AARHUS UNIVERSITY

Security Handin 4

Peter Burgaard - 201209175

May 12, 2015

QUESTION 1: In my answer, I assume the URL is the only thing which connects the server to its certificate in 'checkable way', that is, if the URL is not present in the certificate, we have no idea whether the given certificate is actually the particular servers certificate.

Given the above assumption, if this security check is not done, two given attacks comes to mind.

The first is an attack where the client unknowingly makes the SSL connection to our evil-minded server. In this attack we wait for our client to make a attempt to make an SSL connection with the given server. We redirect this request to our own evil-minded server, where we give our own certificate. Because the user cannot match the URL to our given certificate, his browser will probably happily do the SSL key exchange in good faith that its done with the server to which the URL actually belong. By doing this, we have our own SSL connection with our unaware client.

The second attack is a man in the middle attack. If we make a SSL connection to S, and we copy the above attack, but we give him the pms, we got from our own connection to S. This way we can forward/read/edit/delete the messages C is going to send to S, because all the communication goes through us. We can even for example, wait for C to perform a login of some sort, and then block their connections with S, and then continue were C's connection was cut. The only reason this is possible is because, C browser thinks it is communicating with S, given the certificate it receives is not checkable, as explained in our assumption.

Conclusion: The check makes all the difference!

QUESTION 2: Instead of checking the certificate it self, the browser could involve the user in the process of whether or not to trust the certificate. This could be done by, showing the user the owner or other information from the certificate, and make them either approve or disapprove the certificate based on the given information. Given the above assumption, the browser has no way to assess whether the certificate is actually belongs to the given server the user wants to contact. The only one who knows this is the users, so we need to involve them in the decision making process.

QUESTION 3: The client is the user. Only the user knows where they are headed, and so a responsibility is laid upon the user, to guide them selves in to their targeted destination. These security measures, which the SSL is one of, are only a way to enhance the users safety when guiding them selves to their target. Not an autopilot, which the user blindly can trust, always does the correct thing.