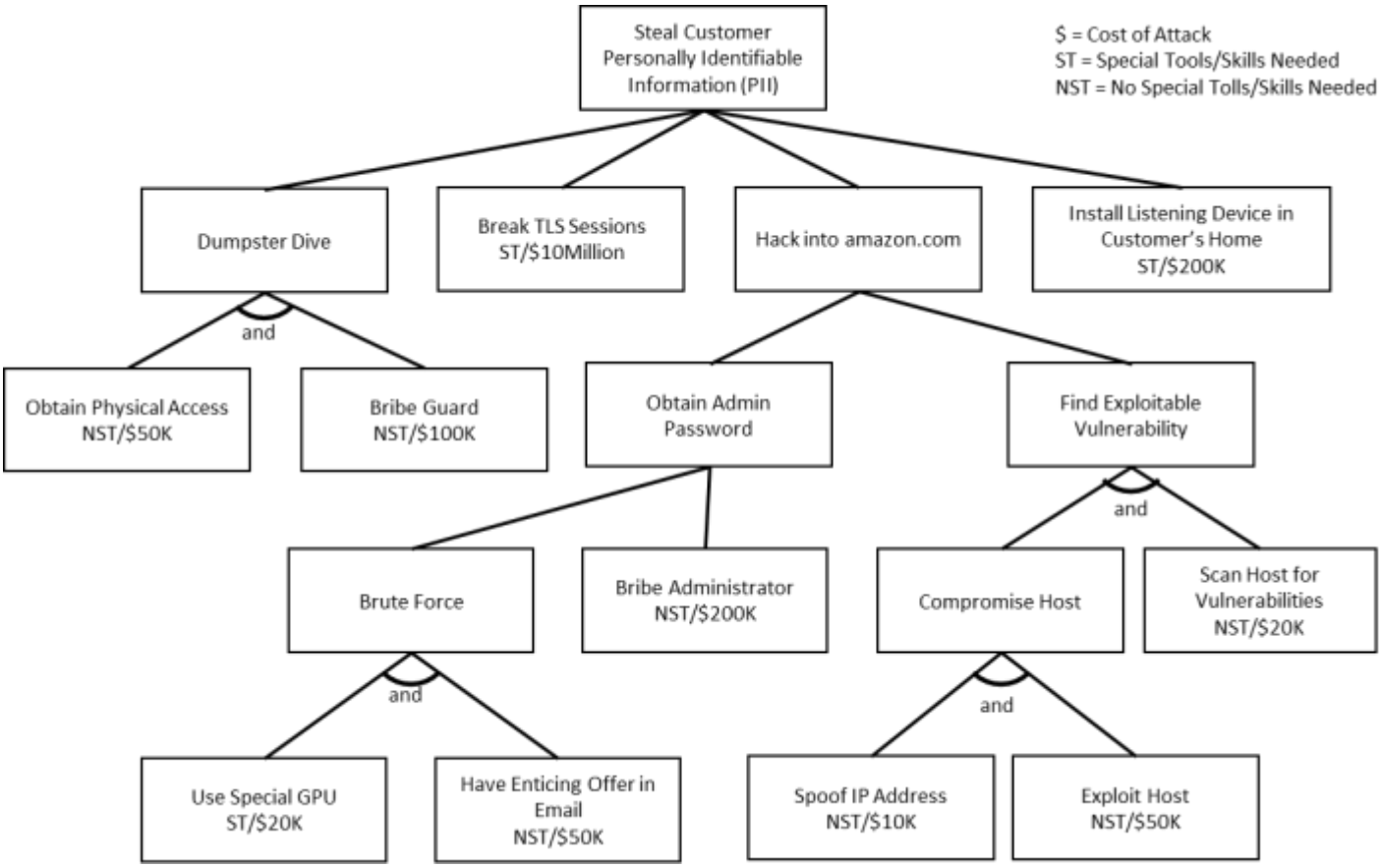
Midterm – CS 6823 – Network Security

Instructions:

- Put your name and ID on your submission and file name.
- Be sure to read the questions carefully and answer all parts.
- All questions require an explanation for full credit. No explanation = no credit.

1. Attack Trees



1a. [3 pts] What's the cheapest attack (name and amount) that requires no special tools or skills?
1b. [3 pts] What's the cheapest and most expensive methods (name and amount) to "Hack into amazon.com"?
1c. [4 pts] Suppose "Exploit Host" is now costs $100K rather than $50K. Does this change the answer in (1a or 1b)? If so, how.

2. Attacks

2a. [3 pts] What is a technical way in which Trudy would obtain the email server's address (i.e., mail.acmecorporation.com) using DNS without being detected by ACME in any way? Explain.
2b. [3 pts] What kind of attack does Split DNS mitigate, and how does it do it?
2c. [3 pts] When using the nmap TCP ACK Scan, what is the meaning if a **RST** is returned for a port?
2d. [3 pts] What is the meaning if the response is **nothing**?

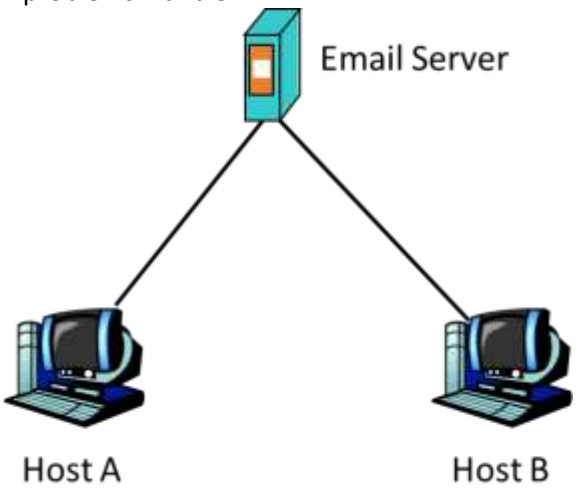
3. Message Integrity

Suppose Alice is buying a pizza from Bob's Pizzeria, and the exchange is as follows:

Alice -> Bob: Hello, I want a pizza
Bob -> Alice: Use this nonce R
Alice -> Bob: signed_using_Bob's_public_key(R, I want one pizza)

3a. [4 pts] Suppose Trudy was able to capture this exchange. Would Trudy be able to replay this message to order extra pizza for Alice? Explain.
3b. [3 pts] Does Alice know that he's talking to Bob? Explain
3c. [3 pts] Does Bob know that he's talking to Alice? Explain

Use the following diagram for problems 4 and 5.



The above diagram depicts a network inside ACME Corporation. Hosts A and B can communicate with the Email Server. Note: For these two problems, there are no other hosts available.

4. Reconnaissance
4a. [8 pts] Suppose Trudy has root access to Host A, and she wants to perform a port scan of Host B with sending as few as possible packets between Host A and B. Explain how Trudy can do this with the minimal possibility of being detected by ACME.
4b. [2 pts] What conditions are required in order to make this attack possible?

5. [10 pts] Covert Channel
Suppose Trudy was able to obtain root access Host A and B, but not to the Email Server. Trudy wants to send a file from Host A to Host B without communicating directly between Host A and B. Explain how Trudy would send a file from host A to B with the minimal possibility to being detected by ACME.

6. [10 pts] Netcat
Suppose Alice is at home and her home PC has an IP address of 10.0.0.10. She's connected to the Internet via a Home Router which has the public IP address of 47.18.200.150. Trudy, whose IP address is 203.36.200.2, wants to steal a file off of Alice's computer using netcat. What are the netcat commands for each side in order for Trudy to accomplish this?

7. Perform RSA key generation with p=3 and q=17. Note: you must show work for any modular mathematics.

7a. [2 pts] Compute n and φ

7b. [2 pts] Choose the smallest possible public (encryption) exponent e

7c. [4 pts] Choose a private (decryption) exponent d

7d. [4 pts] Encrypt the plaintext message m=8 with the public key

7e. [2 pts] Is it possible to have multiple different decryption exponent d for an encryption exponent e?

8. Perform Diffie-Hellman shared key generation with g=7, n=11, Alice selects a=5 as her secret, Bob selects b=6 as his secret.

8a. [3 pts] calculate Alice's public key A

8b. [2 pts] calculate Bob's public key B

8c. [2 pts] calculate Alice's shared key K

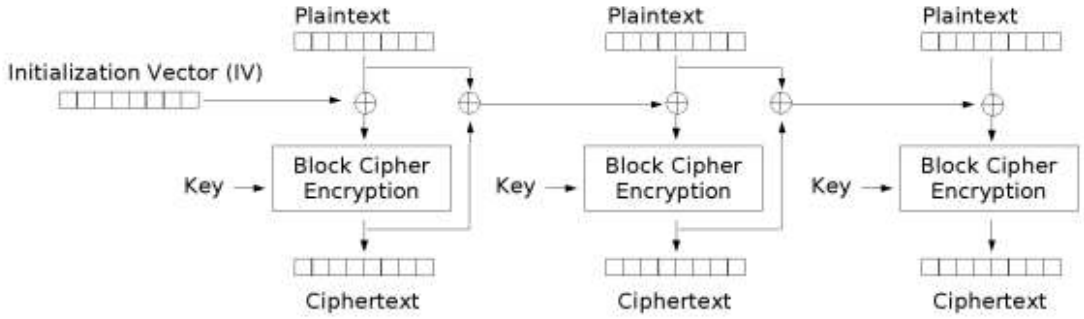
8d. [2 pts] calculate Bob's shared key K

8e. [3 pts] What values are publicly shared in this exchange?

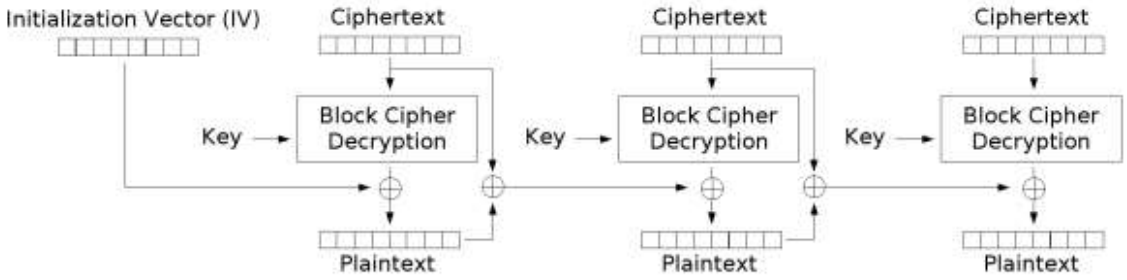
9. Block Cipher Mode of Operations

Input	**Output**	**Input**	**Output**
0000	0111	1000	1111
0001	0110	1001	1110
0010	0101	1010	1101
0011	0100	1011	1100
0100	0011	1100	1011
0101	0010	1101	1010
0110	0001	1110	1001
0111	0000	1111	1000

The following diagram shows Propagating Cipher Block Chaining (PCBC), a similar mode of operation to CBC.



Propagating Cipher Block Chaining (PCBC) mode encryption



Propagating Cipher Block Chaining (PCBC) mode decryption

9a. [3 pts] Should the IV be changed after each message when using the above table in PCBC? Explain why or why not.

9b. [3 pts] If the Cipertext 1001 decrypts to 0101 and PCBC is used, what is the IV?

9c. [6 pts] Using the IV from above, encrypt 110001100011 using PCBC.