

**Optional Problem Set 4 (due December 13, 2009). [50 points]**

*The purpose of this Problem Set is to practice your skills to follow recent security challenges and gather information on your own. This is an individual assignment (no team work).*

**Problem 1 (30 points): Survey of Phishing and Pharming Prevention Techniques**

Phishing and pharming are important and growing problems undermining E-Commerce and the Internet in general. The assignment consists of surveying the recently proposed techniques to prevent pharming and phishing. You can use the following paper as a starting point but you should also get additional papers.

[http://sparrow.ece.cmu.edu/group/pub/parno\\_kuo\\_perrig\\_phoolproof.pdf](http://sparrow.ece.cmu.edu/group/pub/parno_kuo_perrig_phoolproof.pdf)

Your submission should be shorter than three pages. You can have as many additional pages for references as you want. A guideline for the outline of your submission is:

- What are pharming and phishing?
- What are the recent/most efficient/most popular techniques to prevent pharming and phishing?
- How efficient are these techniques? Provide your own opinion.

**Problem 2 (10 points): IKEv2**

Search the Internet for IKEv2 (RFC and other documents).

- Present IKEv2 messages exchange.
- Describe the services provided by IKEv2 and how it is different from IKEv1.

**Problem 3 (10 points): Kerberos PKINIT**

Present (succinctly and concisely) how Kerberos is extended to integrate public key cryptography in the initial authentication exchange? This extension is referred to as PKINIT.