ITIS 6167/8167: Network Security
Homework 2

Student Name: Sireesha Ponnaganti
Student ID: 801310488
Student Email : sponnaga@uncc.edu

Question 1

Delay-Bandwidth Product is a concept that may impact the performance of TCP. If you have a very fast line with very long delay, the amount of traffic that is "on the road" could be much larger than the TCP receiver's window. In this question, you need to:

(1) Read the page about Delay-Bandwidth Product and TCP tuning in the document.

(2) The satellite communication between Earth and Mars has the bandwidth of 256Kbps. The transmission delay is about 13 minutes, 48 seconds. If NASA decides to use TCP for data transmission, does it need to enable TCP Tuning option? Why?

(3) Bonus question: Do you think it is a smart decision to use TCP for data transmission between Earth and Mars? Please explain your answer.

Answer:

Yes, TCP tuning must be enabled. Higher bandwidth delay products need for larger buffer sizes. Depending on the chosen maximum transmission unit of each interface, buffers are divided into several sizes. The likelihood of synchronization may be reduced if there are mass TCP microflows because of the unpredictable arrival of TCP sessions. So, a larger buffer size is required.

Since there are numerous methods for increasing the buffer size, the size of the buffer can be increased using any one of the approaches. TCP tuning approach can be used to accomplish this. Transmission Control Protocol (TCP) tuning strategies modify the network congestion avoidance settings of TCP connections across high-bandwidth, high-latency networks.

Considering the 256 Kbps bandwidth of the satellite communication between Earth and Mars, it takes 13 minute, 48 second transmission delay.

Data rate, bandwidth (c) = 256 Kb/sec

Round trip time delay (RTT) = 13 minutes 48 seconds
= 828 seconds

Bandwidth delay product (W) = c * RTT
= 256 Kb/sec * 828 sec
= 211928 Kb
= 26.491 MB.

Therefore, the window has a size of **26.491 MegaBytes.**

(3) Bonus Question Answer:

No. Using TCP for data transfer between Earth and Mars is not a smart idea. TCP/IP needs an end-to-end routing of routers to send data packets across links like copper or fiber optic cables, or cellular data networks, in order to transfer data over the internet on Earth. Because the cost of memory in the early 1970s made data storage on the Internet impractical.

Therefore, if a path link fails, a router discards the packet and resends it from the source. In the low-delay, high-connectivity environment of Earth, this works beautifully. Networks in space, however, are more susceptible to interruptions, necessitating a different strategy.

Consequently, researchers developed bundled methods. The disruption/delay-tolerant networking (DTN) protocol known as bundling has the power to truly take the internet to the stars. Bundling uses packet switching, just like the internet protocols used on Earth. As a result, data packets flow along the network's path from source to destination via routers that change their direction of motion. Bundling, however, offers features that the terrestrial internet does not, such as nodes that can store data.

Question 2

Please write a half-page summary to explain the Off-path Attack on TCP based on the slides and paper of Week 6. Please explain how the attacker turns two security measures into an attack.

Answer:

Latest data suggests that TCP as well as network stacks are capable of leaking a wide variety of data to an unnoticed off-path attacker via side channels. However, without being present on the communication channel, the adversary cannot simply ascertain whether any two arbitrary hosts also on Network are using a TCP connection.

A connection between arbitrary hosts cannot be interfered with or terminated by an off-path attacker. The "TCP sequence number inference attack," which can be carried out by an off-path attacker, was defined by Qian et al. in 2012. However, in order for the off-path attacker to be assisted by the assault, unprivileged malware must be running on the client; this greatly restricts the attack's potential reach. In 2014, Knockel et al. found a side channel that enables an off-path attacker to track the number of packets sent between any two hosts.

The quick off-course attack which is to check if any two arbitrary Internet hosts are connected through a TCP connection and perform Packet sequence numeric inference, which allows the attacker to later force the communication to end or encrypt the connection with a malicious payload.

The vulnerability is primarily caused by the presence of issue ACK replies and the global rate limitation applied to some TCP control packets. The feature is described in RFC 5961.

At a high level, the flaw enables an attacker to deliver fake packets that can clog a shared resource, in this case the target system's global rate limit counter. The attacker can however keep an eye on the counter's adjustments, which probing packets can spot.

The three hosts in action are an off-path attacker, a victim client, and a victim server. Any computer can assume the role of the attacker in this scenario if its ISP permits the off-path hacker to send packets towards the server with both the victim's fake IP address. The attack's main goal is to quickly and precisely perform the timestamp inference and then use it to

resets an active connection. The faster the attack is successful, the greater the DoS effect.

However, there are two practical constraints that limit the amount of impact there will be. There may be a limit on the bandwidth available between the hacker and the victim. It is possible for packets to get lost between the hacker and the victim, particularly if they are far apart.

Question 3

In SDN networks, attackers can use the "modify field" rules to bypass some security measures such as Firewall. In the Fort NOX slides (Week 10, slides 4), we introduce the Dynamic Flow Tunneling attack.

(1) Please use your own words to describe the attack.

(2) The rules in SDN networks support Wild Card address mapping (e.g., 125.7.10.*). Please discuss how this issue will impact the Fort NOX approach, in which all address substitution possibilities need to be included in the new rule.

Answer:

(1) Dynamic flow tunneling is depicted in the image with below three hosts, actually A part switcher, and an Off control. There is a firewall in use, and one of its rules forbids network traffic from the external host 10.0.0.2 to the internal host 10.0.0.4's web service (Port 80).

Assume that a different OF application updates the OF controller with three new flow control that are connected by GOTO TABLE instructions. If a packet is sent from 10.0.0.2 to 10.0.0.3, the first rule changes the packet's origin IP address to 10.0.0.1. (Port 80). The second rule switches the IP address of the target to 10.0.0.4 if a packet is sent from 10.0.0.1 to 10.0.0.3. (Port 80). Only a message from 10.0.0.1 to 10.0.0.4 may be routed at port 80 according to the final rule.

As a result, the firewall won't be activated if host 10.0.0.2 transmits a packet to host 10.0.0.3's port 80 instead of directly to host 10.0.0.4. The OF control system will finally send this message to the address 10.0.0.4 even if a firewall is preventing this traffic. By just implementing an a Few flow rules, it demonstrates how to easily get around a present firewall. Although this example is straightforward, the true task is to ensure that all OF controllers apps don't violate security standards in sizable real-world network with

numerous OF switches, a range of OF programs, and complex security policies. It is obvious that conducting this type of process manually would be challenging and error-prone.

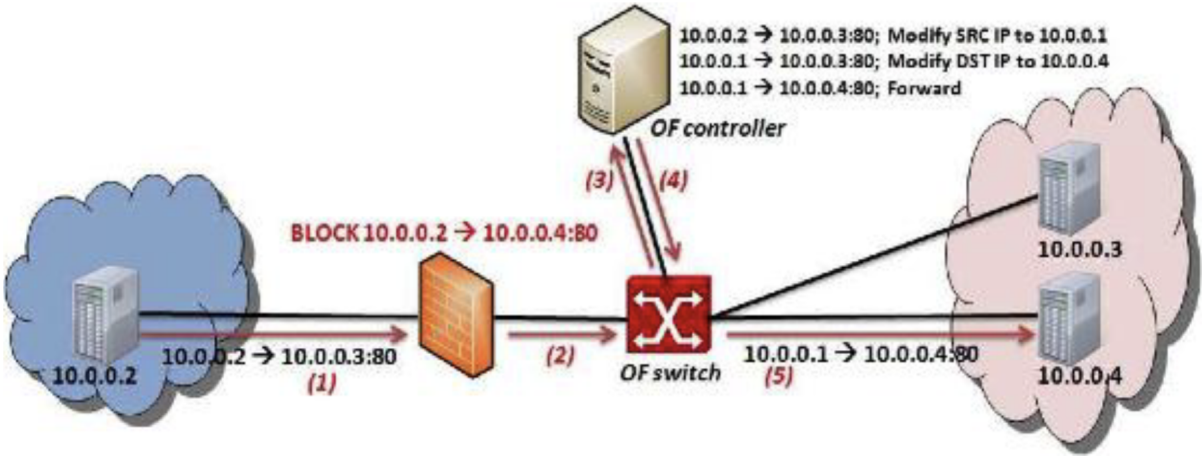

Figure : Dynamic Flow Tunneling

(2) Transforming all rules, such as the applicant rule, into alias reduction rules (ARRs), then run the issue analysis on these ARRs to determine whether there is a difference between a newly added nominee OpenFlow policy and the existing OpenFlow rule set. An alias reduced rule, in its simplest form, is a flow rule that has had its check criteria expressly enlarged to also include set operations transformations and wildcards. An first alias set is created using the IP addresses, connection masks, and routes listed in the first rule. If the rule's action leads to the replacement of a field through a set action, the ensuing value is attached to the term set and used to remove the predicate component of the ARR. The possible ARR is then put up against a group of ARRs that represent the present rule set in a pairwise comparison.

The union of the origin and address sets is used as the synonym set for the following rule if the origin and address sets intersect. On the candidate rule, FortNOX first reduces the alias set of rules. The prospective ARR cRule and the group of ARRs fRule expressing the current flow rules are then subjected to these validity checks, such as, cRule/fRule pairs with mismatched prototypes should be avoided. If a cRule/fRule pair both

forwards or drops a packet, ignore it. Declare a conflict if the alias sets of cRule and fRule cross.

The first potential rule satisfies the first two criteria, presuming both regulations are Tcp / ip network rules. However, the candidate rule is deemed to be in dispute for the third check because the overlap of the source and target alias sets produced (a) and (b), respectively. Because IP address network masks and wildcard field matching are both permitted by OpenFlow rules, identifying an alias set intersection needs more than just a simple membership equality test.

References:

Tutorials point (2019, June 30). Bandwidth Delay Product. https://www.tutorialspoint.com/bandwidth-delay-product

Cloud Architecture Center (2019, March 11). TCP Optimisation for network performance.https://cloud.google.com/architecture/tcp-optimization-for-network-performance-in-gcp-and-hybrid

TCP-Planet(n.d). TCP-Planet: A Reliable Transport Protocol for InterPlaNetary Internet. https://sites.cs.ucsb.edu/~ebelding/courses/284/s07/papers/TCP-Planet.pdf

CloudFare(n.d). Outline methods to protect against on-path attackers. https://www.cloudflare.com/learning/security/threats/on-path-attack/

Usenix(n.d). OFF path TCP Exploits:Global Rate Limit Considered Dangerous. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/cao

IEEEXplore(2021, October 1). Off-path TCP Hijacking Attacks. https://ieeexplore.ieee.org/document/9556515

Juniper(n.d). Security Services Administration Guide. https://www.juniper.net/documentation/us/en/software/junos/security-services/topics/task/ipsec-dynamic-endpoint-tunneling-solutions.html

FortNoxHotSDN(n.d). A Security Enforcement Kernel for OpenFlow Networks https://people.engr.tamu.edu/guofei/paper/FortNOX-HotSDN12.pdf

ProQuest(2014, December). OpenFlow Security Threat Detection. https://www.proquest.com/openview/fdd7f7bf04273ad1ebabfec9945856ad/1?pq-origsite=gscholar&cbl=886380