Bryce Montano
Project 8 – Responses

1. **BGP hijacking can be used for many nefarious purposes. Briefly detail how a BGP hijack can be used to help accomplish the following goals:**
    a. **Denial of Service Attack**

    A BGP attack could be used to perform a Denial Of Service attack (DOS) in a scenario where a malicious autonomous system (AS) could begin making announcements to neighboring AS's to route traffic through them. Once neighboring AS's begin routing their traffic to the malicious AS, the malicious AS could then forward all of that traffic to a single victim host or victim AS that was completely unaware of (and most likely completely unprepared for) the volume of traffic they are receiving / about to receive. This could easily overload a single host or smaller AS and effectively 'DOS' them.

    b. **Theft of valuable information (credit card accounts, credentials, etc)**

    BGP hijacking could also lead to theft of credit card numbers or bank account credentials in the form of phishing attacks where a malicious AS could begin advertising a shortest path to 'Bank ABC', and then route incoming traffic to a phishing website that may look exactly like the real 'Bank ABC' website, but is indeed fake. Once the user from the victim AS is routed to the malicious website and enters their credentials to login, they have been taken.

    Similarly, in a situation where an online clothing store is having their payment information forwarded to payment merchant system, but is instead forwarding to a malicious AS due to a false route advertisement, the card information could be stolen (of course ignoring that the online clothing store did not encrypt the information and was not using SSL)

    c. **Political / Social protests (Hacktivism)**

    In a situation where BGP might be used as a means of political / social protest, a malicious AS could begin routing traffic from organizations they have deemed the 'enemy' such as financial institutions, governmental organizations, etc. to a website with either a message (V for Vendetta anyone?) or simply routing it with the hopes of one of the outcomes mentioned above.

2. **What is the difference between path and origin attestation? Which would be most effective at preventing the hijack we just demonstrated? Why?**
    a. In Secure BGP (S-BGP), a form of BGP developed to protect against BGP-hijacking, S-BGP employs address attestations (origin attestations) and route attestations (path attestations) to enforce authority of prefix (address or subnet) ownership and validate whether traffic is being routed appropriately. An address attestation is created by the owner of a subnet and is used by routers to verify that the AS that advertised that prefix is indeed allowed to do so (advertise a route) to other destinations. Whereas with route attestations (path attestations), these are added to routers in order to 'authorize' a neighboring AS

to propagate a particular route. Both path and origin attestation is needed in order to effectively combat BGP hijacking, though in the case that we just observed, route attestation would be the best to prevent the attack in this lesson as it would ensure that the malicious AS would be unable to alter a path without proper authorization. (Much of my research on this topic was found in this paper[2])

3. **There are many proposals for securing BGP (BGPSec, S-BGP, etc.), however they are not yet fully deployed. Conduct some of your own research and briefly describe a method that does not require an extension to the existing BGP to detect or prevent BGP hijacking.**

   In order to detect or prevent BGP hijacking without extending existing BGP, I found a great research paper from researchers at Purdue who have proposed mitigation in the form of 'trusted' AS's, residing in a 'hijacking detection system' or environment.

   When the system detects that a particular AS may have bad routing information (detection is performed via fingerprinting, analytics, tools, etc.) it takes action against the infected AS by instructing one of the trusted AS's to either correct or remove the false route in the infected AS and replace with a more attractive route that the system deems as safe [1]. Because ASes in this system trust eachother and are able to validate the actions of one another, an infected AS can allow a trusted AS to purge it's bad routing information.

   Obviously with this type of system, it requires that ASes 'buy into' the idea of an 'ecosystem' of trusted ASes as this type of detection / prevention can only occur with networks voluntarily participating to help combat BGP hijacking.

4. **Consider the AS topology detailed below, in which AS4 attempts to hijack the prefix shown. Which of the ASes in the topology will send traffic bound for a server at address 13.0.0.1 to AS4 instead of AS3? Why?**

   All of the ASes with the exception of AS3 will begin sending their traffic bound for 13.0.0.1 to AS4 as this route, though not immediately known to AS1 and AS2 will eventually propagate to those ASes. This is because, the weight of the edge or distance to 13.0.0.1 that AS4 is advertising is smaller (this is based on the assumption that the weights are the same from the initial part of the assignment) than the legitimate route advertisement at AS3.

References

[1] - Zhang, Zheng, Ying Zhang, and Y. Charlie Hu. *Practical Defenses Against BGP Prefix Hijacking*. N.p., 19 Dec. 2007. Web. 30 Nov. 2016. <http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1365&context=ecetr>.

[2] - Sundaresan, Srikanth, and Vytautas Valancius. *Preventing Attacks on BGP Policies: One Bit Is Enough*. N.p., 2011. Web. <https://smartech.gatech.edu/bitstream/handle/1853/38920/GT-CS-11-07.pdf>.