UNIVERSITY OF EDINBURGH

FACULTY OF SCIENCE AND ENGINEERING

COMPUTER SCIENCE FOUR

COMPUTER SECURITY

Wednesday 24 April 2002

14:00 to 15:30

Examiners:

Prof. K. Turner (External)

Prof. C. Stirling (Chairman)

INSTRUCTIONS TO CANDIDATES

Answer any TWO questions.

All questions carry equal weight.

1. (a) Explain the meaning of the terms *authentication* and *authorisation* with respect to notions of access control used in computer security. [*4 marks*]

(b) Consider the access rights $A = \{\mathsf{exec}, \mathsf{read}, \mathsf{append}, \mathsf{write}\}$ of the Bell-LaPadula security model, and the subjects and objects below:

$$S = \{\text{Alice, Bob, Charlotte}\}$$
$$O = \{\texttt{type.exe}, \texttt{alice.msg}, \texttt{bob.plan}, \texttt{mail.log}\}$$

(you should assume that the objects containing a principal's name are owned by that principal).

Give an *access control matrix* for S, O, and A, which assigns the minimal set of permissions such that: (1) the owner of any file is allowed to read or write to it; (2) everyone has execute permission for `type.exe`; (3) everyone has read permission for `bob.plan`; (4) a file ending in the extension `.log` can be appended to by anyone. [*4 marks*]

(c) Imagine that Charlotte has written a Trojan horse program `type2.exe` which she then advertises to the other users as an improved version of the `type.exe` program. In fact, before executing the improved functionality, her program attempts to read a file named <*user*>`.msg` and store the contents in a hidden file owned by Charlotte called `stolen.msgs`.

Show the minimal ACLs (*access control lists*) for the new objects added by Charlotte which would allow this attack to work in general, and maintaining the policy rules from part (b). Then describe the access control checks that happen when Alice executes Charlotte's program. [*6 marks*]

(d) Consider a *multi-level security* (MLS) system with three clearance levels $\mathsf{unclassified} \leq \mathsf{confidential} \leq \mathsf{topsecret}$. Charlotte works as an administrative assistant and has maximal security level unclassified. Alice and Bob, meanwhile, have confidential clearance. Assuming that each object is given the maximal classification of their owners, explain how the Trojan horse attack by Charlotte is prevented in the MLS system. What is the name of the property of MLS systems that prevents this attack? [*5 marks*]

(e) Consider a larger multi-level security system with the same clearance levels as before, but with the addition of two *approval levels*, $\mathsf{external} \leq \mathsf{internal}$. External objects are those which have been granted approval for release from the organization, and internal objects are those which must not be externally released.

Design a lattice for the six security levels which combine a clearance level with an approval level. Explain informally the meaning of the system high and system low levels.

If a user with the highest clearance level wishes to release a top secret document outside the organization but also to let Alice read it, what is the maximal security level it can be assigned? What is the maximal level if Charlotte must also read the document? [*6 marks*]

2. BAN logic can be used to reason about public-key cryptography, using the assertion form:

$$\stackrel{K}{\longmapsto} P \qquad\qquad P \text{ has } K \text{ as a public key}$$

together with some appropriate rules. The private key corresponding to K is written as K^{-1}.

(a) BAN logic with both $\stackrel{K}{\longmapsto} P$ and $P \stackrel{K}{\longleftrightarrow} Q$ assertion forms can be used to analyse protocols which use both public-key and symmetric-key cryptography. Briefly describe an application which uses both forms of cryptography, explaining their respective roles. [*4 marks*]

(b) Suggest a rule expressing the closure of observations for a principal P for messages encrypted under P's public key K. [*4 marks*]

(c) The following public-key protocol is to be analysed using BAN logic.

$$\begin{array}{lll} \text{Message 1} & A \rightarrow S: & A,\ B \\ \text{Message 2} & S \rightarrow A: & S,\ \{\, K_b,\ B,\ T \,\}_{K_s{}^{-1}} \end{array}$$

Alice (A) wishes to talk to Bob (B) so she contacts the server (S) to ask for Bob's public key. The server responds with a *certificate* containing Bob's public key, which is encrypted under the server's private key.

i. What does T stand for in the certificate, and what is its purpose? [*3 marks*]

ii. What is the fundamental property of a *reversible* public-key encryption scheme, and why does this protocol assume it? [*3 marks*]

iii. Convert this protocol into *idealized* form. [*3 marks*]

(d) A suitable *message meaning rule* for reversible public-key encryption is:

$$\frac{P \models \stackrel{K}{\longmapsto} Q \qquad P \triangleleft \{\, X \,\}_{K^{-1}}}{P \models Q \mid\!\sim X}$$

Using this rule in the first step, give a BAN analysis for the idealized protocol from (c)iii. You should clearly state and justify the starting assumptions, and show in detail a proof of $A \models \stackrel{K_b}{\longmapsto} B$. [*8 marks*]

3. (a) The *Vinegar toy cipher* is a polyalphabetic substitution cipher with a block size of 3, that operates on octal digits $\mathcal{A} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and uses three alphabet rearrangements, rotating the alphabet right by 2, 3, and 5 positions, respectively.

   i. Encode the plaintext `123452034521` using the Vinegar cipher.

   ii. What is the main reason that the Vinegar cipher is only a toy, and how would you cryptanalyse this cipher?

   iii. How can the polyalphabetic substitution cipher be improved to make an unbreakable cipher, and what's the disadvantage of this method? *[9 marks]*

(b) The Vinegar cipher is to be improved by converting it into a product cipher of the previous substitution and a simple transposition cipher, which has a block size of 4, and is specified by the permutation $\{1, 2, 3, 4\} \rightarrow \{3, 2, 4, 1\}$. The combined cipher has a block size of 12.

   i. Encode the plaintext `123452034521` using the revised Vinegar cipher.

   ii. Name a simple way of improving the strength of the revised Vinegar cipher, without adding any new cryptographic operations.

   iii. What is an inherent disadvantage of the revised cipher, shared by many unadorned encryption schemes such as DES and RSA? Explain how you could rectify the disadvantage. [**Hint:** the name *Salt and Vinegar toy cipher* has been suggested for the rectified cipher]. *[7 marks]*

(c) One use of RSA is to sign a message and then encrypt the resulting signature. Consider the following table of exponentials under two RSA moduli $n_A = 62894113$ and $n_B = 55465219$:

x	y	n	$x^y \bmod n$
4382681	5	62894113	54383568
1368797	37726937	62894113	59847900
59847900	5	55465219	38842235
38842235	44360237	55465219	4382681

Suppose A's public key is $(n_A, 5)$ and private key is $d_A = 37726937$. Suppose B's public key is $(n_B, 5)$ and private key is $d_B = 44360237$. A now signs a message represented by the integer $m = 1368797$, and encrypts the message for B. By using the figures in the table, answer the following questions:

   i. What is the signed message s and its encryption, c, produced by A?

   ii. B now wishes to decrypt the message and verify the signature. What is the decrypted signed message, c', and the result of verifying the signature, m', both calculated by B?

   iii. Explain why the signature in (ii) does not verify.

   iv. In general, what is the probability of this failure arising? Suggest two ways of regulating this usage of RSA to address the problem. *[9 marks]*