Final Examination
CS 236
On-Line Program
Computer Security
Spring 08

Answer all questions. All questions are equally weighted. The test is open book/open notes. Be sure to provide enough details to demonstrate that you really understand what the questions are talking about.

1. In Kent, Lynn, and Seo's paper on Secure BGP, they describe several criteria for correct and secure BGP operations, and state that their protocol handles six of these eight criteria. Secure BGP does not ensure that sending peers correctly applied BGP rules and local routing policies, nor that the receiver correctly applied BGP rules and local routing policies. Why do the mechanisms in Secure BGP fail to deal with these issues? What could be done that would deal with such issues? (Do not merely repeat the statement in the paper that "the semantics of BGP itself would have to change." I want more details showing your understanding of the issue.)
2. IPSec can be run in multiple modes, producing different security effects. In class, we discussed two such modes, ESP Tunnel Mode and ESP Transport Mode. Which of these two modes is more suitable for implementing a virtual private network? Why?
3. It was recently discovered that Ubuntu Linux had a security flaw based on zeroing out a newly allocated page of memory. The contents of that page was combined with the process ID of the running process to seed a pseudo-random number generator, which in turn was used to generate cryptographic keys for SSL and SSH. Ubuntu effectively has 15 bit process IDs. Why was this a security problem? The problem arose when programmers used a tool called Purify that flags problematic code that is likely to have security problems; the difficulty was caused by the programmers taking Purify's advice, which was not to use uninitialized data. Why does Purify give this advice, and why was it bad advice in this particular case?

4. Consider the following examples of use of biometrics for authentication or identification. For each, indicate the advantages and disadvantages of using the proposed biometric method for this purpose. Indicate if there are unspecified elements of each example that have a significant bearing on whether it is a good or bad use of the biometric.
    a. A large shopping mall plans to install cameras throughout the mall to observe patrons' faces. These will be compared by automatic face recognition software to pictures of patrons who previously visited the mall, which in turn are correlated with data about the stores they visited and the products they bought on previous trips to the mall. Matches will result in customized discount coupons being automatically printed in mall stores and offered to the matching patrons when they enter those stores.
    b. A company that analyzes drug tests for athletes wants to replace the security guard they have at the only entrance to their building with a fingerprint reader, to save money. The company has 100 employees, receives regular deliveries of specimens for analysis daily, and gets relatively few visitors. All employees will be fingerprinted, and will need to put their finger on a fingerprint reader to open the locked door, but there will no longer be a guard or secretary stationed observing people entering the building.
    c. A company proposes to replace physical credit cards with a system whereby a user registers his retinal pattern with a bank and is given a line of credit similar to that of a normal credit card. To make a purchase at a store, the customer will have his retinal scan taken, which will allow the store to determine if the customer has suitable credit. To handle Internet purchases, the company will market a cheap retinal scan device that can plug into the USB port on a typical home computer. The user will log into his computer, have his retinal scan taken through this device, and then proceed to shop. When credit checks are required, the retinal scan taken at login time will be transmitted across the network.