MD5 / TCP-AO

MD5 & TCP-AO, as applied to BGP sessions, can spark considerable debate within the R&E community. Both are used to authenticate BGP sessions, ensuring you are brining up the BGP session with the peer you think you mean to. RFC 2385 describes the MD5 technique, while RFC 5925 and 5926 discuss TCP-AO.

Section 5.1 of RFC 7454 discusses MD5 & TCP-AO. It notes that TCP-AO should be used instead of MD5, but that some vendor implementations may make that difficult. It also mentions, briefly, operational concerns of both MD5 & TCP-AO. It ends up suggested that they be used "where appropriate." The debate around the issues usually comes down around four points: TCP-AO is not supported, MD5 is not secure, it's quite difficult to support operationally, and its generally not needed on a point-to-point connection.

Point One: TCP-AO support among the vendors is not as strong as it could be. The Juniper MX series just doesn't support TCP-AO. And nor does Cisco IOS-IOS-XR. Brocade marketing claims support for TCP-AO, but the documentation seems to be lacking. Needless to say, you can't implement the preferred option if it's not supported on your platform.

Point Two: MD5 is no longer secure. Since 2008, there has been some talk that the MD5 hash is no longer secure. Essentially, the argument goes, MD5 hashing has a weakness with collisions, and on top of that is salted and very fast ... traits not always welcome when you're trying to make things hard on attackers. There's even a CERT article on it. Others would argue that MD5 is still a good solution as long as you select a password that's not in rainbow table.

Point Three: Point to Point is pretty secure already. The weakness around MD5 for collisions comes in to play here, in two ways. On a point to point connection there's not much, if any opportunity for someone to intercept you packets. Hash collisions are unlikely when there are only two speakers on the wire, mitigating the risk of using MD5. Which begs the question, if there are only two speakers on the wire then why are you using MD5 anyway?

Point Four: MD5 can be a pain, operationally. The thought of enabling MD5 fills some operations staff with dread. It requires creating and storing, and perhaps even rotating, secure passwords. There's also the very real risk of a session not coming back up; there's more than one anecdote about BGP sessions remaining down after router maintenance because of issues/bugs/etc with the MD5 passwords. Engineers tend to raise their eyebrows when security improvements end up causing downtime. Concerns are also sometimes raised about the CPU-intensive nature of it, as well as "log storms" during transition events. Finally there is a "lowest common denominator" aspect to authentication. Both you and your peer must enable it, and you both must use the same system. A site that has equipment that supports TCP-AO may not be able to use it with most of their peers, because their equipment only supports MD5.

Many people within the community use MD5 authentication and have had little to no trouble, with others reporting concerns. Sites will need to weigh the pros and cons carefully before making a decision. Sites that choose to not implement authentication should seriously consider GTSM as a mechanism to provide increased security for BGP sessions.

Juniper Example

JUNos uses a two-step process where you first define a key-chain, with the password, and then apply that key-chain to the BGP neighbor in question using the authentication-key-chain and authentication-algorithm commands.

```
bgp {
  group ext {
  type external;
  peer-as 65530;
  neighbor 172.16.2.1;
  authentication-key MyReallyAwesomeKey;
  authentication-algorithm md5;
```

Juniper has a pretty good article description their MD5 option. It's a pretty good paper, describing the use case, even if you don't use JUNos.

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/bgp-authentication.html

Cisco Example

Cisco makes the configuration fairly simple, simply noting the password in the config section for the neighbor ... which is then obfuscated in the config.

```
router bgp 65500
 neighbor 192.0.2.1
  remote-as 65555
  password encrypted 123abc
```

Cisco has an article on how to configure MD5 at:

http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/112188-configure-md5-bgp-00.html

Brocade Example

The Brocade configurationis similiar to Cisco, just applying a password to the session which is then obfuscated in the config.

```
router bgp
 local-as 1111
 neighbor 10.10.200.10 remote-as 1
 neighbor 10.10.200.102 password abc12
```

Brocades article on MD5 can be found at:

http://www.brocade.com/content/html/en/configuration-guide/NI_05800a_ROUTING/GUID-EF71FC9F-1410-4DC5-A415-C41B1186D24D.html