CS5321 Network Security, National University of Singapore
- Semester 2: AY2022/2023 -
Due: 11:59 PM (Singapore Time) on 24 April 2022 (Monday) **[FIRM]**

Take-home Exam 2

Answer to all of the following questions. The answers must be **typed** and uploaded in **PDF** format to "Exam 2" folder on CANVAS before the deadline. (**Late submission is NOT allowed. Missing the deadline results in 0 point.**) Make sure to include your name and ID number on the **FIRST** page of the PDF and name your submission file **"[ID]_[NAME].pdf"**. **Open book. No collaboration is allowed.**

Part 1: BGP Security [20 points]

(a) Let us consider network shown in Figure 1, which does not implement RPKI or BGPSEC. A to F are autonomous systems (ASes) that have customer-provider relationship as shown (Arrows are pointing providers, and they are not necessarily indicating the direction of flows). Now we consider a case where a device in F is sending a packet to a device with prefix P. Relevant routing advertisements are also shown on the figure. Let us consider a case where a malicious AS M mounts "invalid next-hop" attack to mount prefix hijacking attack against a traffic from F to P. Assuming that the route selection at each AS is solely done based on local preference (preference is on customer routes, followed by provider route) as the first priority, followed by AS path length. What route advertisement is given to F from E after M starts attack, and why it is so? Also discuss if hijacking attack is successful (i.e., M can receive traffic from F to P).

(b) M additionally becomes a customer of AS D as seen in Figure 2. M sends fake route advertisement to mount "invalid next-hop" attack. Can M successfully hijack the traffic from F to P? Please further discuss if M can be successful in mounting interception attack (i.e., forwarding the hijacked traffic to the intended destination, P).

(c) To add message integrity to the plain BGP messages, Alice proposes to sign all the BGP update messages as shown in Figure 3 and calls it BGP+. Unfortunately, BGP+ does not counter AS path manipulation. Please explain why and show an example attack. You can assume global RPKI.

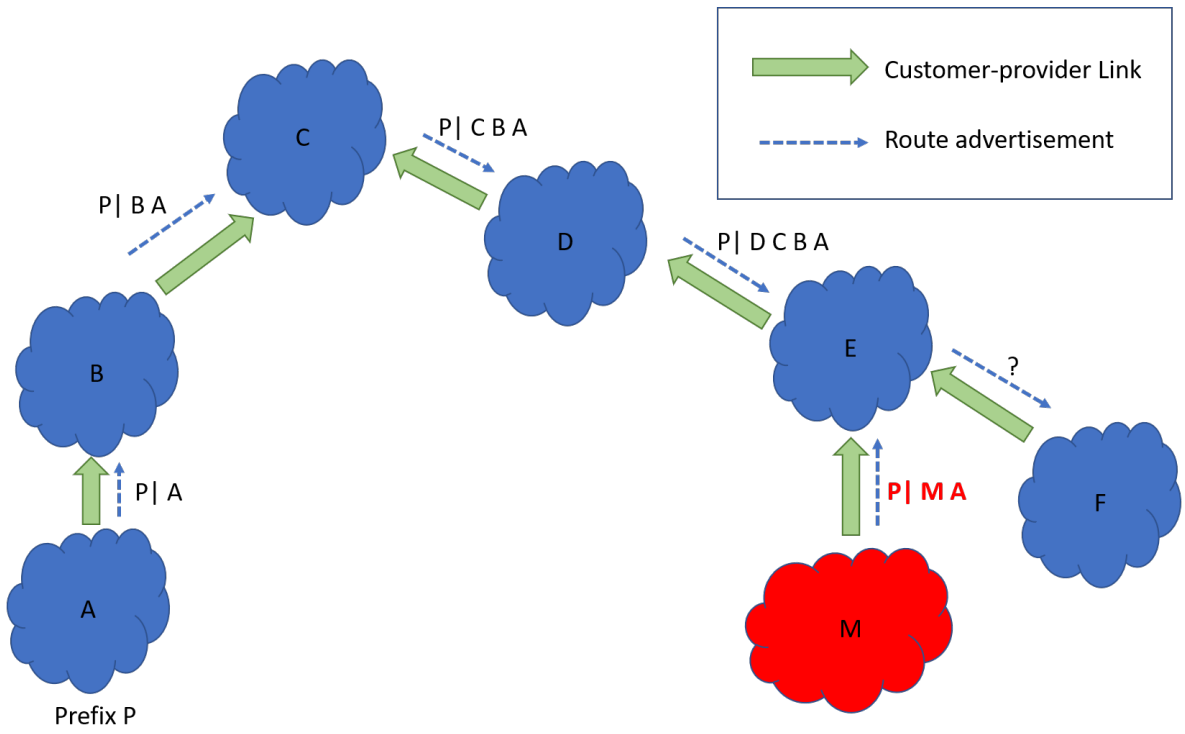

Figure 1: BGP topology (1)

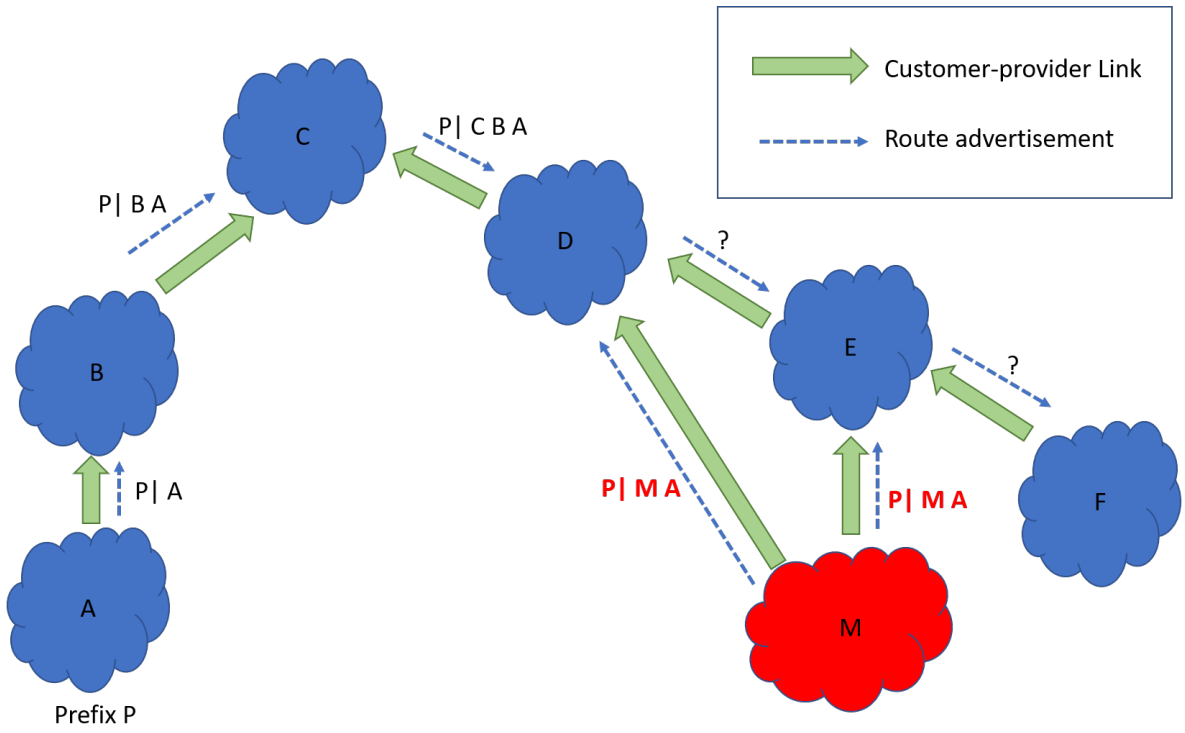

Figure 2: BGP topology (2)

(d) Knowing an issue of BGP+, Bob proposed BGP++ that forces parties to include all the signed update message from its upstream (see Figure 4).

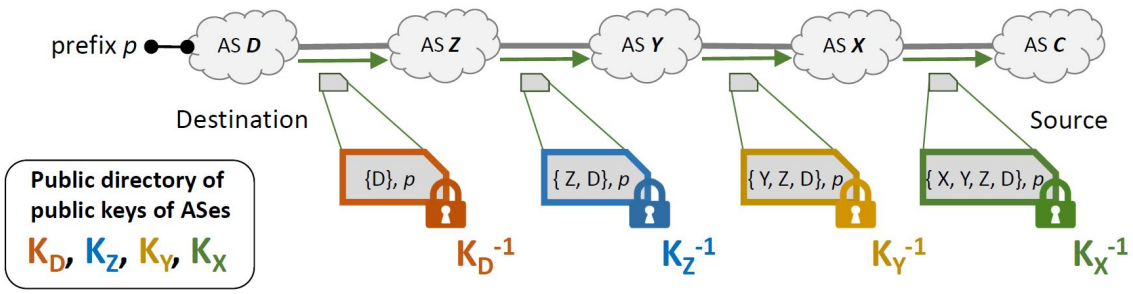

Figure 3: BGP+

Does this counter AS path manipulation? Please explain why. Again you can assume global RPKI and no replay attack.

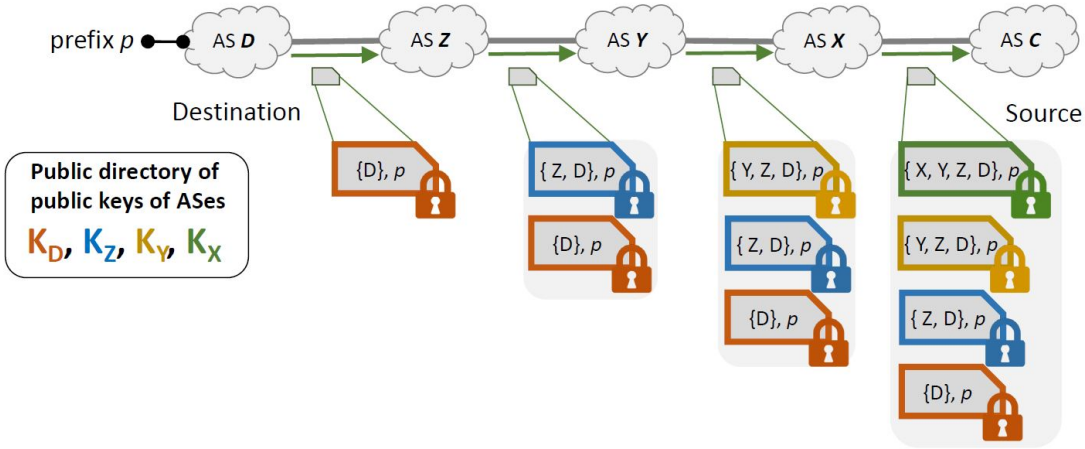

Figure 4: BGP++

Part 2: DNS Security [10 points]

1. Current DNS-over-HTTPS services are predominantly provided by a small number of large cloud providers, such as Google and Cloudflare. There is a good security reason why large cloud providers are more appropriate for DoH resolvers compared to small cloud providers. What is the reason? (up to 3 bullets)

Part 3: DoS Attack [20 points]

1. SIFF assumes that all routers are benign. Consider the following end-to-end routes between C and S. Assume that R1, . . . , R6 are the only routers that

support SIFF between C and S. Calculate the expected number of attack traffic rate (in terms of packets per second) to reach 1 million packets per second (using DTA packets with forged capability) at the target destination. Consider 4 bits per router marking and 3 markings in router's time window. Please show calculation and reasoning.

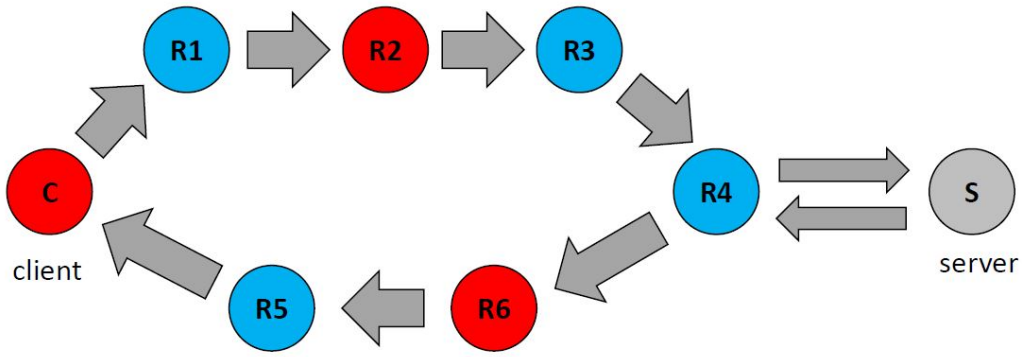

Figure 5: End-to-end route between C and S

(a) R2 colludes with the adversary C.

(b) R6 colludes with the adversary C.

2. Recall Crossfire attack we studied in the lecture.

   (a) Instead of the sophisticated Crossfire attacks, Alice decides to send attack traffic from distributed botnets to the IP addresses of a small number of targeted routers (e.g., backbone routers). Is this attack effective and persistent? Briefly explain your answer.

   (b) Worried about the Crossfire attacks, NUS IT admins have decided to drop, at the gateway of NUS network, any IP packets (whose destination is any server in the NUS network) that are involved in *traceroute* measurements. Would it be an effective countermeasure against the Crossfire attacks? Briefly explain your answer.

Part 4: Anonymous Communication [10 points]

1. One of the drawbacks of Tor is end-to-end latency. As studied in the class, Tor selects relays at random. Thus, for instance, a packet leaving NUS may travel three relays in Canada, Australia, and Germany to eventually reach Facebook server in the US. To improve the situation, *Tor+* (hypothetical) is proposed to optimize relay selection algorithm at each Tor Proxy to choose

relays that minimize the latency. As the result, Tor+ client may carefully choose three relays in Hong Kong, Tokyo, and San Francisco to attain shorter latency. Is this relay selection algorithm as secure as the random selection? Please explain in a few sentences.

Part 5: Anti-censorship [20 points]

To help people in Dictatopia access some censored websites, a large-scale cloud provider Cloudburst decides to build a new anti-censorship system. The idea is simple. Cloudburst installs a anti-censorship proxy within its data center (which hosts many websites) and lets it relay all the HTTPS session initiations of all the hosted websites. If a user in Dictatopia embeds a certain tag that can be visible only to the Cloudburst's proxy (e.g., similar to the Telex's tag), the proxy fetches the tag and redirects its session to the user-intended website (which is blacklisted by Dictatopia). Then, the proxy hijacks the HTTPS session and starts forwarding all packets to the user-intended server, similarly to Telex.

In this exam question, please assume that all the blacklisted websites are hosted by Cloudburst. Also, there's no political pushback from Dictatopia (e.g., accusing Cloudburst of undermining Dictatopia's authority over its own citizens).

1. What is the expected vulnerability of this anti-censorship system, which could allow Dictatopia censors identity who is accessing blacklisted websites? (Discuss up to 2 vulnerabilities.)

2. Please discuss solution(s) to the identified vulnerability (with a few sentences for each).

Part 6: Blockchain Security [20 points]

1. Assume that there are 10,000 Bitcoin nodes in the network and 2,000 of them are controlled by an adversary. Also assume that there are 1,000 Tor exit nodes and 100 of them belong to the adversary. The attacker targets a Bitcoin client that is exclusively connected over Tor. The attack is said to be successful if all eight outgoing connections of the victim goes through an adversarial Tor exit or Bitcoin node (or both). Given that when the victim makes an outgoing connection over Tor, it picks a random Tor exit and a random Bitcoin node in the network. Calculate the probability that the attack is successful without any additional action from the attacker.

2. In class, we discussed Eclipse attack, BTC-hijacking attack (paper by Apostolaki et al.) and Erebus attack (paper by Tran et al.). For each of the following hypothetical scenarios, can the mentioned Bitcoin node/client be attacked using any of attack strategies (YES/NO)? If the answer is YES, please list attacks that work and why (with 1 sentence fir each). If the answer is NO, for each of the three attacks, state 1 sentence to explain why it does not work.

   Notes: Unless otherwise stated, the Bitcoin nodes/clients run Bitcoin Core of the latest version.

   (a) A cryptocurrency exchange runs a node on AWS that has a public IP address belongs to a /24 prefix.

   (b) Alice uses a client version 0.9.3 and connects to Bitcoin network via a VPN.

   (c) After the Blockchain Security lecture, a CS5321 student decides to run a node and mine Bitcoin for one month (1st March - 31th March 2023) since the student happens to have a powerful PC and a public IP address belong to a /23 prefix. The student is also aware of BGP hijacking attacks and hence, regularly checks BGPMon (a BGP hijacking monitor) to see if the node is being attacked.