|  |  |
| --- | --- |
| **Choice 1** |  |
| **Choice 2** |  |
| **Q5** |  |
| **Q6** |  |
| **Q7** |  |
| **Total** |  |

**CSCE 813 – TEST**

**Spring 2014**

**Submit your answer via dropbox or hard copy by 4 pm**

**May 5, 2014.**

**See you at Finley Park on May 5th, 2014 4:00 pm!**

Answer any **two** of the following questions. Approximately ½ - ¾ page per question.

1. Applications Layer Security (20 points)
	1. HTTP does not directly provide session management. Describe one approach supporting security session management on top of HTTP.
	2. Consider the case when your organization uses an application-level proxy firewall to filter incoming requests. Explain how you can establish an end-to-end security (i.e., between the client and the server) such that none of the intermediaries (including the proxy firewall) should gain access to the message content. Why is it a difficult problem?
2. Transport Layer Security (20 points)
	1. Show how SSL supports mutual authentication of the server and the client? Why weak certificates create vulnerability of the protocol?
	2. Describe how the Heartbeat extension of the OpenSSL reduces the computational cost of establishing secure connection.
3. Network Layer Security (20 points)
	1. Your company wants to protect the data link when employees visit the website to work from home. Your supervisor wants to use SSL, you argue for IPsec. List the arguments your supervisor might use in favor of SSL. List the arguments that you would use in favor of IPsec.
	2. Assume that every computer in the Internet is fully capable to do IPSec along with the key management and security association management. Will there be any need for firewalls? Justify your answer.
4. Network Access Layer Security (20 points)
	1. You decided to secure the connection at the network access layer of the TCP/IP protocol stack. How would you configure the required connection? Describe and justify your choice for choosing protocols and security capabilities.
	2. A potential Denial of Service attack against secure end-to-end connection at the network access layer is by terminating PPP connections or L2TP tunnels. Explain how to launch this attack. As a defense, how could you prevent your attack?

Answer the following **three** questions. Approximately 1 – 1 ½ pages per question.

1. Web Application Security (20 points)
	1. Briefly explain how application characteristics and functionality mappings help the attacker to find application vulnerabilities.
	2. Define perimeter in the context of 1) traditional network security and in the context of 2) web application security. Why this change of perimeter creates a security vulnerability?
	3. What is the purpose of trust negotiation in the context of web application? Why do we need technologies to support trust negotiation?

1. Software Security – Operating Systems (20 points)
	1. Consider the security vulnerability discovered in Apple's iOS and OS X operating systems. The problem is based on the fact that the security certificates were not being checked properly (<http://www.bbc.com/news/technology-26335701> ) Check for additional publications on the issue and explain
		1. The main technical characteristics of the vulnerability.
		2. The impact of exploitation of the vulnerability.
		3. The recommended actions users can do to limit the damage of exploitation.
	2. Analyze whether the problem should be addressed from the perspective of security protocol, software implementation, or user awareness.
2. Application vs. Protocol Security (20 points)

Consider the manuscript D. Akhawe, A. Barth, P. Lam, J.C. Mitchell and D. Song, [Towards a formal foundation of Web security,](http://theory.stanford.edu/~jcm/papers/browsermodel-csf-2010.pdf) Proc. IEEE Symposium on Computer Security Foundations, July 2010.

* 1. Briefly describe the main claims of the manuscript and the authors’ support of the claims.
	2. Explain how cross-site scripting (XSS) attacks occur. (You can pick any variation of XSS.)
	3. Can we detect XSS problems using the approach presented in the manuscript? Justify your answer.