Open Book Examination
Introduction to Computer Security (215010)

October 29th, 2007

University of Twente
department of computer science

Answer 6 out of 8 questions. Each question is worth a maximum of 8 marks.
Final mark = 50 marks paper + 48 marks exam + 2 bonus marks = 100.

1. The privium program at Schiphol airport allows its member to bypass passport checks by use of iris scans:

> *... The same advantage applies at the border check, which is directly followed by security. ... The identity is determined by the unique characteristics of the iris, which are stored, neatly encrypted, on the membership card. ... The whole process takes about 30 seconds and then – if everything checks out – a gate opens and the security check of personal items and hand luggage follows. If things do not check out (for example because the iris is not correctly recognized) the traveller can continue to the 'old fashioned' passport check. ... in the US, experiments with palm prints have been taking place for several years already, however that system has quite a few technical difficulties. The biometrics approach of Schiphol can be considered innovative: the accuracy of the iris-scan is much higher than other forms, such as the before mentioned palm print recognition and no other system lets the clients carry their own data with them. This last point is fundamental. "We have had to develop every thing ourselves" says Conny Lanza, "All existing technology assumes that data is stored in a database and we did not want that".* [Translated quote from B. de Winter in `wereldverkenning.nl', feb 2003]

Discuss why the designers chose to store the biometric profiles on a smartcard rather than in a central database. Give advantages as well as risks and disadvantages of both approaches for the different parties involved. Indicate how you would help protect against the risks that you mentioned.

2. Consider again the Iris recognition system of question 1. Biometric samples are never a perfect match and a threshold has to be chosen of when to accept a given sample.
   a) Discuss the consequence of a false accept and a false reject in this scenario and the threshold you would use.
   b) Sketch a graph showing the false acceptance and false reject rates for iris and palm print recognition as functions of the threshold. Also indicate your chosen threshold.

3. An online company allows you to store your personal data in an online database and share it with your friends. Costs are covered by advertisements shown when you access your data. Give a high level description of the system, identify different stakeholders. Briefly discuss possible threats to the interest of different stakeholders in the system along with protection mechanisms to help defend against the threats.

4. Explain, in one sentence each, why the following Java Features are not supported in JavaCard.
   a) Large primitive data types: long, double, float
   b) Parts of the API and exceptions
   c) Multidimensional arrays
   d) Characters and strings
   e) Dynamic class loading
   f) Security manager
   g) Garbage collection
   h) Threads

1. A->B: {A,K}pk(B)
2. B->A: {B}K

Figure 1: Authentication protocol. Here A and B are agent identities, K is a fresh key, pk(B) is the public key of agent B, {A,K}pk(B) is message (A,K) encrypted with the public key of B using a public-key algorithm (as in message 1), and {B}K is B encrypted with key K using a symmetric-key algorithm (as in message 2).

5. The protocol of Figure 1 aims at authentication of agent B to A.
   a) Is B correctly authenticated to A (explain your answer)?
   b) For what purpose is "K" included in Message 1? Is it necessary that "K" is fresh and unpredictable?
   c) Is "A" needed in Message 1? If yes, show an attack when "A" is not included. If no, explain why not.
   d) After the protocol execution, which secret has been established between A and B? Which party fully decides that secret?

6. Assume we try to adapt the protocol in figure 1 to a mutual authentication protocol.
   1. A->B: {A,K}pk(B)
   2. B->A: {nb}K
   3. A->B: {nb}K
   Where nb is a fresh random nonce generated by B.
   a) Explain why A is not correctly authenticated to B.
   b) Assume that A also has a public key, pk(A) and we change message 2 to
   2. B->A: {nb}pk(A)
   Is A now correctly authenticated to B (explain your answer)?

7. Briefly describe the following concepts and the setting in which they are used.
   a) Proof carrying code
   b) Mandatory access control
   c) Public key infrastructure
   d) Watermarking

8. Complete the following table linking the network related security tool or method, its goal and a short description.

Tool	**Goal**	**Description**
Intrusion detection system	*Detect network attacks*	*Detect behaviour corresponding to known network attacks or unusual behaviour.*
Virus Scanner		
Sandbox		
Needham-Schreuder-Low Protocol		
	prevent IP spoofing	
	no weak passwords	
	find ill configured network machines	
	analyse behaviour network attackers	