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

Handout 9
October 3, 1995

Solutions to Problem Set 1

For some of the problems in this homework there were no "real" solutions. So we will just comment on the way students answered the questions and what were the most common opinions in the class.

Problem 1-1. Security Evaluation for your Personal Computer

In general students did a good job on this. Some people were not very neat in their presentations or gave an incomplete evaluation missing some features (as estimation of savings when putting some controls on etc) The most common accidental vulnerabilities were recognized as

- power surge (not too likely)
- accidental deletion of data and software, including hard disk failure (moderately likely)
- spilling food on the computer (very likely)

The most common malicious attacks were recognized as

- theft (not too likely)
- disclosure of confidential data (moderately likely)
- intruders (for machines connected to the net)
- viruses from public–domain software (very likely)

The most common control was to have timely backups. Other popular controls included

- a software to protect against viruses,
- a password software to protect confidential data from occasional users of the system,
- covers for the computer
- locks

Most people realized that there are some controls they have not in place that are cost effective. Some people stated that they are going to think about this.

In case of disaster almost everybody realized that the most important thing to save is the data. Hardware and software can be replaced, data is at times irreplaceable. Again backups stored on a different place (here at MIT this could mean for example on Athena) are going to help.

Problem 1-2. Backup

We do backups in order to achieve the two goals of *integrity* and *availability*. Backups do not help for confidentiality, actually they work against it since they provide an extra entry point to the data for a potential attacker. Almost everybody realized this.

People suggested many different backups policy. The right answer depends of course on what kind of system and application we are discussing. In general it's smart to save several last backups.

Backups should be performed by someone who is allowed access to the data of all users in the system. In general the system administrator. Because of the confidentiality problem mentioned above, backup tapes should be saved encrypted and the encryption key stored in a different place than the tapes. Also some people suggested that such key should be kept by more than one person. Indeed if only the system administrator has the key and he's unavailable during an emergency the backup becomes useless.

Problem 1-3. Access control versus availability

The answers to the questions "Why is there a combo on the door of Athena clusters" were varied. First of all people noticed that it is not true that only authorized users can use Athena Workstations because of the login procedure. Indeed the root password is known to all the users of the system and someone could still login as root even if his/her account has expired. Moreover some services (as library access) are available on Athena even without logging in. Such users have very limited privileges but for example they could create a denial of service problem in a crowded cluster (as at the end of a semester.)

The other most common reason people suggested was to protect the actual hardware from vandalism and theft. Another reason that came up was that the combo is there to protect the users of the system, although I don't see why MIT students need special protection while they are in an Athena Cluster, while the rest of the campus is easily accessible.

Almost everybody realized that writing the combo on the board outside the cluster was not the best solution. However almost everybody claimed it was not such a big deal because random "wanderers" are not likely to be in that part of campus. Alternative suggestions were to distribute the combo inside the freshpeople package (although this would create plenty of paper copies of it) or to communicate the combo orally to the new students when they check in.

People brought many different examples of the conflict between access control and availability (an amazing number came from examples of fraternity lifestyle.) I found the following one suggested by Matt Fredette particularly interesting.

> X also has an access control and availability conflict, because it has no concept of different levels of access. If I make my X display available to anyone, no matter how strongly authenticated, I cannot control what they can do with my display - they can pop up as many windows as they want, as opposed to the one or two that

> I may want them to pop up, and they can snoop on most of the windows that *I* have opened on my display.

Problem 1-4. Physical Security

Answers were unanimous for a "no" on degaussers. Shredders received one third of "yes" and two thirds of "no". The main motivation for the opposition to such devices is that Athena is used for educational purposes and so the data residing on the system should not be that confidential after all.