numbers
```

Adequate initial sequence number randomness [SEQATTACKS] should mitigate most blind attacks, although some research [RANDOMINC] suggests blind attacks may be easier that previously thought, all of these attacks require a large sample set of ISNs, something which can be easily mitigated with proper BGP BCPs.

A.5 Sniff Traffic

Depending on the network topology, there are many ways of gaining read-access to a network to conduct passive attacks. The most common method would be to compromise a system (typically a general purpose operating system) on the segment and install software the puts a network interface card in promiscuous mode and captures traffic.

```
Attack:
OR  1. Gain local network access to a segment
    AND  1. Compromise server
         2. Install sniffing software
    2. Tap physical medium
    3. Redirect traffic through a compromised host
```

ARP/MAC spoofing may be necessary to sniff traffic on switched networks and many tools are available which make this a trivial task.

Intellectual Property Statement

Full Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.