CSci 530 Midterm Examination (Fall 2006)

Instructions: Show all work. No electronic devices are allowed. This exam is open book, open notes. You have 100 minutes to complete the exam.

Please prepare your answers on separate sheets of paper. You may write your answers on the sheet of paper with the question (front and back). If you need more space, please attach a separate sheet of paper to the page with the particular question. Do NOT extend your answer on the back of the sheet for a different question, and do NOT use the same extra sheet of paper to answer more than one question.

In particular, each numbered questions must appear on separate pieces of paper so that the exam can be split for grading. Be sure to include your name and USC ID number on each page.

There are 100 points in all and 4 questions.

1. (20 points) Cryptography
    1. For the following encryption methods, indicate whether the method provides (unconditional/provable, strong, weak, or no) levels of confidentiality and integrity. (12 points)
        1. DES in Cipher Block Chaining mode. Confidentiality_____ Integrity _____
        2. Encryption using an RSA private key. Confidentiality_____ Integrity _____
        3. Encryption using an RSA public key. Confidentiality_____ Integrity _____
        4. Encryption with a one time pad. Confidentiality_____ Integrity _____
        5. AES in Cipher Block Chaining mode. Confidentiality_____ Integrity _____
        6. AES in Output Feedback Mode. Confidentiality_____ Integrity _____
    2. The performance of many forms of public key cryptography is slower than typical systems for conventional cryptography, yet there are many reasons to use public key cryptosystems for security. Explain the approach typically used to provide confidentiality and integrity for medium to large messages that still has the benefit of using public key cryptography, but which also addresses the performance concerns. In you answer be sure to describe how different keys are used, and discuss the cryptographic techniques that are applied (8 points).

2. (25 points) Key Management for Digital Signatures -

    Alice and Bob have each been asked to come up with individual key management solutions for digital signatures in their company.

    Bob suggests that the company just use the conventional method for public key systems. That is, each employee / department uses their own key generation mechanism and stores the private key for their own use and stores the public key on a well known publicly accessible server.

    Alice suggests that instead of putting employees public keys on a public server, all public keys of individuals and departments are stored only on a local server with access to only company employees. Only a single public key of the company would be made available on a public server and it would be signed by a third party for assuring the association to all outsiders. Whenever an outsider needs to communicate with an employee, they encrypt the message with company's public key. When it reaches the company's server, the server uses the internally available public key for the employee to encrypt the message further with this key. The employee has both private keys which can decrypt this double encrypted message.

    1. What are the limitations of Bob's approach?
    2. What are the limitations of Alice's approach? What about the approach is troublesome? Can you suggest possible improvements upon Alice's approach?

3. (25 points) Managing Trust -

   For each of the systems and services listed below, explain which entities (people, processes, servers, hardware) are relied upon for the expected service to be provided securely and for the expected assurance (e.g. confidentiality, authentication, etc) to hold. For each subpart of this problem (3.1, 3.2, etc) give an example where the security is compromised if one of the trusted parties does not act in the way that it is supposed to act. Please note that in grading this question, your score will depend on how strong an example you provide - i.e. you may provide a correct example but might get full credit if there is a better one that you miss. There will, however, me multiple examples that can get full credit.

   1. Cross realm authentication using Kerberos of a user at USC to a server at MIT.
   2. PGP or GPG authentication of an email message from someone that you do not know personally.
   3. Authentication of your bank's online server when you use online banking through and SSL or TLS protected session in your web browser.
   4. Public key based authentication for SSH (this one is a little bit tricky).
   5. Validation/authentication of the software running on a client computer using trusted computing?

4. (30 points) Design problem

   You have been hired by a consortium of online game facilitators to design the next generation security architecture for online games. A recent problem for gaming companies is the use of Phishing and malicious code to steal the identities of legitimate users, whose characters online wealth is then stolen and passed on to other characters.

   Your first task is to advise the consortium on the design of an authentication system by which users will prove their identity (and hence the ownership of their online persona) when playing a game. The system you suggest should allow a user to prove his or her identity only when using legitimate, unmodified (i.e. no cheats) versions of the online game, and the approach should be resistant to attempts to steal a user's identity by malicious software such as viruses or bots that might have infected the user's computer.

   1. Describe a system that meets the design goals set forth above? (Before answering, please read question B, so that the parts of your answer that best fit there - are left until part B).
   2. Describe the enrollment and registration activities needed by your approach? Who maintains information about registered users? Are users registered or just characters / personas? What information might be known about each online identity? Discuss the tradeoffs of maintaining particular pieces of information about users and characters, and discuss where each such piece of information might be maintained? Justify your answer.
   3. Discuss the impact of your approach on the usability of the game, and the impact it may have on legitimate users of the game? Are you placing new requirements on what is needed to play the game that might reduce the number of legitimate users? Can you suggest steps that might be taken to allow new users to join the game as an impulse decision (i.e. without having to wait).
   4. How do you see your approach evolving as the technology typically found on computing desktops changes? Are there specific changes you would suggest be made to future desktop computers, and especially those sold as gaming platforms?