COMP 189: Homework 8

Assigned March 18, 2022
Due midnight March 25, 2022
42 points total

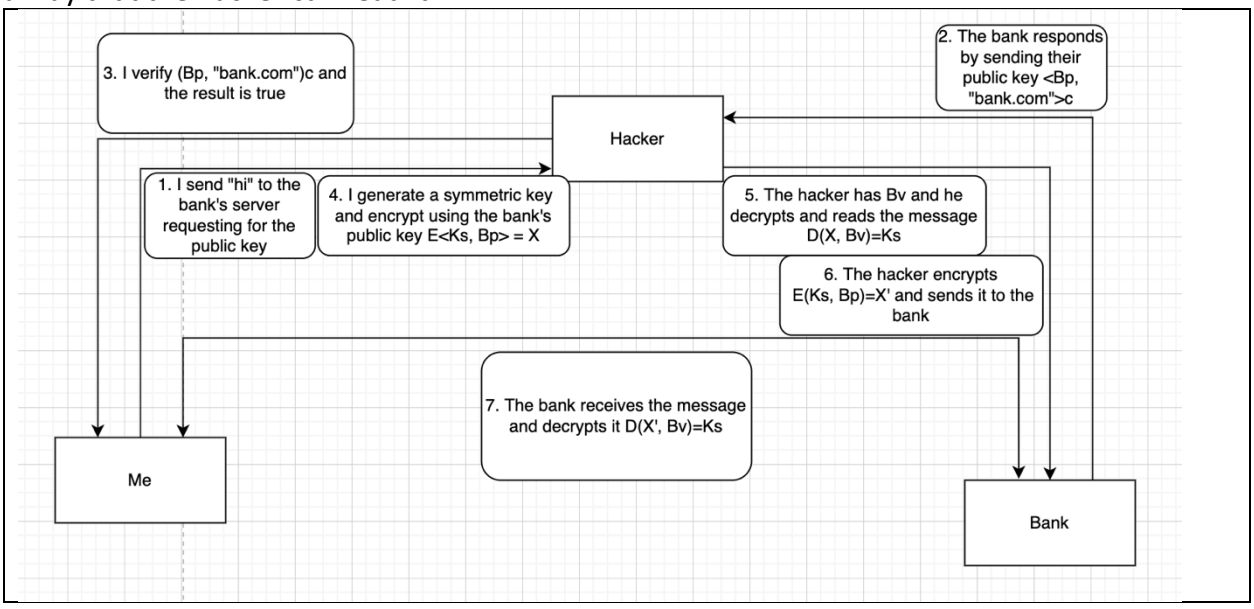
Technical Exercises

For each problem, show all your work (required for credit). For answers requiring written answers, while no more than five or six sentences are expected, sufficient justification must be given for any position, opinion, or perspective taken.

1. Lost Private Key (15 pts)

Your bank has the key <Bp, Bv> as well as the certificate (Bp, "bank.com")$_C$. A hacker manages to steal the private key, Bv. Days later, your computer attempts to establish a secure connection with the bank, but the hacker is able to successfully complete a man-in-the-middle attack so that it can see (and even modify) all the encrypted traffic you are exchanging with your bank.

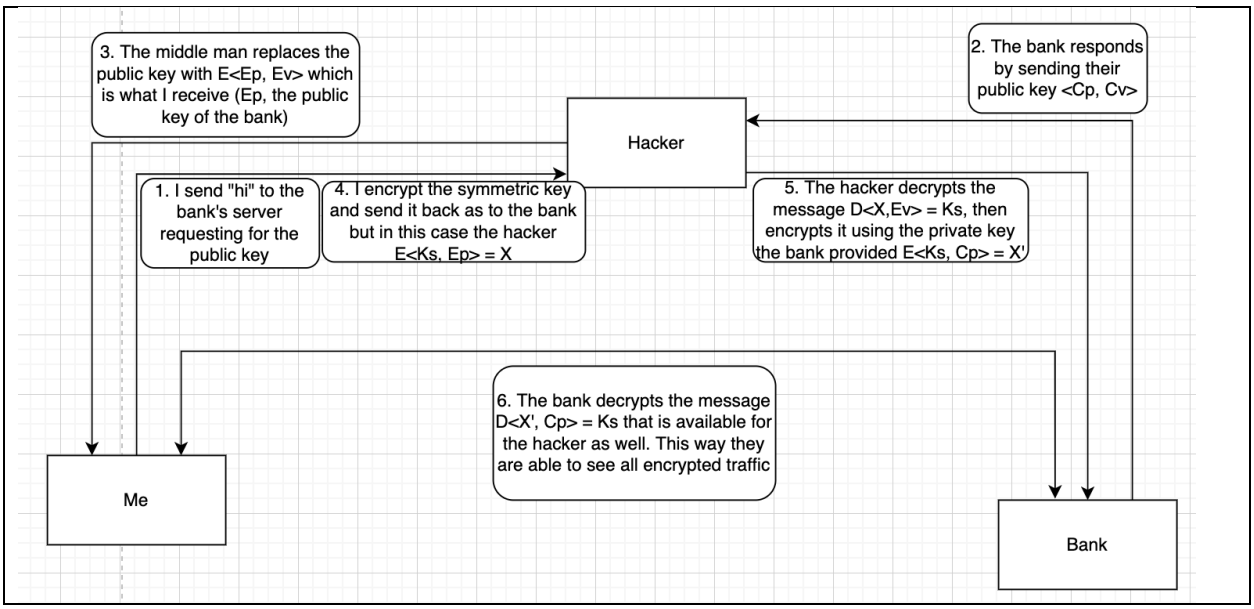
Diagram the SSL protocol showing how the hacker managed to successfully complete the man-in-the-middle attack. Your diagram should show ALL stages of the SSL protocol that we discussed in class. Your diagram should begin with your computer saying "hi" to the bank server and end with your computer sending a message encrypted by the symmetric key in such a way that the hacker can read it.



2. Compromised Certificate Authority (15 pts)

A certificate authority has key <Cp, Cv>. A hacker manages to steal the private key. Days later, your computer attempts to establish a secure connection with your bank, but the hacker is able to successfully complete a man-in-the-middle attack so that it can see (and even modify) all the encrypted traffic you are exchanging with your bank.

Diagram the SSL protocol showing how the hacker managed to successfully complete the man-in-the-middle attack. Your diagram should show ALL stages of the SSL protocol that we discussed in class. Your diagram should begin with your computer saying “hi” to the bank server and end with your computer sending a message encrypted by the symmetric key in such a way that the hacker can read it.



3. SQL Injection (12 pts)

Twitter provides the ability to search for users. To do so, you enter the user you want to search for in a text box on the website and hit <enter>. Behind the scenes, the string you entered (call it <x>) is entered directly into the search query:

SELECT username FROM users WHERE name LIKE “<x>”;

1. What search can you perform that will perform an SQL injection attack against Twitter and drop the users table. As done in class, show how the substitution is done to achieve the desired effect.

SELECT username FROM users WHERE name LIKE “blah”; DROP TABLE users; –";

The core command is “SELECT username FROM users WHERE name LIKE “<x>”;” and we can’t change that, but we want to add drop table users into <x>. Meaning we try to inject DROP TABLES users into <x>

The proper way to do it using the command SELECT username FROM users WHERE name LIKE “<x>”; is:
<x> = username
➔ which returns SELECT username FROM users WHERE name LIKE “blah”;

SQL injection happens like so:
<x> = username”; DROP TABLE users; --
➔ which returns SELECT username FROM users WHERE name LIKE “blah”; DROP TABLE users; –";

Drop tables is a valid SQL command. So, when running the SQL command, the server thinks it’s running a single command, but does not know that the drop table is also being executed hence a successful SQL injection.

2. You discover that Twitter has gotten wise to SQL injection attacks and replaces any “--” characters with an empty string “”… in effect removing the ability to add an SQL comment into your command. Revise your command so that your SQL injection attack an succeed without using the SQL comment. As done in class, show how the substitution is done to achieve the desired effect.

Similarly, to above we can use another comment other than the double dash. For example, we can add “00” or “#” as a comment. So, our command would be:
SELECT username FROM users WHERE name LIKE “blah”; DROP TABLE users; 00”;

Like above the core command is “SELECT username FROM users WHERE name LIKE “<x>”;” and we can’t change that, but we want to add drop table users into <x>. Meaning we try to inject DROP TABLES users into <x>

The proper way to do it using the command SELECT username FROM users WHERE name LIKE “<x>”; is:
<x> = username
➔ which returns SELECT username FROM users WHERE name LIKE “blah”;

SQL injection happens like so:
<x> = username”; DROP TABLE users; 00”;
➔ which returns SELECT username FROM users WHERE name LIKE “blah”; DROP TABLE users; 00”;

Drop tables is a valid SQL command. So, when running the SQL command, the server thinks it’s running a single command, but does not know that the drop table is also being executed hence a successful SQL injection.