EECE 512, Fall 2013

Quiz #1

September 26, 2013

This quiz consists of 7 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: _____

#	Points	Out of
1		5
2		5
3		5
4		5
5		5
6		5
TOTAL		**30**

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

1. **Explain the differences between isolated flow attacker and chosen flow attacker, as proposed in the paper on attacks on timing-based flow watermarks.**

2. **Explain the way an adversary who controls femtocell can circumvent IPSec communications with the security gateway to the back-end network, as reported in "Weaponizing Femtocells …" paper.**

3. **Describe the adversary model for the case of Dishonest Display Attack reported in "Security Analysis of India's Electronic Voting Machines" paper.**

4.

    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.

5. Explain the differences between authorization and authentication

6. **List the names of the 10 principles of designing secure systems that were discussed in the security bootcamp, and briefly explain each one.**

    1.

    2.

    3.

    4.

    5.

    6.

    7.

    8.

    9.

    10.