Quiz 3

Fall 2013 – EECE 512 – UBC

November 21, 2013

Candidate's name:

Candidate's student number:

Candidate's signature:

Remarks

1. No books, notes, or any other devices with text storage or communication capabilities are allowed.
2. Be brief and to the point.
3. **There are seven questions on this quiz. Each question is 5 points. Five best answers will be counted.**
4. The maximum score possible on this quiz is 25.
5. *The duration of this quiz is 50 minutes.*

This page left intentionally blank.

1. **Why did the authors of "Strengthening User Authentication through Opportunistic Cryptographic Identity Assertions" choose NOT to use a Near Field Communication (NFC) smartcard or dedicated token for the communication channel between the user's phone and the PC?**

2. **Why an adaptive password-strength meter is better in classifying passwords than a simpler scheme that classifies passwords as weak by counting the number of times a curtain password is present in the password database?**

3. **What are the stages in a typical attack profile, identified by the analysis of exploitation behaviors on the Web?**

4. **A telemetry study by Akhawe and Felt discovered that Google Chrome users were about 2 times more likely to click through an SSL warning than Mozilla Firefox users. What are the five passible causes for such a difference that their paper discusses?**

5. **What's the intuition behind the method for determining *authentication points* in "Adaptive Defences for Commodity Software ..." paper?**

6. **Explain the differences and similarities in the risks between 'wake-up' and 'bubble-up' modes of the meters that support automatic meter reading.**

7. **What are the capabilities that an adversary is assumed to have during the attack in order to conduct a *delay attack* on a real-time pricing system in a smart-grid?**