Cover Sheet for Examination Paper to be sat in March 2006

COMPGA10: People and Security

Time allowed 2.5 hours

Calculators are NOT allowed

Answer THREE Questions
A mutual savings based in Frankfurt has a very large (1 m) and heterogeneous customer base, including business people who travel frequently and have complained about the cost and difficulty of conducting their banking via the bank’s telephone service.

The telephone banking service uses the following authentication protocol:

1. Full name
2. Account number (if this fails, move to step 3 and add steps 5 and 6)
3. 2 positions of a 6-digit PIN (if this fails, move to step 4 and add steps 5 and 6)
4. 2 specific characters of a 6-8 character password (if this fails, add steps 5 and 6)
5. Significant date
6. Name of the first school you attended

If the customer fails more than 1 of challenges 3-6, she is passed to a special authentication desk for a detailed assessment, which takes 5-8 mins to complete.

1a. Analyse the usability of the above authentication protocol from the customer’s point of view: what is the workload for the customer, and which steps might be particularly difficult?  

[12 marks]

1b. Analyse the vulnerability of the above authentication protocol – which type of attacks and attacker would be likely to succeed, and what countermeasures could you take to prevent them?  

[15 Marks]

1c. How would you improve the above authentication protocol in terms of usability and security? What technologies would you consider, and what would be the drawbacks?  

[6 Marks]

[Total 33 Marks]
2. Quisney Corporation runs a large amusement park in Northern Florida. Following 3 attempted abductions of young children, the company is looking to tighten up security and employ a range of technologies to provide “seamless security for all our visitors”.

2a. One proposal is to fingerprint all adults and children entering the park (using biometric fingerprinting equipment) and tie the children’s records to one or more adults’ records, so children can only leave with the adults they arrived with. Assess the usability implications of the proposed solution, and identify threats that this countermeasure is not effective against. Is this solution likely to be compatible with Quisney’s business?

[16 marks]

2b. Another technology being considered by Quisney is to add RFID chips to tickets as another way of tying children to accompanying adults. The idea is that RFID sensors deployed throughout the park (rides, restaurants, washrooms) would trigger an alarm if a child is detected without accompanying adult, and the company’s existing CCTV system could be used to locate and track the child while dispatching staff on the ground to safeguard the child and find the accompanying adult. Assess the usability implications of the proposed solution, and identify threats that this countermeasure is not effective against. Is this solution likely to be compatible with Quisney’s business?

[17 Marks]

[Total 33 Marks]
3. Risk is a key concept in security.

3a. Describe how risk analysis is traditionally employed in computer security.

[4 Marks]

3b. What is a risk register, and how can a risk register be used in the design and operation of a secure system?

[4 Marks]

3c. What is the difference between a traditional risk analysis and the AEGIS method? What are the benefits of the method for system developers, and the organisation commissioning a secure system?

[10 marks]

3d. John Adams developed a theory of risk perception, and how it influences human behaviour.

i. State the factors that influence people’s perception of risk. How can we employ this knowledge in the design and operation of a secure system?

ii. Describe Adams’ concept of a risk thermostat.

iii. One might argue that the discovery of a risk thermostat means “trying to mitigate risks in a secure system is pointless.” What can a designer of a secure system, or someone in charge of managing a secure system, do to counteract the effects of the risk thermostat?

[15 Marks]

[Total 33 Marks]
4. Please have a look at the attacked AOL advert on Internet security.

4a. Assess the suitability of the ad for the following purposes.
   i. to increase the security awareness of AOL customers
   ii. to help AOL customers avoid transferring viruses onto their home PC.

   [15 marks]

4b. Imagine you have been put in charge of “educating our customers about security” for an ISP such as AOL. Outline the stages of the campaign you would conduct. Then answer the following specific questions:
   i. which channels of communication would you use to communicate what information to your customers?
   ii. can this campaign be a one-off activity? Please justify your answer.

   [18 marks]

[Total 33 Marks]