Final Examination

CS 239, Spring 2002

Answer all questions. All questions are equally weighted. The test is open book/open notes.

1. Consider a network intrusion detection system that is performing packet sniffing on a network of several hundred machines located behind a firewall. Each of the following issues will raise certain difficulties for the IDS system. Describe the difficulties and what (if anything) can be done to deal with them.

    a. Some attacks divide their malicious payloads across multiple packets, and it is not always possible to detect them by looking at any single packet.

    b. Some traffic between hosts in the network and remote hosts outside the firewall is encrypted for legitimate purposes.

    c. High scale flooding DDoS attacks may penetrate the firewall.

2. Some people advocate building an alternative Internet backbone by having homeowners and other interested parties put up wireless antennae and use their home computers to serve as routers. Such a network would perform hop-by-hop wireless routing from end user machines to any other point in the Internet, possibly eventually connecting to the regular backbone, possibly traveling only on the wireless network. What are the special security concerns for this proposed new infrastructure that are different than the security concerns related to operating the existing backbone? What approaches should be taken to overcome such problems?

3. Consider a distributed operating system meant to operate in a tightly connected environment. The system is intended to support dozens to hundreds of machines belonging to a single organization located in close physical proximity, perhaps in one building or a campus setting. The total number of supported users is close to the number of machines. The operating system provides all users easy access to all files stored on all machines, and the designers of the system want to use a Unix-like access control mechanism for the files. What are the special security problems that the system must solve to provide this form of access control in this environment that were not of concern in a single Unix machine?

4. Consider a system in which users dispatch software agents into the network to perform tasks for them. Some of these tasks involve communicating with network services that require authentication. The owning users may wish to limit the access privileges available to their software agents to a subset of what the users themselves can access. Assume a very large number of users, a large number of network services, and many agents per user with varying needs between different agents and different users (i.e., different agents for the same user get different privileges, and agents of the same type acting on behalf of different users get different privileges). Describe a common authentication service to be used between agents and services for this scenario.