Open Book Examination
Introduction to Computer Security
215010

October 27th, 2008

University of Twente
department of computer science

Answer 6 out of 8 questions. Each question is worth 15%.

Illegible answers or excessively long answers will not be marked.

1a) Explain in one sentence why security cannot be perfect.
1b) Give three important characteristics of "economically feasible" security.
1c) What is the common purpose of access control and accountability?
1d) Give three essential differences between access control and accountability?

2a) List three different biometric techniques that you deem appropriate for preventing unauthorised access to heavy, dangerous equipment, such as aircraft and mechanical diggers, and explain in one sentence why the technique is appropriate both from the usability and security point of view.
2b) Draw a desirable Receiver Operating Characteristic for the heavy, dangerous equipment application, indicating the area on the curve that corresponds to the best compromise between the FAR and FRR and describe the consequences of the FAR/FRR settings for the usability of the system.

3a) RFID tags are a potential threat to people's privacy, especially when attached to items purchased in shops. It is relatively easy to disable an RFID tag permanently during checkout. However, an operational RFID tag could provide some useful services to the customer. List three uses of RFID tags after the purchase of expensive, RFID tagged goods.
3b) List three methods than can be used to disable an RFID tag, either temporarily or selectively.

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

5) Brinkman's secret sharing technique[1] represents the hierarchical structure of an XML document as a polynomial. His technique deals exclusively with the tags of the XML document, not with the data contained in the document. How would you extend Brinkman's secret sharing scheme to deal with the data?

6a) Give the three most important properties that a cryptographic hash function should have.

6b) How could a cryptographic hash function be used to authenticate keys in authenticated broadcast for wireless sensor networks?

7a) Give the general reason why it is a bad idea to use RSA with the same public/private key pair for message signing and for message confidentiality.

7b) A blind signature can be used to decrypt a message. Show how this attack can be achieved by a carefully constructing the message to be signed.

7c) How could this attack be avoided?

1. A→ B: PZL,R
    B computes X := F(<t,R,S>) and Y := F(<t,R,X>)
2. B→ A: YES,Y
    A searches for <t',R',X'> such that F(<t',R',X'>) = Y
3. A→ B: SYN,t',R',X'
    B checks that F(<t',R',S>) = X' and t ≈ t' and assumes that R = R'

Figure 1: Simple Client Puzzle protocol. Here S is a secret known only to B, t is the local time of B, F(.) is a one-way function, <...> is the concatenation of its arguments, and R is a request parameter.

8a) Given the client puzzle protocol of Figure 1. On average, how many searches must A perform in step 2? Explicitly state any assumptions on probability distributions that you are making.

$2^{\#bits(t',R',X')}$

8b) Assume that B wants to control the amount of work performed by A by disclosing n bits of X. On average, how many searches must A perform in step 2?

8c) When would the assumption R = R' in step 3 be justified? • not many collisions.

8d) If A can search for <t',R',X'> such that F(<t',R',X'>) = Y, then A could also try to search for <t',R',S'> such that F(<t',R',S'>) = X' and thus discover the secret S'. How could this be avoided?

[1] [Bri04b] R. Brinkman, J. M. Doumen, and W. Jonker. Using secret sharing for searching in encrypted data. In W. Jonker and M. Petkovic, editors, 1st VLDB Workshop on Secure Data Management in a Connected World (SDM), volume LNCS 3178, pages 18-27, Toronto, Canada, Aug 2004. Springer.