Quiz 2

Spring 2012 – EECE 571B – UBC

April 5, 2012

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.**
4. The maximum score possible on this quiz is 35.
5. *The duration of this quiz is 1 hour 15 minutes.*

This page left intentionally blank.

1. **List main conclusions suggested by the authors of “Why Phishing Works” [1].**

2. **Explain general (i.e., not specific to any particular scheme) differences (and similarities) between approaches to graphical passwords based on recall, recognition, and cued-recall.**

3. **Classify the following strategies for managing privacy in online social networks using the framework suggested in "We're in It Together" [2]**

   (a) Asking for approval before disclosing content from those involved

   (b) Avoiding publicizing content that could be problematic

   (c) Interpreting a potentially problematic issue to be non-serious

   (d) Asking another person to delete content

4. **What factors, according to "Mobile Security Catching Up?" [3], contribute to the security of mobile devices being different from common computer security?**

5. **Explain its assumptions and the solution for avoiding bandwidth starvation in the presence of DoS attacks on cloud infrastructure, as proposed by Liu [4].**

6. **According to the Facebook Immune System paper, which of the following are the <u>root causes</u> of threats to Facebook social graph? Check all applicable**

   - ☐ compromised accounts
   - ☐ malware
   - ☐ phishing
   - ☐ fake accounts
   - ☐ creepers
   - ☐ spam
   - ☐ none of the above

7. **List main results of "Efficiency of Vulnerability Disclosure Mechanisms" paper [5] in the single-vendor case.**

References

[1] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *CHI '06: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Montréal, Québec, Canada: ACM, 2006, pp. 581–590.

[2] A. Lampinen, V. Lehtinen, A. Lehmuskallio, and S. Tamminen, "We're in it together: interpersonal management of disclosure in social network services," in *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems*, ser. CHI '11. New York, NY, USA: ACM, 2011, pp. 3217–3226. [Online]. Available: http://doi.acm.org/10.1145/1978942.1979420

[3] M. Becher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, and C. Wolf, "Mobile security catching up? revealing the nuts and bolts of the security of mobile devices," in *Proceedings of the 2011 IEEE Symposium on Security and Privacy*, ser. SP '11. Washington, DC, USA: IEEE Computer Society, 2011, pp. 96–111. [Online]. Available: http://dx.doi.org/10.1109/SP.2011.29

[4] H. Liu, "A new form of dos attack in a cloud and its avoidance mechanism," in *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, ser. CCSW '10. New York, NY, USA: ACM, 2010, pp. 65–76. [Online]. Available: http://doi.acm.org/10.1145/1866835.1866849

[5] H. Cavusoglu, H. Cavusoglu, and S. Raghunathan, "Efficiency of vulnerability disclosure mechanisms to disseminate vulnerability knowledge," *Software Engineering, IEEE Transactions on*, vol. 33, no. 3, pp. 171 –185, march 2007.