EECE 571B, Spring 2012

Quiz #1

March 6, 2012

This quiz consists of 11 pages. Please check that you have a complete copy. You may use both sides of each sheet if needed.

Your Family name: __________________

Your Given name: __________________

Your student ID: __________________

Name of your left neighbor: _________________

Name of your right neighbor: _________________

#	Points	Out of
1		5
2		5
3		5
4		5
5		5
6		5
7		5
8		5
9		5
10		5
TOTAL		50

ATTENTION: When necessary, make reasonable assumptions and state them clearly in your solutions.

1. **What are the four most prominent characteristics of malicious Sybils in Renren OSN, that were used for detecting them? Briefly describe each characteristic, i.e., how that characteristic was different for malicious Sybils vs. legitimate accounts.**

2. Based on finding of Monarch authors, how are e-mail spam and tweet spam compared?

3. **a) What are the main differences between the approach in the adaptive password-strength meter (APSM) proposed by Castelluccia et al. and such meters as the one by Microsoft?** (Hint: this question is about the difference in the ideas, rather than characteristics of the approaches.)
   b) List advantages and disadvantages of the above two approaches, as compared to each other.

4. **List the key differences between the original Encrypted Key Exchange (EKE) proposal by Bellovin and Merritt and the original SRP proposal by Wu.**

5. **a) Define “detection rate” and “Bayesian detection rate” in the context of intrusion detection.**
   b) Based on the findings of Axelsson (i.e., “The base rate fallacy …” paper), what’s the main factor limiting the performance of an IDS?

6. **Summarize the pure fragmentation attack from “The Final Nail in WEP’s Coffin” paper that allows an adversary to decrypt any packet on a WEP-protected network, when it’s connected to the Internet.**

7. **Describe the adversary model in the fragmentation attack from the previous problem.**

8. **a) Summarize the idea of the countermeasure that the authors of the *optimistic* acknowledgment (opt-ack) DoS attack ("Misbehaving TCP Receivers …") propose.**

   b) Explain why it does not harm much the communications with benign clients and helps detect malicious clients.

9. **a) Define acronyms MAC and HMAC and explain the difference(s) between MAC and HMAC, as applications of hash functions. No need for exact HMAC formula.**

   b) Explain how one can use public key crypto to sign a message and to verify a signed message.

10. List the 10 principles of designing secure systems that were discussed in the security bootcamp.