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?**

   Sample Answer: The use of dedicated tokens has usability problems—e.g., requiring changes in user behavior (either to keep the token with the user or to place the token near the computer when authenticating); these user behavior changes violate their goal to keep the action of logging in invariant. An additional advantage of using a phone is that users already possess such a device, whereas otherwise they would have to obtain a special-purpose authentication device from somewhere.

   □

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?**

   Sample Answer: The simple scheme cannot generalize on common variations of weak passwords, e.g., “password1”. These variations have to become popular before the system can mark them as weak. The proposed adaptive password-strength meter can easily classify those variations as weak by leveraging capabilities of Markov models.

   □

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

   Sample Answer: A typical attack profile would include the following stages:

   1. A *s*cout bot would visit a page.
   2. Few seconds after the scout has identified the page as an interesting target, a second automated system visits the page and executes the real exploit.
   3. If the vulnerability allows the attacker to upload a file, the exploitation bot uploads a web shell.
   4. Several hours later, the attacker logs into the machine using the previously uploaded shell.

□

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?**

   Sample Answer:

   1. **Number of Clicks.** Google Chrome users click one button to dismiss an SSL warning, but Mozilla Firefox users need to click three buttons. It is possible that the additional clicks deter people from clicking through.
   2. **Warning Appearance.** The two warnings differ in several ways. Mozilla Firefox's warning includes an image of a policeman and uses the word "untrusted" in the title.
   3. **Certificate Pinning.** Google Chrome ships with a list of "pinned" certificates and preloaded HTTP Strict Transport Security (HSTS) sites. Users cannot click through SSL warnings on sites protected by these features. Certificate pinning and HSTS cover some websites with important private data such as Google, PayPal, and Twitter. In contrast, Mozilla Firefox does not come with many preloaded "pinned" certificates or any pre-specified HSTS sites. As a result, Chrome shows more non-bypassable warning.
   4. **Remembering Exceptions.** Due to the "permanently store this exception" feature in Mozilla Firefox, Mozilla Firefox users see SSL warnings only for websites without saved exceptions. This means that Mozilla Firefox users might ultimately interact with websites with SSL errors at the same rate as Google Chrome users despite having lower clickthrough rates.
   5. **Demographics.** It's possible that the browsers have different demographics with different levels of risk tolerance.

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

   Sample Answer: Authentication points are determined by monitoring application's execution flow when a user successfully authenticates, and comparing it with another flow produced from a failed authentication attempt.

   □

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

   Sample Answer: Readings transmitted by both types of meters can be eavesdropped, jammed, and spoofed. 'Wake-up' meters are also prone to battery drain attacks.

   □

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?**

   Sample Answer: The adversary is assumed to be able to modify either data packets sent to the smart meters or the smart meters' internal clocks.

   □