CS558. Network Security.
Boston University, Computer Science.
Midterm Spring 2013.

Instructor: Sharon Goldberg

April 4, 2013. 3:30-4:50 PM.

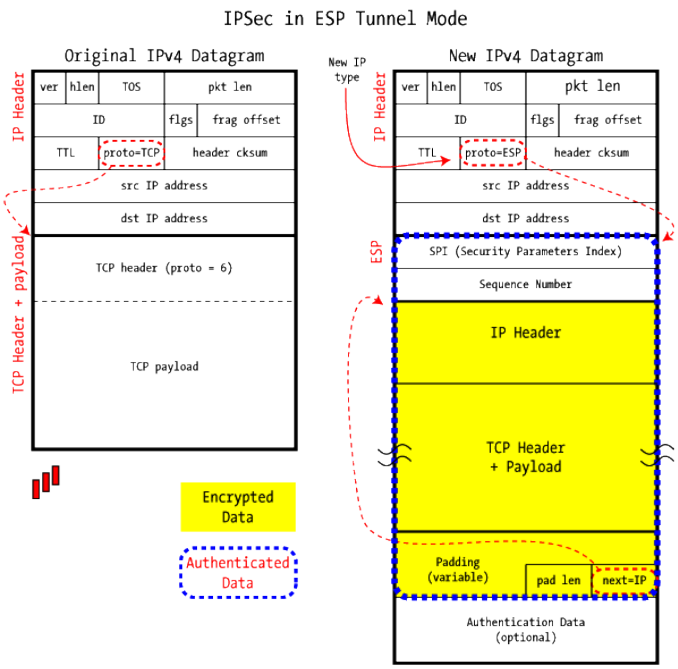
- Be specific and precise with your answers.
- Show your work. Answers without justification will be given little credit.
- Please clearly indicate which parts of your solution you want graded.
- You can use the back of each page as a scratch paper. We will only grade the work you do on the exam pages unless you specifically tell us to do otherwise.

Good luck!

Name: ______________________________

Problem	Grade
1	/4
2	/2
3	/6
4	/6
5	/4
Total	/22

Problem 1. Here is an IPsec packet:

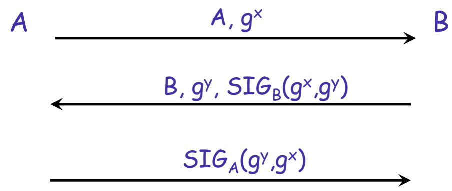


1. **(2 points.)** Suppose the "sequence number" field was removed from the IPsec specification. What attacks now become possible? (In your answer, explain the details of the attacks.)

2. **(2 points.)** The IPsec packet is authenticated using a MAC. Why, then, does it still have a header checksum?

Problem 2. (2 points.) Give a technical explanation of the attack in this photo:

Problem 3. (Key exchange). Consider the following key-exchange protocol the we discussed in class. Recall that the shared key is $k = g^{xy}$, and that $SIG_A(m)$ is the (public-key) digital signature on message m signed by the secret key of A.



Suppose there is a man-in-the-middle adversary E that can intercept, add, drop, and the modify the traffic that A sends to B.

1. **(4 points.)** E can launch an "identity misbinding attack" where she convinces B that he shares the key $k = g^{xy}$ with E, while convincing A that she shares $k = g^{xy}$ with B. Explain exactly how E does this. (What messages does she send, and to who?)

2. **(2 points.)** Give an example of a scenario where this attack might create problems.

Problem 4. (CPA secure encryption.)

1. **(2 points.)** Write down the definition for a CPA-secure symmetric encryption scheme. Remember to define both security and correctness.

2. **(4 points.)** True or false.

   Suppose we have a CPA-secure encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$. Then no adversary running in polynomial time that knows a polynomial number of (plaintext, ciphertext) pairs can learn the secret key. (Hint. If this is true, prove it in the contrapositive, using a reduction. If this is false, provide a counterexample.)

Problem 5. (4 points.) Recall that BGP announcements have the format (IP prefix, AS-path), and that the first AS on the AS path is known as the "origin AS".

Here is a sample BGP announcement where the origin AS is AS 13:
(Prefix: 4.0.0.0/22, AS-path: [13, 4, 6, 33])

Suppose the RPKI contains a valid ROA authorizing AS 12 to announce the prefix 4.0.0.0/22. The ROA is interpreted as follows:

1. A BGP announcement for prefix 4.0.0.0/22 and origin AS a is **valid** if $a = 12$.
2. A BGP announcement for prefix 4.0.0.0/22 and origin AS a is **invalid** if (a) $a \neq 12$ and (b) there is no valid ROA authorizing AS a to announce the prefix 4.0.0.0/22.
3. A BGP announcement for a prefix π and origin AS a is **invalid** if (a) prefix π is a subset of prefix 4.0.0.0/22, and (b) there is no ROA authorizing AS a to announce the prefix π.

What attack on BGP would be possible if the third bullet point was missing? In your answer, explicitly state the details of the attack.