THE UNIVERSITY OF AUCKLAND

SECOND SEMESTER, 2008
Campus: City

COMPUTER SCIENCE

Software Security

(Time Allowed: TWO hours)

NOTE: Attempt ALL questions in the 12-page script book provided, using approximately 25 words to answer each 5-mark question, 50 words to answer each 10-mark question, and approximately 75 words to answer each 15-mark question.

Total possible: 100 marks.

A. Dwoskin and Lee, in "Hardware Rooted Trust…" describe a trust model and a usage scenario for their authority-mode SP devices. The following questions refer to a case in this scenario with the following security principals and objects.

- Firefighter P_f has an SP device S_f. Device S_f allows P_f to read building plans D_f.
- Paramedic P_p has an SP device S_p. Device Sp allows P_p to read medical records D_p.
- Building plans D_f are a subset of the records stored in a database maintained by fire department X_f.
- Medical records D_p are a subset of the records stored in a database maintained by public health department X_p.
- The SP devices are issued by emergency-response department X_e.
- Government G controls the fire department X_f, public health department X_p, and the emergency-response department X_e.
- Paramedic P_p should be allowed to read building plans D_f, using S_p, during any period of time that government G is operating in a state of emergency.
- Government G can declare any day to be the start (or the end) of a state of emergency.

1. Draw, and briefly discuss, a figure illustrating the trust relationships among the principals in this scenario. To receive full credit, your figure should be in the style of the diagrams in the cited article by Dwoskin and Lee. Arrows with dashed lines in your figure should indicate temporary delegations of trust, and arrows with solid lines should indicate permanent (or very long-term) delegations of trust. Briefly discuss each arc, indicating how it affects the transfer of data (and the authorisations for data access) between principals in the system. **(10 marks)**

2. Identify, and briefly discuss, one reference monitor in this scenario. **(5 marks)**

3. Define, and briefly discuss, two trust boundaries in this scenario. To receive full credit, you must identify at least one security goal of the guard of each trust boundary, and you must indicate what principal(s) serve as the guard for this boundary. **(15 marks)**

4. Dwoskin and Lee write that "… while we protect the confidentiality and integrity of the secrets and sensitive data, we do not defend against Denial of Service attacks." Briefly discuss this portion of their threat model in the context of an emergency similar to the 911 attack – in which a skyscraper collapsed, after being hit by an airplane that was under the control of terrorists. To receive full credit you must clearly state, and defend, one critical comment and one appreciative comment. **(10 marks)**

B. Alice is using an enhanced version of the OP web browser described in the required reading by Grier et al. This browser enforces the locked same-origin policies described in the required reading on “Dynamic Pharming Attacks…” by Karlof et al. Alice’s online bank accepts three types of authenticators:

- her password,
- an inkblot authenticator (similar to the one described in the required reading by Stubblefield and Simon), and
- a fingerprint.

Alice’s laptop has a fingerprint reader. Her OP web browser is able to forward her fingerprint minutiae to her bank, for authentication. Her bank will allow her to conduct online transactions, if she identifies herself with her bank account number and then provides any two of her three authenticators.

5. Draw, and briefly discuss, a figure illustrating the major components of this system. **(5 marks)**

6. Phil is trying to access Alice’s bank accounts, using the attack scenario described in “Social Phishing” by Jagatic et al. Briefly explain how Phil’s attack would proceed, indicating whether or not any of the security provisions in Alice’s online banking system would provide any defense. **(10 marks)**

7. Paul is another attacker who is trying to access Alice’s bank accounts. Paul has read the required readings on “Attacks on Biometric Systems: A Case Study in Fingerprints” by Uludag and Jain. Paul has read the articles on dynamic pharming and on Man-in-the-Browser attacks. Furthermore, Paul has a good education in computer science, and is able to implant a Trojan in Alice’s computer. Briefly explain how Paul’s attack might proceed, indicating anything else that he must know or be able to do in order to succeed. **(10 marks)**

8. Bob is the IT manager at Alice’s bank. He has read the article on “Password Memorability and Security: Empirical Results” by Yan et al. What requirements would Bob place on Alice’s passwords? **(5 marks)**

9. Sue is Alice’s friend. Sue has read the article on “Password Management Strategies for Online Accounts” by Gaw and Felten. What advice would she give Alice? **(5 marks)**

C. In “Strengthening EPC Tags Against Cloning”, Juels describes an authentication technique that is applicable to EPC Class-1 Gen-2 tags.

10. Briefly describe a scenario where authentication of a Class-1 Gen-2 EPC tag in a passport would provide a security advantage. To receive full credit, you must clearly describe this advantage by comparing your scenario to a scenario in which an EPC is read from a passport without any authenticating information from the EPC tag. **(15 marks)**

11. Franklin et al., in “An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants”, discuss an active underground economy. If the attack scenario described in Juels’ article is successful, there might be an underground economy in valid EPC tags for passports. Briefly discuss three security controls which, if implemented, would limit the impact of EPC cloning on passport security. For full credit, your controls must not all be architectural (in Lessig’s taxonomy), and they must not all be in the same category of Lampson’s taxonomy of defensive strategies. **(10 marks)**