**Homework 04 (totally 124 pts)**

1. (8pts) Consider the Kerberos interaction discussed in this chapter.
   1. Why is the ticket to Bob encrypted with KB?
   2. Why is “Alice” included in the (encrypted) ticket to Bob?
   3. In the REPLY message, why is the ticket to Bob encrypted with the key SA?
   4. Why is the ticket to Bob sent to Alice (who must then forward it to Bob) instead of being sent directly to Bob?

>>>

a. So that only Bob can decrypt it. The session key KAB that Alice and Bob will

share is included in the ticket.

b. Bob will know that the included key is to be used to communicate with Alice.

c. This serves no obvious purpose, since the ticket to Bob is already encrypted

with KB, which only Bob and the KDC know. Also, Alice sends the ticket to Bob

without any additional encryption.

d. It would be more efficient (in terms of bandwidth usage) to send it directly to Bob,

but then Bob would have to remember this info until Alice contacts him. That

is, Bob would have to maintain state, and Kerberos is all about being stateless.

1. (8pts) Consider the Kerberized login discussed in this chapter.
   1. What is a TGT and what is its purpose?
   2. Why is the TGT sent to Alice instead of being stored on the KDC?
   3. Why is the TGT encrypted with KKDC?
   4. Why is the TGT encrypted with KA when it is sent from the KDC to Alice’s computer?

>>>

a. Ticket Granting Ticket | it serves as a user's “credentials," that is, it enables a

user to request ordinary tickets. Exchange ordinary tickets

b. This enables the KDC to remain stateless. In effect, the KDC distributes the

database of TGT information to the clients.

c. The KDC--and only the KDC---can decrypt a TGT, which enables the KDC to

“remember" everything it needs to know about the user.

d. Apparently, this serves no purpose, since the TGT is already encrypted and it is

freely passed about (with no additional encryption) in subsequent interactions.

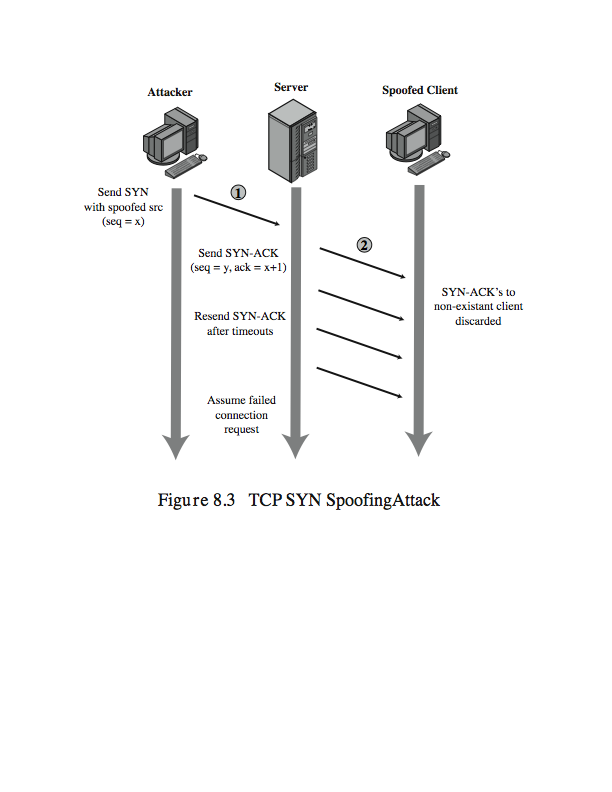
1. (8pts) Describe (enumerate) the insecurity of GSM and then modify the GSM security protocol (Figure 10.25) so that it can provide mutual authentication.

>>> a. answer any four of the following insecurity are sufficient.

* hash functions A3/A8 and encryption function A5 are easy to break.
* **no encryption** from base station to base station controller
* Attacks on SIM card
* **Fake base station**
* Denial of service is possible
* Base station can replay

There are many other reasonable approaches as long as the BS can compute a MAC (or even digital signature if you assume public key infrastructure) or an encryption of a plaintext. Below is an examples. The mobile could send a nonce R in message one, and the base station could return RAND and Enc(R, Kc), in message 4 .

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



Or similar figures such as #14 in “net attacks”. Details refer to slides.

5. (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>）

See slides #14-19 in DDoS

6. (8pts) Using a TCP SYN spoofing attack, the attacker aims to flood the table of TCP connection requests on a system so that it is unable to respond to legitimate connection requests. Consider a server system with a table for 256 connection requests. This system will *retry* sending the SYN-ACK packet five times when it fails to receive an ACK packet in response, at 30-second intervals, before purging the request from its table (pay special attention when you compute the time a connect request stays in the table). Assume that no additional countermeasures are used against this attack and that the attacker has filled this table with an initial flood of connection requests.

1. At what rate must the attacker continue to send TCP connection requests to this system in order to ensure that the table remains full? (4 pts)
2. Assuming that the TCP SYN packet is 40 bytes in size (ignoring framing overhead), how much bandwidth does the attacker consume to continue this attack? (4 pts)

>>>

(a) For a TCP SYN spoofing attack, on a system with a table for 256 connection

requests, that will retry 5 times at 30 second intervals, before purging the request

from its table, each connection request occupies a table entry for 6 30secs (initial

+ 5 repeats) = 3min. In order to ensure that the table remains full, the attacker must

continue to send 256/ 3 or about 86 TCP connection requests per minute?

(b) Assuming the TCP SYN packet is 40 bytes in size, this consumes about 86 x 40 x 8 / 60, which is about 459 bits per second, a negligible amount.

7. (6 pts) Describe (with some details) three methods for DoS attack prevention or mitigation or defense.

> any 3 out of the following: Rate limiting, random drop, syn cookies, client puzzle, Ip traceback (or other ideas if they make sense). Details see slides #20-28 in DDoS.

8. (9 pts) This problem deals with storing passwords in a file.

1. Why is it a good idea to hash passwords that are stored in a file?
2. What is a salt and why should a salt be used whenever passwords are hashed?
3. What are the criteria for a good password hashing function?

>>> a. because hash function has the one-way property, so from the hashed passwords an attacker cannot derive the passwords.

b. a salt is random data that is used as an additional input to a one-way function that hashes a password. The primary function of salts is to defend against dictionary attacks.

c. besides being a secure hash function, it should also be slow to thwart dictionary attacks.

9. (8 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.

1. Assuming no feedback to the adversary until each attempt has been completed, what is the expected time to discover the correct password?
2. Assuming feedback to the adversary flagging an error as each incorrect character is entered, what is the expected time to discover the correct password?

>>>a. there are 26^4 total passwords. On average, the adversary has to try half of them to succeed, so the expected time will be 26^4/2 =…

b. in this case every character may be guessed correctly in 26/2 = 13 times. So totally 13x4=52 times guessing. The time needed is 52 seconds.

10. (10pts) 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 , the user’s public key , and the corresponding private key . This private key is encrypted using DES with a key derived from the user’s login password . When A logs in, the system decrypts E(PRa, Pa) to obtain PRa.



1. The system then verifies that was correctly supplied. How?



1. How can an opponent attack this system?



1. (8 pts) Problem 7.26.

>>>



1. (9pts) Problem 7.38 (a)(b)(c) only .

>>>



1. textbook 11.6.a (6pts)

>>> If the canary value is overwritten, then there is likely a problem with the return address.

1. 11.15 (8pts)

>>>

a. The results are buf2 = 22222222 and buf2 = 11122222.

b. Apparently, buffer 1 has overwritten the start of buffer 2.

c. Trudy might be able to overwrite some important data to, say, change a failed authentication into a successful authentication.

1. 11.16 (8 pts)

a. If len is negative there is a problem. The test in the if will be passed, but then

memcpy assumes that len is unsigned. So, a negative value for len is interpreted

as a very large number, which would lead to a buffer overflow.

b. Explain how an integer overflow might be exploited by Trudy. Trudy can overflow

an array and cause problems.