OLLSCOIL NA hÉIREANN
THE NATIONAL UNIVERSITY OF IRELAND, CORK

COLÁISTE NA hOLLSCOILE, CORCAIGH
UNIVERSITY COLLEGE, CORK

SUMMER EXAMINATION 2000

Fourth Year Computer Science

CS 4993: Computer Security

Professor J. G. Hughes,
Professor C. J. Sreenan,
Dr. S.N. Foley

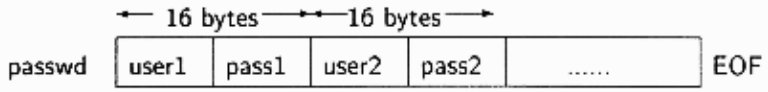
Answer Three questions

$1\frac{1}{2}$ Hours

1. (a) Describe how the RSA scheme is used to implement digital signatures, and how these in turn are used to implement public key certificates. *(15 marks)*

   (b) Alice and Charles know Bob's public key K_B. Bob knows Alice's and Charles' public keys as K_A and K_C, respectively. Describe how Alice should send a secret message to Charles. Note any weaknesses in your approach. *(15 marks)*

2. A server maintains details of users and their passwords in a file composed of sequences of 16-byte records, each one giving an 8 character user-id and 8 character password. The file is encrypted under key K using DES-ECB.



Client systems (who share K) maintain copies of `passwd` for local user authentication. The server periodically broadcasts copies of `passwd` to clients over a public network.

$$Msg1: \quad Server \rightarrow Client: \quad \{\texttt{passwd}\}_K$$

where $\{\texttt{passwd}\}_K$ represents the cleartext password file encrypted under K.

(a) Describe how a client should use K to authenticate the server. *(8 marks)*

(b) Outline an attack on the password file that would enable a user to gain unauthorized access to somebody else's login account on a client. *(10 marks)*

(c) Suggest how the attack could be avoided. *(10 marks)*

(d) What advice about designing security protocols would you give to the designer of this system? *(2 marks)*

3. (a) Outline how and why the S/KEY one-time password scheme works. *(15 marks)*

(b) A bank provides one-time password key-fobs to customers who wish to do their banking over the Internet. Each customer is given a unique key-fob which generates fresh time-based pass-codes at 30 second intervals. Each key-fob is tamper-resistant and stores a master secret key K (known only to the bank) and its owner's *userid*. A key-fob calculates the pass-code as $(\{time\}_K, \{userid\}_K)$. When a customer attempts to login, she provides $(userid, passcode)$; the remote bank system decrypts the pass-code fields, matches the use-rid and checks that the time is current.

Outline an attack on this scheme that would allow an eavesdropper gain access to a another customer's account (without having to steal the victim's key-fob). *(15 marks)*

4. (a) Explain how a multilevel secure system might be used to provide a defense against malicious code. How would this approach differ from a *wrapper* based approach? *(10 marks)*

(b) A multilevel secure system has only one printer which is used to print jobs at all security levels. It is in a secured area and printouts are carefully labeled. A multilevel secure (trusted) print queue manager accepts requests from subjects at any security level. Its operations are:

i. `lpr <filename>`. Assign job number and add file to print queue. Returns `job#` to requester.

ii. `lprm <job#>`. Remove specified print job. Returns `success` or `failure`.

Sketch suitable algorithms that describe the behaviour of the above operations taking care to ensure that multilevel security is preserved. For the sake of simplicity it is not necessary to consider printer controls/scheduling. *(20 marks)*