UConn CSE 5095: Network Security, Fall 2024

HW 5: Routing Security, submit in Husky and [https://bgpsimulator.com](https://bgpsimulator.com/) by Dec. 1st, 11:59pm Prof. Amir Herzberg.

**Luke Pepin**

You will do this assignment using the [https://bgpsimulator.com](https://bgpsimulator.com/) website. You should first register an account and then sign up for our class using the access code: f80747be-be33-4d06-840b-f89c5fa53cb0 , and register using your NetID as the user-name. Be sure to write down the password as the system does not yet support password recovery.

The class has five labs, but you only need to do the first four (labs 1 to 4); the fifth lab is a more challenging version of Lab 4 which you’re welcome to do but are not required to do.

Each of theses ‘labs’ requires you to do an attack and/or defense in a given scenario. The panel on the left allows you to edit the graph, including changing the policy of each AS, and to edit the scenario, i.e., which announcements are announced and which ROAs are defined. In both, there is a ‘simulate’ button which will cause simulation of the current scenario.

Note that when the scenario has multiple non-overlapping prefixes, the simulator only shows the *local RIB* of each AS, i.e., it’s BGP routing table, but cannot visualize packets flows or the status of each AS (attacker success, victim success, or disconnected).

The lab-text button will show you the instructions and the text-editor button will allow you to enter text explaining your submission. Once you are done, click ‘Submit and download’ and save the file; submit all the files in a zip file in Husky. You can select the lab in the top of the right-hand panel (using the arrows or pull-down menu).

IMHO, this simulation system is real nice, and you are encouraged to use it beyond the assignments to understand better BGP routing security. However, this web-interface to the simulator is very new and could have bugs. In particular, the autograding is limited and may have bugs - or simply, you may come up with a solution it will not recognize; and it only grades binary - 0 or 100. We will manually verify failing solutions (esp. if you tell us you believe auto-grading failed).

Note that each student will receive a different scenario (but all of them are equivalently hard).

For your convenience, we repeat here the question (labs). In all of the labs:

* Do not change the topology.
* Use only prefixes of length /8, /16 or /24.
* Provide the ‘minimal’ solutions, e.g., change policies in the minimal number of ASes, include only necessary ASes in the AS path, etc.

**Lab 1**. *In the scenario shown, AS 666 hijacks the subprefix 1.2.3.0/24, i.e., announces it without authorization. As a result, it intercepts traffic from all of the ASes, even AS 1 which adopts ROV. All other ASes run plain BGP.*

*Adopt ROV in exactly one more AS, so that traffic from AS 1, and at least two more ASes, will not be hijacked.*

**Lab 2**. *As shown, the attacker tries to launch a sub-prefix hijack, but this fails to intercept much of the traffic to the announced prefix (1.2/16). Change the announcement made by the attacker so that the attacker will succeed in intercepting traffic from at least two ASes, including AS 11. The attacker should announce only one announcement, and it must be to a /16 or /24 prefix, and have the shortest AS-path which will suffice for the attack.*

**Lab 3**. *As shown, the attacker intercepts traffic from several ASes, including AS 11 which adopts ROV and BGPsec. Adopt ROV, BGPsec and/or ASPA in the minimal number of ASes to prevent the interception of traffic from AS 11; as a secondary goal, try to minimize interception from other ASes too, but without changing policies in more ASes.*

**Lab 4**. *This question explores a routing attack against the Tor anonymous network service, where traffic is anonymized by forwarding it via multiple "onionrouters", where communication between onion-routers is protected by TLS. Tor can be deanonymized by an attacker that can eavesdrop on the traffic and observe traffic patterns.*

*For the question, consider an attacker (AS 666) whose goal is to eavesdrop (or, become MitM) on the communication between two Tor onion-routers (ORs): OR A at IP 5.6.7.8 and OR B at IP 1.2.3.4. OR A is in prefix 5.6.7.0/24 announced by AS 11 and OR B is in prefix 1.2.0.0/16 announced by AS 777.*

*In this version of the lab, we show part of the attack, specifically, we show how the attacker is able to become a MitM to the traffic from OR B to OR A. The attacker achieves this by announcing (5.6.7.0/16, 666-1-11). This is an origin hijack, allowing it to intercept traffic from AS 777 (via ASes 2 and then 5), but with a twist. The twist is that AS 666 included also AS 1 in the AS path. As a result, when this announcement reaches AS 1, then AS 1 will drop it due to the BGP loop-prevention mechanism. As a result, AS 666 can send packets to OR A by sending them to AS 1, who forwards them to AS 11 (and OR A). This technique of including ASes in the AS-path in order to cause the announcement to be ignored by these ASes is called path poisoning, and can be used for attacks (and sometimes for legitimate purposes).*

*Your task is to complete the attack, allowing the attacker to similarly eavesdrop (in fact, become MitM) to traffic from OR A to OR B. Namely, the complete attack would allow AS 666 to: 1. Intercept traffic sent by OR B (at IP 1.2.3.4) to OR A (at IP 5.6.7.8). 2. Send to one of its neighbors packets with source IP of OR B (1.2.3.4), so that they would reach OR A (at IP 5.6.7.8). (For the attack against Tor, these would typically be the intercepted packets, since TLS authenticates the communication.) 3. Intercept traffic sent by OR A (at IP 5.6.7.8) to OR B (at IP 1.2.3.4) 4. Send to one of its neighbors packets with source IP of OR A (5.6.7.8), so that they would reach OR B (at IP 1.2.3.4). (For this attack, these would typically be the intercepted packets, since TLS authenticates the communication.)*

*Note that tasks 1 and 2 are already achieved by this version of the lab, i.e., you just need to leave this part of the attack as-is. If you want, there’s a harder, ‘no-hint’ version of this lab, where you need to find the complete attack; that lab is not mandatory.*

*Your attack should not require AS 666 to send any announcement to only some of its providers, i.e., any announcement that AS 666 originates as part of the attack and sends to one provider, should be sent to all of its providers. Also, keep the attack as simple as possible: no unnecessary announcements or unnecessary ASes in an AS-path.*

*Note: the auto-grading may give a grade of 0 to partially-correct answers,*

*e.g., if you include some ASes in the AS path unnecessarily, and maybe even to a fully correct answer that we did not anticipate, or due to a bug. Don’t worry; we will grade your answers manually and give partial credit.*