Nicholas Nikas
260870980

COMP 189: Homework 6

Assigned April 9, 2021
Due midnight April 23, 2021
46 points total

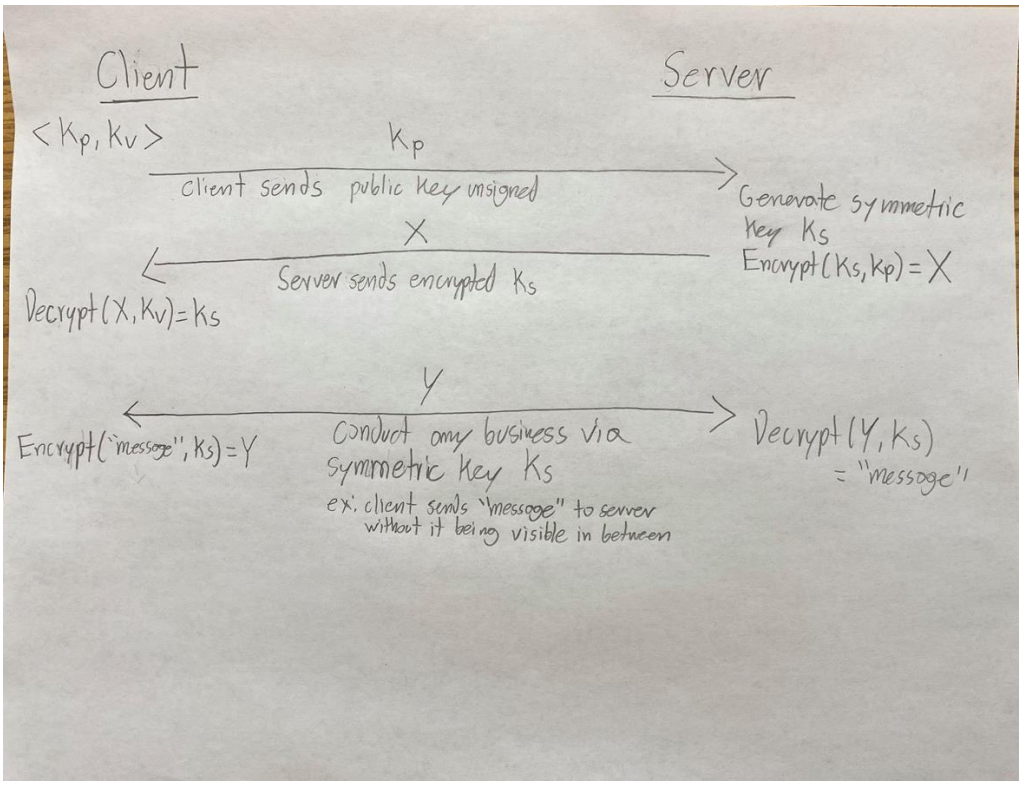
Technical Exercises

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. SSL key exchange (10 pts)

The SSL protocol does not involve the client (you) sending a public key. This is because this would be a bad design.

1. Write out the complete SSL protocol except where the client sends an unsigned public key instead of the server sending the public key. As steps, be sure to include symmetric key generation, all encryption and decryption steps, and all communications sent between client and server.



2. Why can't the client provide a signed public key in the same way as the server does in the actual SSL protocol?

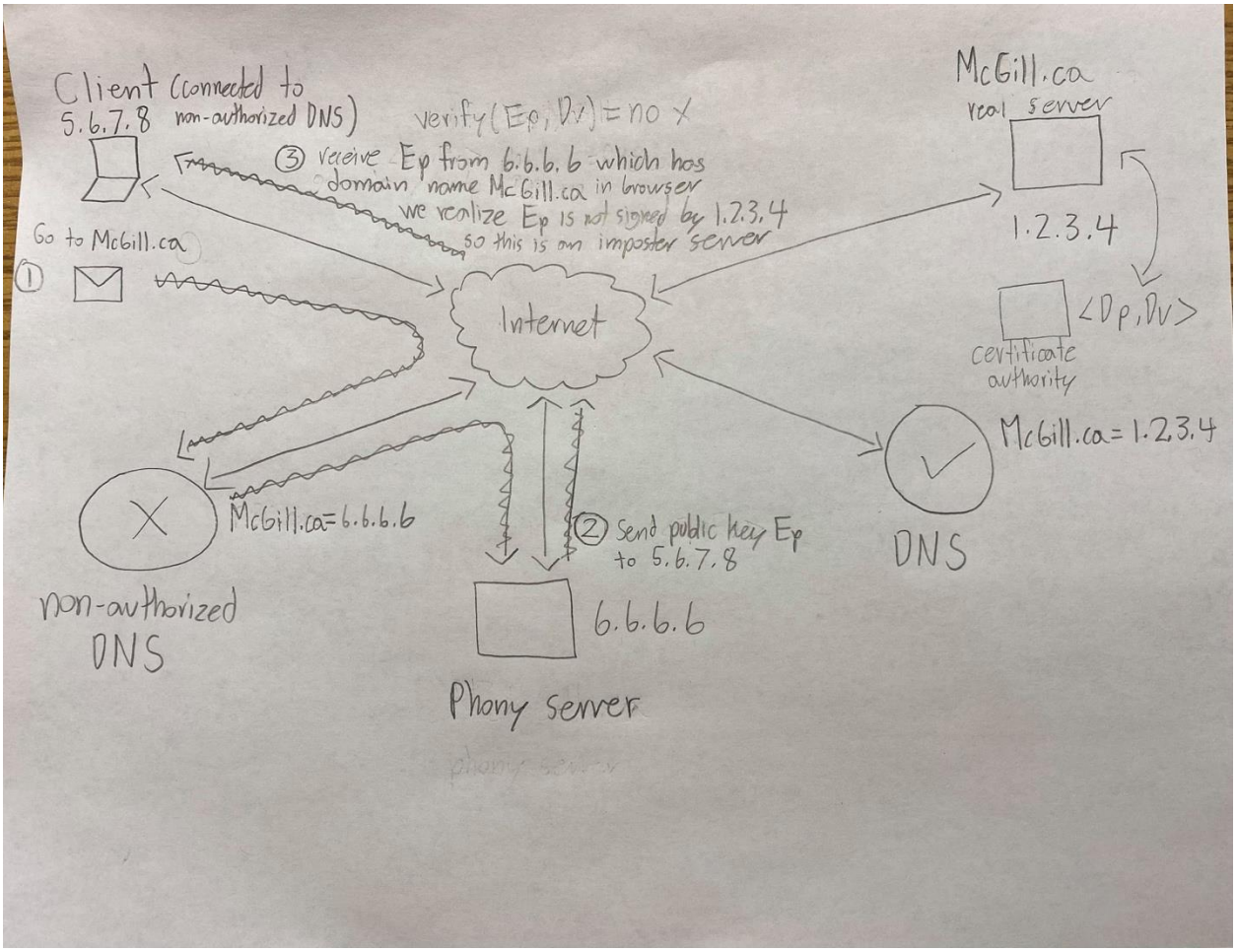
   The client cannot provide a signed public key the same was the server does because certificate authorities are tasked to sign public keys that belong to specific domains of websites. This is a way we know if the public key we receive really belongs to the domain we want to send information to. We cannot do this similarly with certificate authorities signing public keys associated with clients because we don't have an efficient way of distinguishing all computers from each other like domain names. This is because IP addresses of computers can be masked by VPNs and computers can share IP addresses in a common LAN thus making it much more inefficient to distinguish individual computers from each other. So, it is much easier to instead have certificate authorities sign public keys associated to specific domain names so clients can ensure they are sending information to the correct server which prevents DNS poisoning and man-in-the-middle attacks.

2. DNS Poisoning (10 pts)

1. A web browser is attempting to contact www.mcgill.ca. Explain how DNS poisoning enables an attacker to fool a web browser into connecting to a server that is NOT actually associated with the domain.

   DNS poisoning is giving non-authorized DNS servers wrong information. This is done when the DNS server is hacked and the domain of www.mcgill.ca is changed to an IP address of a malicious website. This happens in the situation where a user connects to public WIFI in a Starbucks but outside there is a van with a stronger WIFI network with same network name as Starbucks and has its own non-authorized DNS. The user can connect to this network thinking its Starbucks public WIFI and when going to www.mcgill.ca he will go to a different IP address of a site that looks like www.mcgill.ca but is not and his sensitive information can be stolen when typed to log in. Even though the domain typed: www.mcgill.ca is correct, the user does not know he is in a malicious website because the IP address attached to it has been changed via non-authorized DNS he's connected to.

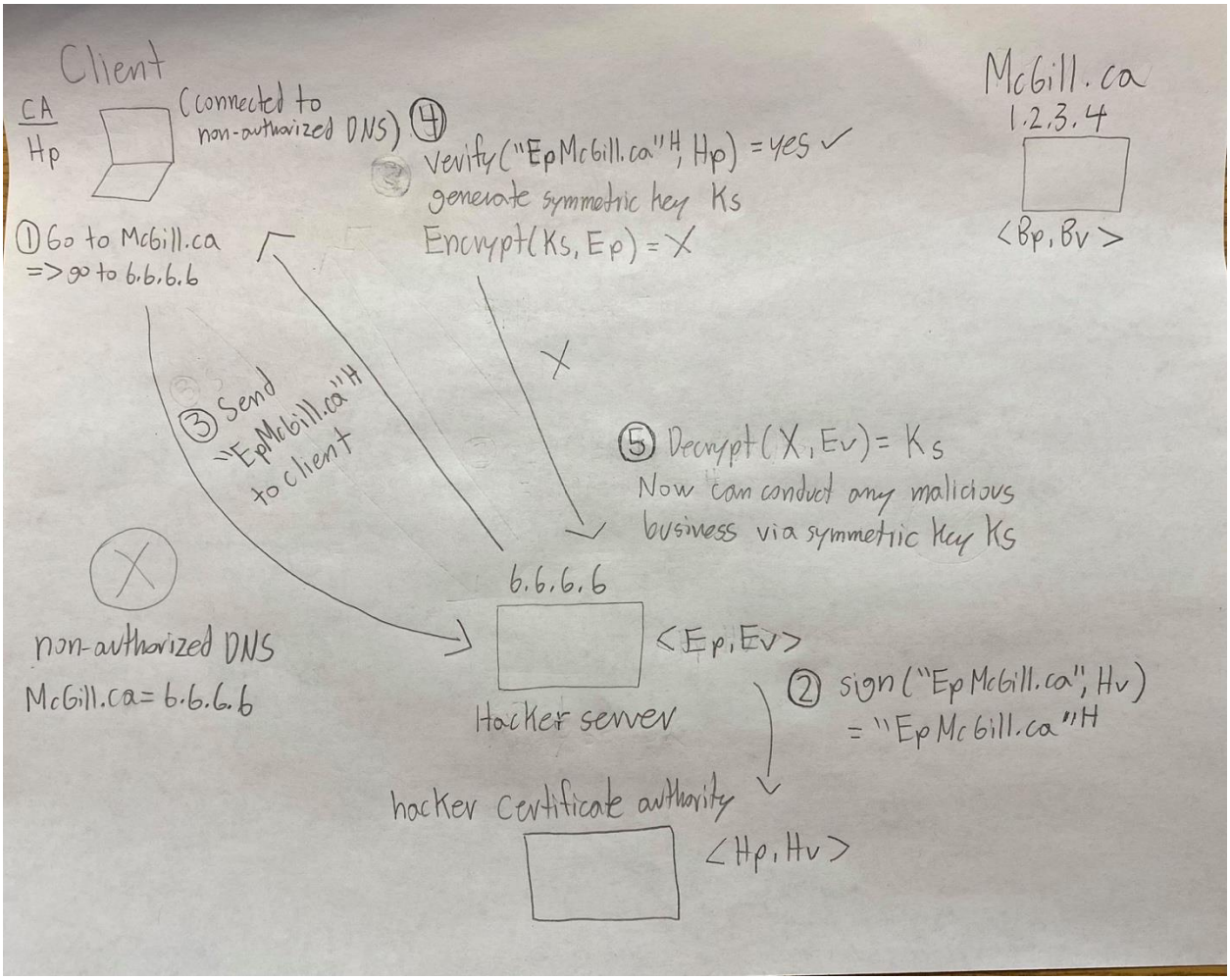
2. Diagram the SSL protocol that the web browser carries out with this phony server. Assuming that your browser is checking signed public keys, show where your web browser discovers that the server is an imposter.



3. Key hacking (15 pts)

A hacker has a key pair <Hp,Hv>. She hacks into your computer and adds Hp to the certificate authority public keys in your operating system. Later, you try to visit www.mcgill.ca but (as in Problem #2) you are subject to a DNS poisoning attack – landing on a server that belongs to the hacker who infiltrated your computer.

This time the attack succeeds because your computer is fooled by a signed public key. Diagram the successful SSL protocol, showing each key involved, each encryption/decryption/verification step, and each communication passed.



Discussion1

In the following questions, give a written answer (not bullet points).

1. Symmetric encryption (5 points)

Explain why we can't use ONLY symmetric encryption to keep all communications secret on the internet. Be precise – what aspect of symmetric encryption makes it impossible to keep secrets on the internet.

We cannot use only symmetric encryption to keep all communications secret because the sender and receiver must agree on a common key beforehand since both computers have never contacted each other before. There is no secure way to this as a hacker in between can see the common key passed if we try to send it. To fix this we must initially begin with an asymmetric encryption of the symmetric key using a public key and private key which prevents a hacker from being able to decrypt the symmetric key at any point in time. Once a symmetric key is safely communicated then we can safely communicate via this one symmetric key over and over.

2. Lost Private Key (6 points)

A bank discovers that its Thawte-signed public-private key pair has been copied and is now known to a group of hackers.

1. What are the implications of this?

   This is not good because these hackers can now easily decrypt the information you send in between as they have access to the private key which should never happen. Essentially the information you send in the network can be exposed and stolen by these hackers.

2. Does the bank have an ethical responsibility to disclose that its private key has been stolen? Why?

   Yes, the banks absolutely have an ethical responsibility to inform all customers that its private key has been exposed. Any one of their customers sensitive bank information is potentially exposed to these hackers and the bank must urge all customers to stop sending their private information to their sever or temporarily shut their server so no information can be passed until they resolve the issue by issuing a new private and public key pair.