Homework 04

Pramod kumar

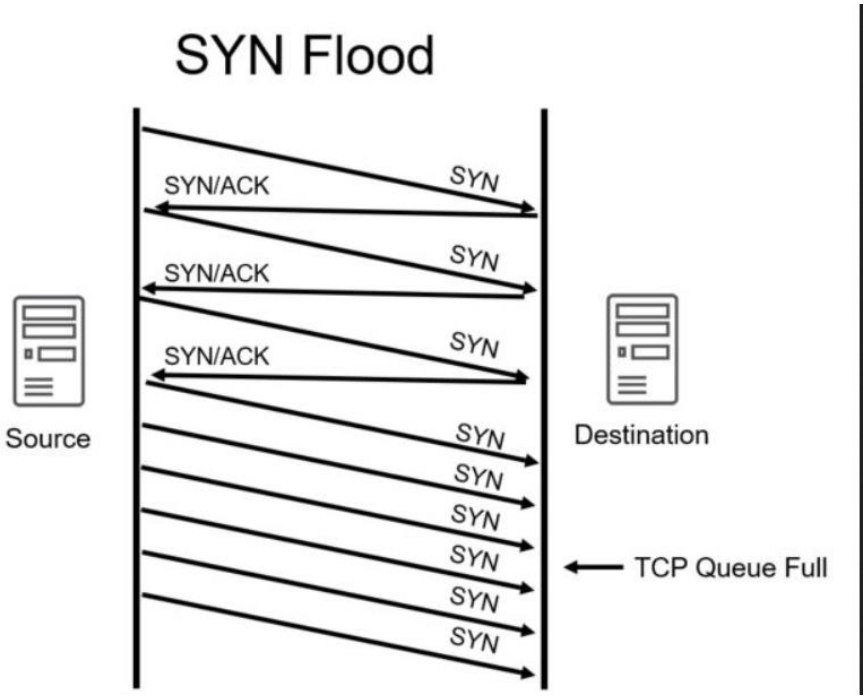
pjk5502@psu.edu

1. **(6 pts) Explain how TCP SYN flooding attacks work? (with a figure)**

Normal TCP connection involves 3-way handshake:

1) Client send SYN request to server
2) Server acknowledge it with SYN-ACK response
3) Again client responds with ACK, which is last step in the connection.

In SYN attack, attacker do only half-open connection i.e only send SYN request but repeated (with spoofed Ip address which fool defense mechanism by pretended as different clients.). Which makes TCP full(resource execution) hence when genuine client request comes it will be dropped. Its DDOS category attack.

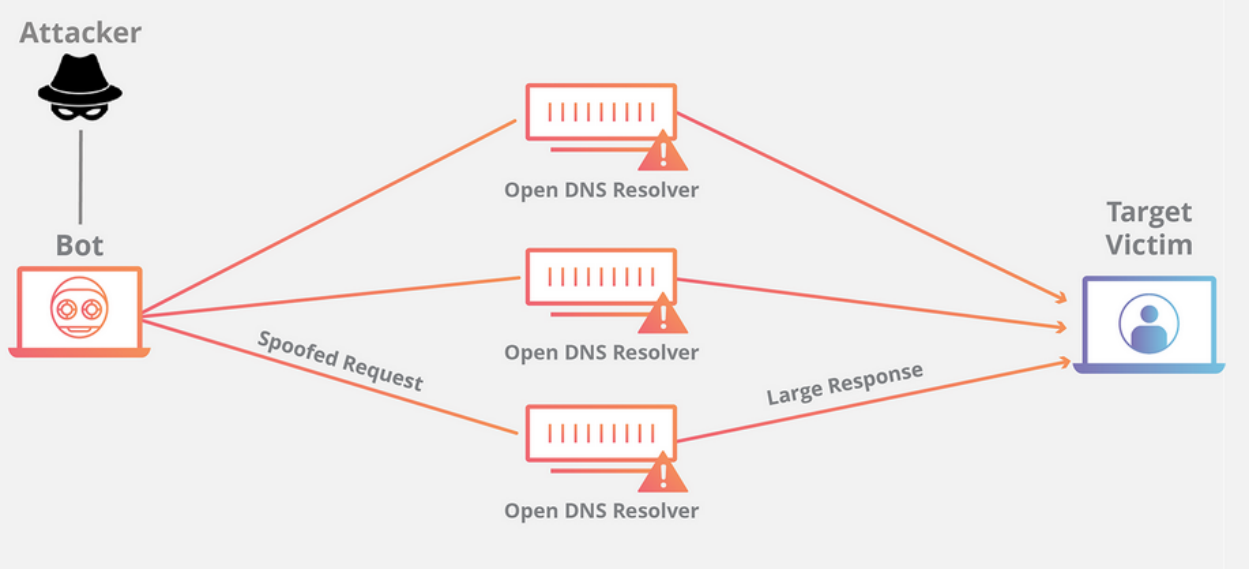


2. **(6 pts) Describe how reflection attacks and DNS amplification DoS attacks work**

   (you may read this article to get a deeper understanding of reflection DDoS attacks: https://www.akamai.com/us/en/about/news/press/2015-press/akamai-warns-of-3-new-reflection-ddos-attack-vectors.jsp)

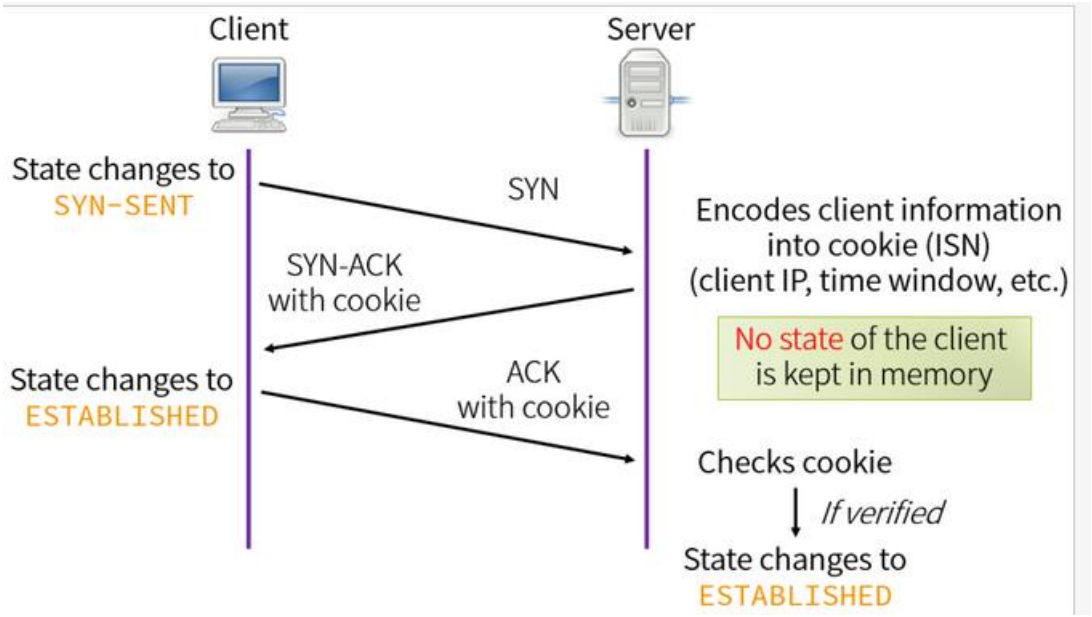
In Reflection attack we have 3 players i.e target system, victim system and the attacker. Instead of sending query directly to target, attacker send it to list victim(client) hosts but with spoofed target ip address as source address. Which make victims/clients to send response to target machine. Generally, such attacks are performed when response for a query is bigger then the query size, which amplifies the attack.

In DNS amplification DoS attack, By sending small queries that result in large responses, the malicious user is able to get more from less. By multiplying this magnification by having each bot in a botnet make similar requests, the attacker is both obfuscated from detection and reaping the benefits of greatly increased attack traffic. Each bot making requests to open DNS resolvers with a spoofed IP address (targeted victim), the target then receives a response from the DNS resolvers. To create a large amount of traffic, the attacker structures the request in a way that generates as large a response from the DNS resolvers. As a result, the target receives an amplification of the attacker's initial traffic, and their network becomes clogged with the spurious traffic, causing a denial-of-service.



3. **(5pts) Explain what is SYN Cookie and what it is for? You may use a figure to help illustrate.**

Sync cookies are used as a defense against sync flood attack (explained in question 1) where during initial handshake. When sync cookies is enabled, tcp server doesn't keep state of half-open connection as it calculate a TCP sequence number(secret) using a secret math combination. When a genuine user replies to SYN-ACK with a ACK and tcp sequence number, that seq number will be check against the same secret function which will validate if response is genuine. As in syc attack, packet has spoofed IP address, which doesn't have any real user behind hence only client with genuine connection request will respond to SYN-Ack request.



4. **(5 pts) What is DNS spoofing attack?**

Domain Name Server (DNS) spoofing is an attack in which altered DNS records are used to redirect online traffic to a fraudulent website that resembles its intended destination. Once there, users are prompted to login into (what they believe to be) their account, giving the perpetrator the opportunity to steal their access credentials and other types of sensitive information.

It can be achieved by following methods:

1) Man in middle

2) DNS server hijacking and then configuring malicious IP address.

5. **(6 pts)** What is proof of work (POW) and why is it deployed in bitcoin?

Proof of work is consensus algorithm, which is used to produce a new block in the chain, it hard to produce but easily for other to verify. Miners complete against each other to complete a transition on the network and get rewards. Producing POW be any random process with low probability so it takes lots of trial and error before valid proof is generated.
Why deployed in bitcoin?
The main benefits are the anti-DoS attacks defense and low impact of stake on mining possibilities.
Defense from DoS attacks. PoW imposes some limits on actions in the network. They need a lot of efforts to be executed. Efficient attack requires a lot of computational power and a lot of time to do the calculations. Therefore, the attack is possible but kind of useless since the costs are too high.

6. **(6 pts**)Assume that passwords are selected from four-character combinations of 26 alphabetic characters. Assume that an adversary is able to attempt passwords at a rate of one per second.
   (a) Assuming no feedback to the adversary until each attempt has been completed, what is the expected time to discover the correct password?

Answer: 26x26x26x26 = 456976 and its 1 per second so
456976sec/60*60 = 126.9 hours

   (b) Assuming feedback to the adversary flagging an error as each incorrect character is entered, what is the expected time to discover the correct password?

Answer : 26+26+26+26 = 104

104/60 = 1.7 Minutes.

7. **(8pts)** Because of the known risks of the UNIX password system, the SunOS-4.0 documentation recommends that the password file be removed and replaced with a publicly readable file called /etc/publickey. An entry in the file for user A consists of a user's identifier ID_A, the

user's public key PU_a, and the corresponding private key PR_a. This private key is encrypted using DES with a key derived from the user's login password P_a. When A logs in, the system decrypts E(PRa, Pa) to obtain PRa.

a) The system then verifies that P_a was correctly supplied. How?

Answer: since public and private key can be used interchangeably to encrypt and decrypt.

1) We can decrypt the private key with PA and
2) encrypt some file/bytes/content with public key and
3) try to decrypt with private key or vis versa..

if we get same file back then we are sure that its correct P_a which got us correct private key

b) How can an opponent attack this system?

Answer: Framework in sonOS uses arbitrary bit of content to encrypt it with private key(which we got from P_a) . the framework decodes this encrypted content utilizing the public key. If the decoded content matches framework is vulnerable to attack.

8. (8 pts) Problem 7.26.

Answer :

1) Number of test: 100,000 = 10^5 and 10^7 is figure print in database.

So total number of comparison is 10^12 .

Error is 1/10^10 for each. So total is 10^12/10^10 = 100

2) For individual mean 10^7 total comparison ..
with propbalituy of 1/10^10 , it will be 10^7/10^10 =>0.001

9. (9pts) Problem 7.37 .

Answer:

1) D(alice,bob)
d (alice, bob) = 0.453125
d(ALice charli) = 0.609375
d(bob charli) = 0.53125

2) Applying threshod of .32 (given in the book at page 248)
Distance of Alice from U,V,W,X,Y
d(U alice) = 0.5625
d(V alice) = 0.453125
d(W alice) = 0.15625
d(X alice) = 0.515625
d(Y alice) = 0.5

Alice matches with W

Distance of BOB from U,V,W,X,Y

d(U bob) = 0.578125

d(V bob) = 0.4375
d(W bob)= 0.484375
d(X bob) = 0.15625
d(Y bob) = 0.421875

bob match with X

Distance of Charlu from U,V,W,X,Y

d(U charli) = 0.171875
d(V charli) = 0.46875
d(W charli) = 0.546875
d(X charli) = 0.5625
d(Y charli) = 0.484375

charli marches with U.

10. **(9pts)** Construct an access matrix for the following case. There are three users (Cartman, Butters, and Public) that own the files (o1, o2, and o3, respectively). An owner can read and write his own file. Cartman and Butters do not want Public or each other to read anything that they write, whereas Public allows everyone to read his file.
    a. Draw the access matrix. Fill in the access matrix with the maximal number of read permissions possible for the three files.
    Solution:

	O1	O2	O3
Cartman	RW	--	R
butters	--	RW	R
public	--	--	RW

    b. Suppose we want to implement this model using (1) an ACL, (2) a capability list (C-list). Show what the lists look like.
    Solution:

ACL

O1	Cartman:R Cartman: w Cartma: own
O2	Butters : R Butters : W Butters : OWN
O3	PUBLIC: R Butters : R Cartman:R PUBLIC: W PUBLIC: OWN

Capability list

catman	O1/R, O1/W,O1/OWN, O3/R
butters	O2/R, O2/W,O2/OWN, O3/R
publics	O3/R, O3/W,O3/OWN,

c. List two advantages of ACLs over C-lists and two advantages of C-lists over ACL.

Advantage of acl:

1) Provide superior access review on per-object basis

2) Provide superior access revocation on per-object basis

3) Good when user maintain its file

4) Protection is data oriented

5) Easy to change persmision on resource

Advantage of capability list:

1) Provide superior access review on per-subject basis

2) Provide superior access revocation on per-subject basis

3) Easy to add/delete users

4) Easer to avoid confused duty

11. **(4 pts)** Assume a system with N job positions (i.e., roles). For job position i, the number of individual users in that position is U_i and the number of permissions required for the job position is P_i.
    a. For a traditional DAC scheme, how many relationships between users and permissions must be defined?
       Tradition DAC is relation between object and subject. In DAC we will have for each job we will have UxP as a row where U total number of users in the systems, P total type of permission
    b. For a RBAC scheme, how many relationships between users and permissions must be defined?
       P, it based on group.

12. **(8 pts)** The high water mark principle and low water mark principle both apply in the realm of multilevel security.
    (a) What is MLS?
    (b) Define the high water mark principle and the low water marker principle in the context of MLS.
    (c) Is BLP consistent with a high water mark principle or a low water mark principle, both, or neither? Justify your answer.

(d) Is Biba's Model consistent with a high water mark principle or a low water mark principle, both, or neither? Justify your answer.
Answer:

a) It is required different level of subject/object used the same systems. Hence based on the level access will be provided.

b) high-water mark, any object less than the user's security level can be opened.

In the low-water mark model, read down is permitted, but the subject label, after reading will be degraded to object label. It can be classified in floating label security models.

c) BLP is based on high water mark principle. can't read data from higher level and can't write data to lower level. As it aimed at higher secrecy. S can read O if and only if L(O)<=L(S) . S can write O if and only if L(s)<=L(o) i.e No read up and no read down.

d) It is based on low water mark principle. As is defined for integrity. I denote intergrity

S can write O of and only If I(O) <= I(S) and s can only read O if and only if I(s)< I(o)

i.e I(s) = minimum of (I(S), I(o))

13. textbook 11.6 (6pts)

a) canary is a random variable which is put on the stack immediately after the return address. When someone try to overwrite/overflow the buffer this value will also be overwritten and at runtime system will get to know about attack.

b) Implementation was flawed as when canary check failed, program will pass the control of the program to a user defined handler function which means attacker defined function hence it will lead to implication.

14. 11.15 (8pts).

1) 11122222

2) Because program wrote "1" is difference between base pointer of both buffer and + 3. Hence first 3 byte of buf2 also got over written.

3) Using this and knowing the stack size, Trudy can overwrite return address of the function to jump to another location when function returns.

11.16 (6 pts)

Answer:

1) Potential problem is argument to function is signed and memcpy take unsigned

2) hence user can passed as negative value which will bypass the “if” condition and “len” will be auto converted to unsigned which will make it very big value, hence it will breach the char buf[800] size and overflow will occur.