UNIVERSITI SAINS MALAYSIA

CMT321
MANAGEMENT & ENGINEERING OF DATABASES
SEMESTER I 2022/2023

Assignment 1

For the attention of
Dr. Suzi Iryanti Binti Fadilah

Name	Matric Number	USM Email Address
TAN PEI YONG	152900	peiyong@student.usm.my

Submission Date : 19 December 2022

TABLE OF CONTENT

PART 1: TWITTER

1.1 Introduction

Social networking sites (SNS) are becoming an important component of contemporary social interaction as a result of the social media industry's fast development and expansion. It has altered how individuals communicate and interact with others. It provides a platform for individuals to showcase their individual profiles, share information, images and experiences with others online as well as establish and maintain connections with others. The main driver that contributes to the popularisation of SNS is establishing, fostering and maintaining social connections by making with new people, keeping in touch with friends and general socializing. (Brandtzaeg & Heim, 2009). The two most popular SNS, Twitter and Facebook will be compared in this topic.

Twitter, which was launched in 2006, is a microblogging site for users to share a limited 140 characters of status update for every tweet to their followers. Users can participate in conversations using mentions, replies and hashtags in Twitter (Stec, 2015). As a platform for communication, Twitter enables the unrestricted exchange of opinions between individuals interested in related fields of knowledge both domestically and internationally. It also gives users the chance to join in spirited discussion. Therefore, Twitter is becoming popular and there are about 396.5 million registered users with over 206 million daily active users for Twitter currently. (Dean, 2022).

Facebook, which was launched in 2004, is a well-known SNS for individuals to establish and maintain connections with their friends, family and acquaintances. It enables individuals to publish their details such as their job, political and religious opinions and their personal interests by creating their personal profile with their friends. Additionally, Facebook also acts as a platform for users to communicate with others privately and publicly as well as real-time instant messaging. All these

functionalities contribute to the popularity of Facebook and thus currently Facebook possesses 1.9 billion daily active users and 2.9 million monthly active users currently. (Dean, 2022).

1.2 Comparison between Twitter and Facebook

There are some key distinctions between Twitter and Facebook. Both Twitter and Facebook allow individuals to share their opinions on different issues, but there is one key distinction which is the restriction on character. Twitter users has the restrictions on word count. They only have up to 140 characters in sharing their opinions. This presents a problem as the users must present their opinions concisely and consistently while using fewer words. Hence, this is quite challenging for some people to fully share their opinions. However, the content for Twitter is usually clear and bold due to its limitation of words. On the contrary, Facebook users do not have any restrictions on the number of characters or words they can use. Their opinions do not need to be shortened and simplified into 140 characters. Therefore, Facebook users can freely share their opinions and perceptions on any societal topic or life-changing event as they do no have the restriction on the amount of words and characters.

The way of each social network site communicates is also one of the differences between Twitter and Facebook. When comparing to Facebook, a passive form of social and network communication Twitter is more active. In addition, Twitter is frequently compared to a large gathering where everyone is eager to meet and make new friends although they do not know each other. Facebook, on the other hand, is compared to a reception where family and friends are the main attendees. This is because Twitter is a platform where people to start a conversation with strangers who share similar interests. Whereas Facebook is a platform for people to keep track of friends and continue sharing and people will know their added friends in Facebook.

Another difference between both SNS is its privacy setting. There are only two privacy options available for Twitter users which are private and public. Twitter is public by default. Their contents are posted publicly and is visible to other users unless they specifically change their privacy settings to private. Facebook, in contrast, users are given a variety of privacy options. They can choose to have their profile entirely available to public or only available to friends who have given permission. The privacy option for each individual post can be customised to public, friends only, private or custom. Besides, Twitter users do not need get the permission to follow people they interested while Facebook users must get the permission from the user who is not in their friends list.

Moreover, the target market between both SNS is entirely different. Twitter is an ideal platform for users to express their feelings and look at the responses from others. Besides, due to the widespread popularity of Twitter, it is also a channel for the announcements of formal politics. A number of influential presidents and ministers keep a professional Twitter account to increase their reputation and win the trust of the populace. It is the starting point for numerous political and social conflicts and identifies which side of debate is more widely supported. Whereas the main goal of Facebook is to share and discover other people and activities across the world. It strives to build the ideal social world that connects every people and everything. It is a great platform for hanging out and spending time.

Apart from that, there are distinctions between the two SNS in terms of real-time content and timeliness. The real-time nature of Twitter makes it frequently considered as a news source. The posts on Twitter are shorter but frequent and Twitter users and brands frequently provide a running commentary on the topics they are interested in. As a result, the lifespan of the posts on Twitter lasts for a shorter period when comparing to Facebook as the posts on Facebook are evergreen.

1.3 Conclusion

Both Twitter and Facebook share certain similarities despite having numerous differences. They both facilitate connection with people worldwide. Therefore, both SNS are broadly utilised by an enormous audience around the world due to their credibility and reliability. They both are multiuser systems but system downtime for both platform is randomly happened due to their concurrency control on database is well-established. The system for both SNS support simultaneous access on database by numerous users without interfering with one another. Users can login different devices with same account and perform concurrent operations and it will not cause issues such as lost update problem, uncommitted dependency problem and inconsistent analysis problem caused by concurrency. Besides, both Twitter and Facebook have strong database security measures to protect the privacy and security of all data in the database.

PART 2: DENIAL-OF-SERVICE ATTACK

2.1 Introduction

Nowadays, the fast development of technology, application service providers, cloud services and the availability of network capable mobile devices have contributed to the increasing reliance of people on networks for activities such as online banking, information search and other services (Kumar, 2016). However, this has led to significant growth in criminal acts in the networks and their contents have become more cunning and destructive, especially one of the challenging attacks which is Denial of Service (DoS) attack. Additionally, Internet is more open and scalable as an end host can easily connect to the network and exchange packets with other hosts to communicate with them. However, this has allowed network attackers to launch numerous assaults on network resources and deny authorized users from accessing the network service which forms a Denial of Service (DoS) attack. DoS floods the destination of network service with excessive traffic or send information that causes a crash in network service to shut down the machine or network so that it is unavailable to its intended users. (Jain & Chawla, 2020). Therefore, there are countermeasure to combat this attack and will be compared in this topic.

2.2 Prevention Techniques for Denial-of-Service Attack

2.2.1 Hop Count Filtering

The purpose of hop count filtering is to block or eliminate malicious traffic with a spoofed address and it is installed on the routers of destination network equipment (Jin et al., 2003). Each host's IP address and its related distance to each router in a network are recorded and stored in a database. Every incoming packet will be verified it's legitimate by checking if the source IP address and the related distance match with those in the database. Therefore, this can ensure that the packet with a distance traveled that is different from the distance traveled by a packet originating from the actual source will be considered as an attack and discarded. However, this approach has a

disadvantage which is the need to update the source addresses and the relevant address in the database and it is challenging because of route changes.

2.2.2 Ingress Filtering

Ingress filtering is a simple implementation of the DoS prevention method where any assault or malicious traffic with a spoofed IP address detected will be blocked by this method. (Adetoye Adeyemo, 2019). If the source address of a packet same as one of the internal network's IP addresses, the installed edge router will reject its access to the network (Baker & Savola, 2004). Therefore, this can lessen the DoS attack by preventing the entry of packets with a spoofed IP address into the network to track the traffic to its actual source network. However, it needs to deploy at every point of entry into a specific network to ensure its functionality and effectiveness and the cost of its installation and maintenance is high.

2.2.3 Hardware (Netscreen 5GT)

Netscreen 5GT (NS-5GT) is a Juniper's Internet security device and its effectiveness was assessed in the study of Kumar and Gade (2011). NS-5GT defends the network against Layer-4 TCP-SYN flood DoS assaults and UDP flood assaults by using its embedded TCP-SYN proxy protection and UDP protection functions. From the real experiment that was conducted in the study to determine how well the NS-5GT provide protection during the TCP-SYN and UDP flood attacks, it was discovered that it partially reduced the impact of DoS attack especially when the attack was lower loads. However, this device is only effective for the small networks with rate of transmission or bandwidth usage not higher than 40 Mbps as no defense will be provided if the traffic is higher than that.

2.2.4 Extended Access Control List

Access control lists (ACL) are used on a router or switch which consist of a series of rules that regulates whether traffic can pass through a device or enter a network to filter unwanted and dangerous traffic. The DoS attack can be reduced by identifying and categorising the types of attacks to specifically define and incorporate the ACL rule that will allow or prohibit traffic into the list of ACL rules. Multiple ACLs are added relating to different types of traffic such as ICMP, TCP, UDP and other traffic on router or switch interfaces to identify and categorise attack traffic (V. Ramachandran & S. Nandi, 2005). ACLs have a counter that keep tracks of the quantity of packets, size of ACL matches, source and destination addresses that passes across the interface where the ACL is in use. By periodically querying the counter, it is simple to distinguish between malicious and genuine traffic. ACL rule will prohibit the entry of that traffic the next time if that traffic is identified as malicious traffic by the counter. As a result, this can ensure that all malicious traffic access will be prevented by the rule. Nevertheless, if the ACL rules and packet flood is lengthy, ACL may use up the CPU processing power and thus compromise the router's main job which is routing. Besides, ACL also another drawback which is it is more prone to error as the categorization of compound DoS attacks with ACLs is done by human. (Adetoye Adeyemo, 2019).

2.2.5 Capability-Based Method

The purpose of capability-based mechanism is to give destination a method to regulate the traffic flow that is directed towards itself with its own capability. In this technique, the first step of the machine that intends to establish a connection or deliver a message is sending a request packet to connect to the destination. When the request packet passes through the router, the router will add a router mark (precapability) to the request packet. When the packet arrives at the destination machine, it will then be examined and its permission is either granted or denied by the destination machine. The destination machine will grant the permission of the source machine by returning the

packet with capabilities, otherwise, the permission is rejected. The primary benefit of this method is that the destination has a way to regulate the traffic flow with its own capability in order to prevent DoS attacks occur because the packets without capabilities are considered as legacy and may be discarded at the router during the occurrence of congestion. However, this method has the potential to cause the occurrence of Denial of Capability (DOC), a new kind of attack that prohibit new capability-setup packets to travel to their destination. Additionally, the computational complexity of and storage requirement of the system are high. (Gupta et al.,2010c).

The table below provides the summary of the prevention techniques of Denial-of-Service attack:

Prevention Technique	**Pros**	**Cons**
Hop Count Filtering	• Reduce spoofing	• Challenging to update the source address and the relevant address in the database due to route changes
Ingress Filtering	• Reduce IP spoofing	• Need to install for multiple entries and the cost for installation and maintenance is high
Hardware (Netscreen 5GT)	• Fewer installation	• Not effective for traffic higher than 40Mbps.

Extended Access Control List	• Records all the packets that traverses the interface where it is put to use	• If the ACL rules and packet flood is lengthy, ACL may use up the CPU processing power
Capability-Based Method	• Destination can regulate the traffic flow that is directed towards itself with its own capability	• The computational complexity of and storage requirement of the system are high

2.3 Conclusion

In a nutshell, there are a variety of countermeasure to prevent DoS attack, but every prevention technique has its own pros and cons. Therefore, combining several prevention techniques is necessary to combat DoS attack. Preventing DoS attack on database system is one of the database security measures to ensure the confidentiality, integrity and availability of data in the database system.

Reference

1. Liu, Y., & Ying, X. (2010). A Review of Social Network Sites: Definition, Experience and Applications. *Scientific Research*. https://www.semanticscholar.org/paper/A-Review-of-Social-Network-Sites%3A-Definition%2C-and-Liu-Ying/c4395fa75d36a1c9f1d67e5b26ed43e2606429d0
2. Social Networks Sites : Usage and Effects. (2013). *Journal of Educational and Psychological Studies*, *7*(4), 549–558. https://doi.org/10.12816/0002604
3. Brandtzæg, P. B., & Heim, J. (2009). Why People Use Social Networking Sites. *Online Communities and Social Computing*, 143–152. https://doi.org/10.1007/978-3-642-02774-1_16
4. Stec, C. (2015). Social media definitions: The ultimate glossary of terms you should know. Hubspot. Retrieved from http:// blog.hubspot.com/blog/tabid/6307/bid/6126/The-UltimateGlossary-120-Social-Media-Marketing-Terms-Explained.as
5. S, S. (2017, May 19). *Difference Between Facebook and Twitter (with Comparison Chart)*. Key Differences. https://keydifferences.com/difference-between-facebook-and-twitter.html
6. Peachyessay. (2020, June 20). Comparison and Contrast between Facebook and Twitter. https://peachyessay.com/sample-essay/comparison-and-contrast-between-facebook-and-twitter/
7. Ken. (2020, December 9). *Facebook VS. Twitter: a Comparative Analysis - Free Essay Example | EduZaurus*. EDUZAURUS. https://eduzaurus.com/free-essay-samples/facebook-vs-twitter-a-comparative-analysis/
8. EssayZoo. (2021, July 30). *Facebook Vs Twitter, Compare and Contrast Free Essay Sample*. https://essayzoo.org/blog/facebook-vs-twitter-compare-contrast-essay
9. Rey, F. (2012, July 26). *Facebook vs Twitter – The Rivalry, Differences, Privacy Issues*. https://socialbarrel.com. https://socialbarrel.com/facebook-vs-twitter/41152/
10. Alhabash, S., & Ma, M. (2017). A Tale of Four Platforms: Motivations and Uses of Facebook, Twitter, Instagram, and Snapchat Among College Students? *Social Media + Society*, *3*(1), 205630511769154. https://doi.org/10.1177/2056305117691544

11. Hughes, D. J., Rowe, M., Batey, M., & Lee, A. (2012c). A tale of two sites: Twitter vs. Facebook and the personality predictors of social media usage. *Computers in Human Behavior*, *28*(2), 561–569. https://doi.org/10.1016/j.chb.2011.11.001
12. Carr, C. T., & Hayes, R. A. (2015b). Social Media: Defining, Developing, and Divining. *Atlantic Journal of Communication*, *23*(1), 46–65. https://doi.org/10.1080/15456870.2015.972282
13. Dean, B. (2022, January 5). *How Many People Use Twitter in 2022?* Backlinko. https://backlinko.com/twitter-users
14. Dean, B. (2022, January 5). Facebook Demographic Statistics: How Many People Use Facebook in 2022? https://backlinko.com/facebook-users
15. *Difference between Twitter and Facebook*. (n.d.). Twitter Vs Facebook. https://www.differencebetween.info/difference-between-twitter-and-facebook
16. Kumar, G. (2016). Denial of service attacks – an updated perspective. *Systems Science &Amp; Control Engineering*, *4*(1), 285–294. https://doi.org/10.1080/21642583.2016.1241193
17. Thakur, K. (2015b). Analysis of Denial of Services (DOS) Attacks and Prevention Techniques. *International Journal of Engineering Research and Technology*, *4*(7).
18. Jain, S., & Chawla, D. (2020). A Relative Study on Different Database Security Threats and their Security Techniques. *International Journal of Innovative Science and Research Technology*, *5*(1). https://doi.org/10.13140/RG.2.2.11657.60000
19. Adetoye Adeyemo. (2019). COMPARATIVE ANALYSIS OF VARIOUS DENIALS OF SERVICE (DoS) ATTACK MITIGATION TECHNIQUES. *International Journal of Computer Science Engineering*, *8*(4), 163-167. https://www.researchgate.net/publication/338675935_COMPARATIVE_ANALYSIS_OF_VARIOUS_DENIALS_OF_SERVICE_DoS_ATTACK_MITIGATION_TECHNIQUES
20. Gupta, B. B., Joshi, R. C., & Misra, M. (2010c). Distributed Denial of Service Prevention Techniques. *International Journal of Computer and Electrical Engineering*, *2*(2), 268–276. https://doi.org/10.7763/ijcee.2010.v2.148
21. V. Ramachandran & S. Nandi (2012). Bleeding Edge DDoS Mitigation Techniques for ISPs, Cisco Systems, Inc. Bangalore, India. https://www.semanticscholar.org/paper/Bleeding-Edge-DDoS-Mitigation-Techniques-for-ISPs-Ramachandran-Nandi/bd7610ec9ef0f73e62cdc23d6133168ddeaae68a

22. Kumar, S., & Gade, R. S. R. (2011). Experimental Evaluation of Juniper Network's Netscreen-5GT Security Device against Layer4 Flood Attacks. *Journal of Information Security*, *02*(01), 50–58. https://doi.org/10.4236/jis.2011.21005
23. P. Ferguson and D. Senie. (2000). Network ingress filtering: Defeating denial-of-service attacks which employ IP source address spoofing. RFC 2827. https://www.semanticscholar.org/paper/Network-Ingress-Filtering%3A-Defeating-Denial-of-IP-Ferguson-Senie/c951a01cbb8cd7b96fd9c36f64e0efbe3c78d4e2
24. Jin, C., Wang, H., & Shin, K. G. (2003). Hop-count filtering: An Effective Defense Against Spoofed DDoS Traffic. *Proceedings of the 10th ACM Conference on Computer and Communication Security - CCS '03*. https://doi.org/10.1145/948109.948116
25. Baker, F. and P. Savola. (2004). Ingress Filtering for Multihomed Network. BCP 84, RFC 3704, https://doi.org/10.17487/RFC3704