Massachusetts Institute of Technology
6.915: Network and Computer Security
Professor Ronald L. Rivest

Handout 3
September 14, 1995

Problem Set 1

This problem set is due on *Thursday, September 21, 1995* at the end of class.

Each solution is to be handed in *separately*, i.e. on separate sheets of three-hole punched paper. If the solution to a single problem takes more than one page, staple together only the pages relative to the same problem. Mark the top of each sheet with your name, 6.915, the problem number, and the date.

If you collaborate with other students, you MUST write up solutions on your own and acknowledge the people you work with.

Readings: Chapters 1, 11, 12, 13, 15 and Section 9.4 of Pfleeger

Problem 1-1. Security Evaluation for your Personal Computer

Perform a security analysis for your personal computer. (If you don't have a personal computer, imagine that you have an IBM laptop with an internal modem, a 360MB hard disk, and an internal floppy, running Microsoft Windows 3.1, or else pick your own favorite personal computer configuration.) First of all do the risk analysis following the steps on page 458 of Pfleeger (you need only use what you think are the four most important vulnerabilities of your system). Based on those threats describe a plausible security policy (e.g. always lock door, hide sensitive floppies, regular backups, etc etc). Also describe an emergency plan in case of a disaster (fire, earthquake, etc.)

Problem 1-2. Backup

Regular file backups are a main tool for security. At the same time they are a security problem by themselves.

Why do we do backups? What do they help us to achieve? Think in terms of general security goals.

How many backups should one save? Only the last one? Or many of them?

How should the backup tapes be stored? Encrypted? If so who should keep the encryption key?

Who should perform backups?

Problem 1-3. Access control versus availability

The combination on the doors of the Athena clusters is a rudimentary form of access control.

However only authorized users can use Athena Workstations because of the login procedure. Then why do you think there is a combination lock on the door of the clusters? What security purpose does it fulfill?

During R&O week the combination number was clearly displayed on the SIPB whiteboard outside the main cluster in the 5th floor of the student center. This was done in order to make the system available to the new students. Clearly access control and availability are conflicting requirements. Comment on the way the conflict was solved in this particular case and suggest better approaches.

Discuss two other examples of the conflict between access control and availability.

Problem 1-4. Physical Security Devices

Do you think there is a need for shredders in the Athena Clusters? What about a degausser for floppy disks? Justify your answers.