CS 239: Security for Networks and System Software

Final Exam

June 16, 2000

This test is open book, open notes. You may use any material you have with you, but you may not consult with anyone else.

Answer four of the five questions. All questions are equally weighted. These are large, complex questions, and I do not expect utterly complete answers on any of them. If you do a pretty good job on all four questions, you will do well on the test. Demonstrating that you understand large, important issues is more important than details, writing style, or neatness. BUDGET YOUR TIME CAREFULLY!!! Not answering one question at all or in the most superficial way will likely lead to an extremely low grade.

1. Consider a company that sells an interactive Internet game. While it receives some money for selling the game software itself, its major income is from monthly fees for players to continue participating in the game. The nature of the game is such that it encourages interaction and competition among players. The company maintains a large on-line database of information related to the state of the overall game, which is consulted and updated constantly by the software that implements the server side of the game. What security problems does this company face? What mechanisms should they implement to solve those problems? Keep in mind that their major source of income is from subscriptions of players who interact with the game in real time over the network.
2. The US government has been disappointed with how slowly its agencies responded to recent viruses and worms. Hours or even days after the threat has been discovered, machines in these agencies were still being infected by these malicious programs. One proposed solution to the problem is to design a system to deliver security updates automatically to all machines under the control of any US government agency. When a new threat is discovered, the announcement of its discovery would automatically propagate to all government machines, allowing faster response to the threat. Design such a system, paying special attention to the security issues, but not neglecting practicality and performance.
3. Some people postulate that in the near future many people will have a personal area network that connects various computing and communications devices (watches, PDAs, intelligent eyeglasses, cellular telephones, etc.) that they carry around on their bodies. The personal area network would handle communications between these devices and provide a wireless bridge to the rest of the machines in the world. The personal area network itself would probably be based on low-power wireless technology, such as Bluetooth. Is a firewall an important component of a security solution for a personal area network? What challenges must be overcome to use a firewall in this environment, or what factors make firewalls unsuitable for this use? Is an intrusion detection system a valuable component of a security solution for a personal area network? If so, describe how it would help. If not, describe why it is unhelpful.

4. The music industry has a severe problem. Music can be easily transformed into digital formats that allow reproduction at sufficiently high fidelity for most purposes. These formats are relatively compact. The industry would like to sell access to music over the Internet using these formats, but they are concerned about the safety of this intellectual property. Once the digital format has been delivered to a single user, they want to prevent that user from making copies of it and delivering them to many other users, who presumably would not pay for them. What technical approaches to computer and network security would provide some help for the music industry?
5. Up to the present, fortunately no one has combined a worm with a distributed denial of service attack. Consider the following combination of the ideas: a hacker injects into the Internet a malicious program that first seeks to silently spread. At some predefined moment, all existent copies in the network start a denial of service attack. Simultaneously, they try to spread to other machines, from which they will continue the attack. The worm could easily seek to spread widely, both in numbers and in geographic/network-topological scope. What could be done to prevent such an attack from ever happening? What could be done to stop it once it an attack had started?