CS5321 Network Security, National University of Singapore
- Semester 2: AY2022/2023 -
Due: 11:59 PM (Singapore Time) on 24 April 2023 (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).

[5points]

Hijack can be successful, After M begins an attack, E gives F the route advertisement, which is $P|EMA$. Since the malicious route advertised by E is also less expensive than the legitimate route via D, the hijacking attack will be successful.

[-2pt] Say unsucessful but explained about $P|EMA$, route advertisement

(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

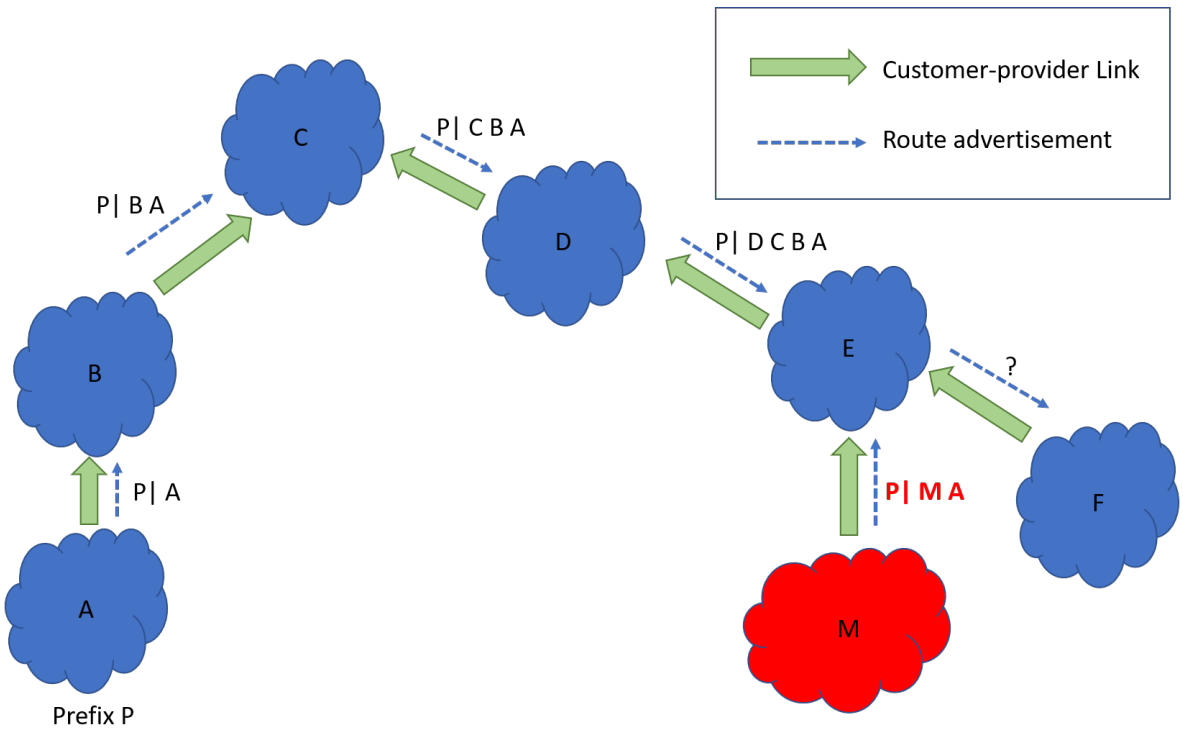

Figure 1: BGP topology (1)

be successful in mounting interception attack (i.e., forwarding the hijacked traffic to the intended destination, P).

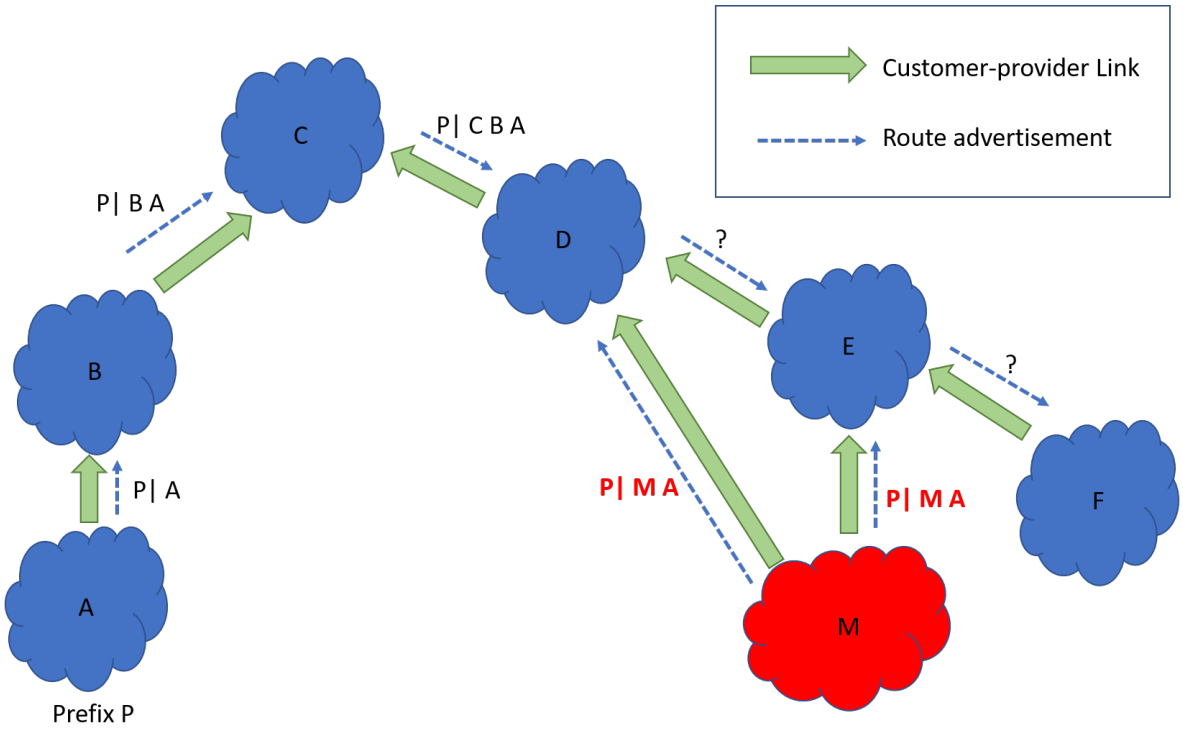

Figure 2: BGP topology (2)

[5points]

M can successfully hijack the traffic from F to P since the malicious route via M will be cheaper than the valid route via D. However, M cannot be successful in mounting an interception attack. This is because M can only choose either AS E or AS D as next hop to forward the packets to P. However, both the ASes will end up choosing the invalid route advertised by M. Hence, interception is not possible.

[-2pt] Answers both unsuccessful.

(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.

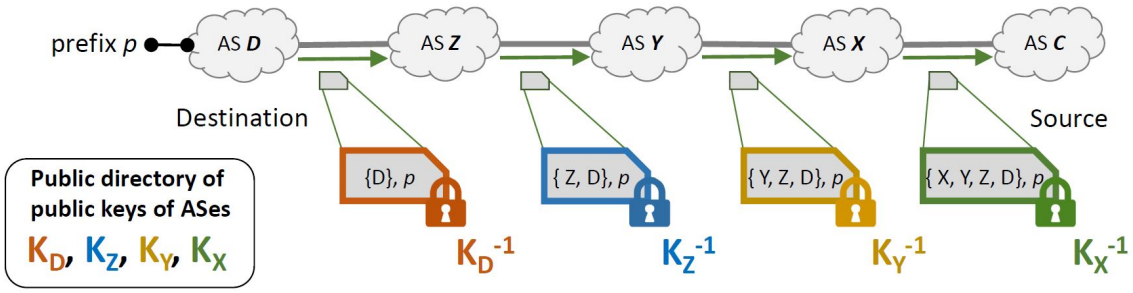

Figure 3: BGP+

[5points]

BGP+ only protects authenticity (and integrity) of BGP messages. While it is effective to counter manipulation on network, it does not prevent malicious router from sending out fake path information. For instance, a malicious AS M can announce {M, D}, p signed with its private key. Note that, because of RPKI, M cannot announce M, p.

[-2pt] Does not say BGP+ is only for authenticity of BGP message.

[-2pt] Does not discuss any example attack.

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

[5points]

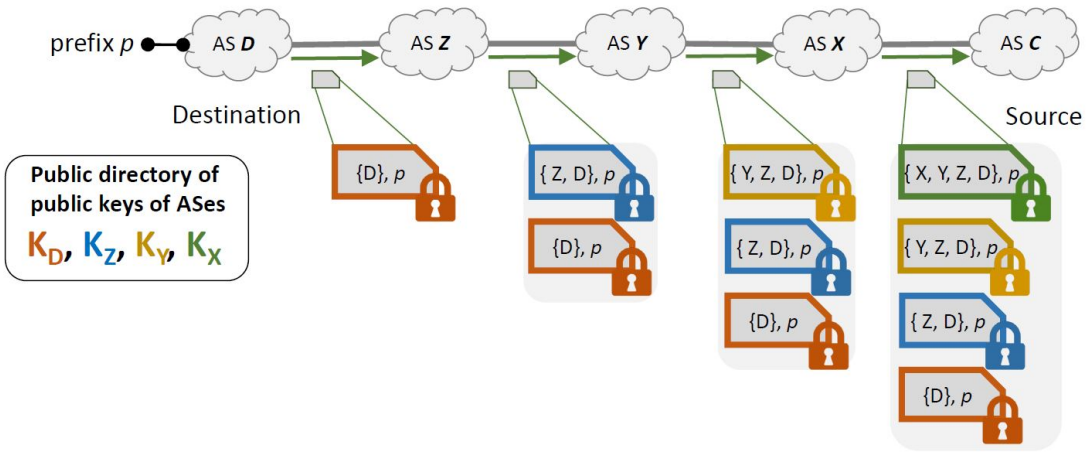

Figure 4: BGP++

No, BGP++ does not yet solve the security issue. BGP++ is sending concatenation of signatures, but there is no verifiable tie between signatures. To mount next-AS attack, a malicious AS M could send {M, D}, p signed with its private key along with {D}, p and signature on it, which can be obtained elsewhere. Note that {D}, p is distributed publicly and thus it is not difficult for M to obtain it even if it is not located near D.

[0pt] Answers Yes.

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)

   Using a DoH service provided by a large cloud provider makes filtering (i.e., dropping) DoH packets difficult. DoH packets can be highly indistinguishable from other HTTPS packets. Thus, when DoH packets are mixed with other HTTPS packets to/from a large cloud provider, it is hard to filter them because of potential collateral damage (e.g., you don't want to block all your Google or Amazon traffic!). However, when DoH is served by a small DoH special vendor, the local ISP can simply filter out all the encrypted packets going to/coming from the small DoH vendor address(es) without the risk of collateral damage.

Another reason why DoH is implemented by large cloud resolvers could be availability and reachability of DoH resolvers. Large cloud providers like Google, Cloudflare etc. will have enough resolvers and servers to provide continued services to users if some resolvers get attacked. DNS services offered by large cloud providers will not get disrupted if an attack like DDoS is launched against some of the DNS resolvers.

[-3pt] No mention about collateral damage by simply filtering out.

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.

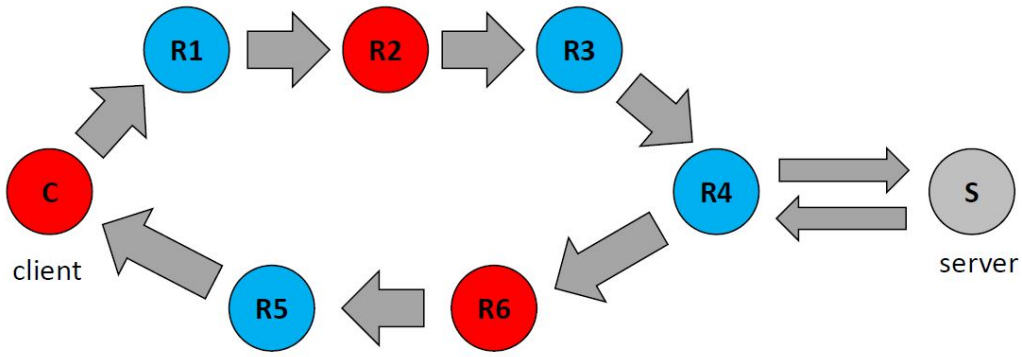

Figure 5: End-to-end route between C and S

(a) R2 colludes with the adversary C.

[5points]

The probability that a randomly guessed capability will pass a particular router is given by: $P(x,z) = 1-(1-\frac{1}{2^z}))^x$. where z is the number of bits per router mark and x is the number of markings per router window. Then the probability of passing d routers is given by $P(x,z)^d$.

In the given SIFF architecture, the path from C to S is $C \rightarrow R1 \rightarrow R2 \rightarrow R3 \rightarrow R4 \rightarrow S$. If R2 colludes with the adversary C, then C does not

need to forge capability for R2. Note that marking of R1 is known to R2 and thus C does not have to guess. Thus, C needs to forge the marking of R3 and R4. Probability that a randomly guessed capability will pass a router can be calculated as: $P(x, z) = 1 - (1 - \frac{1}{2^4}))^3 = 0.17602539062$
Then, the probability passing 2 routers is: $0.17602539062^2 = 0.03098493814$
Then, the expected attack traffic rate (in terms of packet/sec) to reach 1 million packets at the server can be given as: $1,000,000/0.03098493814 = 32,273,745$ (packets/sec).
[-1 to -3pt] Based on correct usage of formula and procedure to calculate.

(b) R6 colludes with the adversary C.
[5points]
If R6 colludes with adversary C, it might not be able to help C to forge capability in the DTA packets since the path from C to S does not contain R6. Hence, C would have to guess the capability for all the routers in the path. There are 4 routers in the path from C to S. The probability that a forged capability will pass one router is 0.1760253906 as calculated above, and the probability to pass 4 routers is $0.1760253906^4 = 0.0009600664$.
Expected attack traffic rate = 1,000,000/0.0009600664 = 1,041,594,623 (packets/sec).
[-1 to -3pt] Based on correct usage of formula and procedure to calculate.

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.
[5points]
No. This attack would not be effective or persistent. Basically no legitimate traffic is sent to the core /backbone router IP address, and thus such direct flooding attacks can be trivially distinguished from legitimate traffic and filtered. Besides, unlike Crossfire attack, Alice cannot change targets to make the attack persistent.
[-2pt] Wrong argument either in effectiveness or persistence.

(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.

[5points]

No. Blocking traceroute measurements at the NUS gateway only preventing the outsiders from measuring the complete paths to the NUS server IP addresses. However, the complete paths are not necessary for the attackers because (1) NUS is not a transit ISP, its network resources are not the targets of the Crossfire attacks, and (2) learning the paths from bots to NUS gateway is already enough to attack the larger area that covers NUS. Besides, this countermeasure would not allow even a benign person to send traceroute measurements to the NUS network.

[-2pt] Answers Yes, but with partially correct argument.

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.

   No, it's not as secure as TOR. Because they can also utilize the route optimization to select a small number of highly likely relays for the connection, adversaries may be able to predict the relays that may be used for a given session between a Tor+ client and a website. This creates numerous new attack avenues for traffic analysis. Contrarily, it is exceedingly challenging for an opponent to determine which way is utilized for anonymous communication because TOR chooses relay at random.

   [-3pt no explicit mention about predictability of Tor relays to be selected.]

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.)

   [10points]

   Dictatopia can still monitor the traffic pattern (e.g., packet sizes, inter-packet delays) to detect whether its citizen is visiting a blacklisted website or not. This is possible because different websites have largely different traffic patterns due to their different contents and usage patterns.

   [-3pt]No mention about traffic analysis

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

   [10points]

   Let us consider two websites, NotBlocked.com (not blocked by censor) and Blocked.com (blocked by censor). To combat traffic analysis, the anticensorship proxy can try to mimic the response of NotBlocked.com while delivering the response of Blocked.com to the user. For example, for every request made by a user to Blocked.com, the Cloudburst proxy can send a request to NotBlocked.com and use its response characteristics to shape the response packet from Blocked.com. For instance, the packet size and timing of Blocked.com's reply can be matched with the packet size and timing of the response from NotBlocked.com. In this manner, it will become difficult for the censor to analyze the traffic and distinguish packets between

Blocked.com and NotBlocked.com.

[-3pt]No mention about countermeasures against traffic analysis

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.

   [5points]

   Probability of adversary naturally controls one connection is: p = 1-(1-2000/10000)*(1-100/1000) = 0.28.

   Then, the probability to control 8 connections is $(0.28)^8 = 0.00003778$

   [3pt]The probability for a single connection is calculated correctly.

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.

   [5points]

   Eclipse Attack: No. It is not effective against the latest version of Bitcoin Core.

   BTC-hijacking: No, /24 prefix is not hijackable in general.

Erebus attack: Yes. It is vulnerable to the Erebus attack because the node has a public IP, and the question doesn't restrict attack execution time.

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

[5points]

Eclipse Attack: No. The node is behind VPN.

BTC-hijacking: No. The attacker does not know the IP of the node (i.e., which AS it is in). Note that VPN service allows to choose different servers easily.

Erebus attack: No. The node does not have public IP.

(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.

[5points]

Eclipse Attack: No. The node runs the latest version of Bitcoin Core.

BTC-hijacking: Yes. Prefix is hijackable. Also the monitor help detect hijacking but not prevent it.

Erebus attack: No. Erebus attack doesn't work because 1 month of attack execution is not enough.

[-2pt] Wrong reason for some attacks.

[-3pt] Overall YES/NO is wrong, but with some valid answer to any of the attacks. ("Overall" means whether any attack works or not.)

[0pt] Regardless overall Yes/No is correct, all reasonings are wrong.