Quiz 2 Key

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].**

   Sample Answer:

   - Even in the best case scenario, when users expect spoofs to be present and are motivated to discover them, many users cannot distinguish a legitimate website from a spoofed website.
   - Indicators that are designed to signal trustworthiness were not understood (or even noticed) by many participants.
   - The indicators of trust presented by the browser are trivial to spoof.
   - It is not sufficient for security indicators to appear only under trusted conditions—it is equally, if not more, important to alert users to the untrusted state.
   - A usable design must take into account what humans do well and what they do not do well.
   - Security interface designers must consider that indicators placed outside of the user's periphery or focus of attention may be ignored entirely by some users.

   □

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.**

   Sample Answer:
   All schemes are vulnerable to to shoulder-surfing and malware, as well as to MITM phishing attacks.

   In **recall-based** approaches, users have to reproduce a graphical password. It's inherently more susceptible to shoulder surfing attacks than the other two approaches since the user has to draw the whole password. The existing recall-based schemes are also vulnerable to malware attacks based on screen scrapers, and mouse-loggers. Since users choose their own passwords, a personalized attack may be more successful on recall-baed schemes than a general attack.

   Recognition-based systems generally ask users to memorize a portfolio of images during password creation, and then recognize their images from among decoys to log in. To remain usable, most such schemes have password spaces comparable in cardinality to only 4 or 5 digit PINs. Phishing attacks are somewhat more difficult with recognition-based systems, as a correct set of images must be presented to the user before password entry. Yet, phishing sites can launch MITM attacks against all existing recognition-based schemes. Shoulder-surfing is of particular concern in recognition-based systems, when an attacker can record or observe the images selected by users during login. The authentication server must know which images belong to a user's portfolio in order to display them, which makes recognition-based schemes vulnerable to attackers with access to server-side files.

   Cued-recall systems typically require that users remember and target specific locations within an image, an easier memory task than pure recall. A shoulder-surfing attack may reveal a user's password in a single login, as the entire password may be observable on the screen as the user enters it in the case of cued-recall schemes.

   □

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
   Sample Answer: collaborative, preventive, behavioural

   □

   (b) Avoiding publicizing content that could be problematic
   Sample Answer: individual, preventive, behavioural

   □

   (c) Interpreting a potentially problematic issue to be non-serious
   Sample Answer: individual or collaborative (depending on the issue), corrective, mental

   □

   (d) Asking another person to delete content
   Sample Answer: collaborative, corrective, behavioural

   □

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

   Sample Answer:

   - **Creation of cost**: there is a risk of the mobile device owner to be charged for services she did not meant to use.
   - **Network environment**:
     - Device's SIM-card is owned and controlled by the mobile network operator (MNO). As a result, the MNO has significant control over the device itself.
     - Firmware updates are critical for the purpose of keeping devices secure, yet they are difficult and expensive to perform.
     - Mobile devices can be managed and "killed" remotely by the MNO or via the device vendor services.
   - **Limited device resources**, compared to desktops, particularly the power source, battery.
   - Relatively **expensive wireless link** makes distributed algorithms impractical.
   - **Reputation of the MNO** might be jeopardized if the customers have negative experience due to security issues with their mobile devices.

   □

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].**

   Sample Answer:

   There is a monitoring agent which resides either in a different subnet or outside the cloud infrastructure, e.g., in a corporate data centre. The monitoring agent and the application constantly probe each other to see the available bandwidth in both directions. When the application notices that the available bandwidth degrades below a certain threshold, it starts sending a large number of UDP packets to the monitoring agent to ask for help. When the monitoring agent either detects a bandwidth deterioration or receives a help packet, it initiates application migration into a different subnet behind a different router. If the bandwidth to the new standby application instance is not sufficient, it keeps on launching new instances until it can find a free subnet. If the agent cannot find a free subnet in a few trials, it then starts to launch new servers in a different cloud provider. When it finds a good subnet to host the active standby, the agent converts it to be the main application. To prevent further attacks, one can optionally implement application hopping—moving the application from one subnet to another every few minutes before the adversary could launch enough servers in the new subnet to attack again.

   The proposed solution assumes that not all cloud providers are under attack at the same time.

   □

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

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

Sample Answer:

- ☒ 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.**

Sample Answer:

1. None of the disclosure practices, immediate public, full vendor, or hybrid, is optimal all the time. However, only one disclosure practice is optimal in a given scenario.
2. The grace period provided to the affected vendor cannot be the same for each vulnerability.
3. An early discovery improves the social welfare.
4. The society might not always be better off with an early warning system that disseminates the vulnerability knowledge to a selected set of users.

□

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.