Report of the CSAIL Prox Card Privacy Committee

May 24, 2007

**Background**

In April 2004 CSAIL constituted the Prox Card Privacy Committee in response to privacy concerns of some Laboratory members regarding the use and possible abuse of information collected by the Laboratory’s card entry system. The Committee held an open meeting on 29 April 2004 led by Hal Abelson, Ron Rivest and Danny Weitzner.

Following this open meeting a working group consisting of Hal Abelson, Ron Rivest, Danny Weitzner, Lissa Natkin, Ben Adida, Simson Garfinkel and Keith Weinstein had a series of meetings with representatives from the MIT Card Office and the MIT Campus Police to learn the technical details of the system and make recommendations. The group had occasional meetings in the spring, summer and fall of 2004.

**Findings**

The CSAIL’s card access system consists of several parts:

- In each MIT ID card there is a **Radio Frequency Identification (RFID) chip** which transmits a persistent identifier when interrogated with a wireless signal.
- **Readers** stationed around the laboratory constantly transmit wireless signals to RFID chips. When chips are detected a signal is sent to the panel responsible for the door stationed near the reader.
- **Panels** located in secure locations receive signals from readers. Panels control the lock mechanisms. Each panel can also communicate with a central computer operated by the MIT Card Office. Panels also contain a small amount of cache memory. This memory can hold a list of individuals approved to open a door, as well as door open/close events.
- **Network Connections** between the Panel and the Card Office’s prox card server. In most cases the network uses dedicated wires or a secure VPN connection.
- **An Authentication Server**, located at the Card Office in the basement of the MIT Student Center. This authentication server is loaded on a regular basis with a list of each member of the MIT community and the doors on campus that they are allowed to open.
- One or more **Client Stations**, which make it possible to monitor the status of particular doors, individual cards, and view various logs.

In addition to the card access system, the Committee learned of several other surveillance systems:

- There are video surveillance cameras in the Stata Center (not within CSAIL) located at the loading dock and on the first floor. In total, there were 106 such cameras on campus in June 2004. Some of these cameras work, some of them don’t. In some cases the video is archived, in other cases it is not.
• There are many wireless access points in CSAIL which can record the MAC address of laptops. It is possible to monitor laptops and Wi-Fi enabled PDAs or cell phones as they move through the laboratory using these access points.

Regarding the operation of the prox-card system, we found:
• The prox card system is part of the Stata Center’s integrated access control, burglar alarm and fire alarm system. It cannot be turned off.
• Nevertheless, most people entering or leaving CSAIL do so without being monitored by the system. This is because the laboratory’s doors are usually unlocked. Only individuals using their MIT ID card to gain access in the early morning, evening or night have their actions monitored.
• Most doors at CSAIL that are equipped with automatic locks have two sensors—the can detect if they are open or closed, and they can detect if they are locked or unlocked. Thus, a door can detect if it has been forced open.
• The system has the capability to log every card access and door opening.
• Although there is a belief on the part of both the community and the MIT Campus Police that the system can be used for solving crimes, the Campus Police was not able to provide the Committee with a single case in which log information from one of the campus access control systems had directly resulted in recovery of evidence that led to a crime being solved. When there has been an on-campus theft in the past, the logs have been useful for people to interview or exclude from an investigation. This saves the Campus Police time and makes their officers more effective in the investigation.
• Despite the fact that the log files have not generated evidence useful in solving a crime, the campus police are of the opinion that the system acts as a deterrent against both property crime and violent crime. Reasons for the deterrent include the keeping of the logs and the ability to deactivate a card in the event that it is lost so that it cannot be used by an unauthorized individual.
• Most property crime at CSAIL has not required the use of a card, either because the thefts have occurred during the day (when a card was not needed), because doors or windows have been left open, or because thieves have been able to force access.

CSAIL is equipped with a parallel access system that uses metal keys. Regarding this system we found:
• There are many doors at CSAIL that can only be opened with a metal key. This includes office doors, equipment closets, and so on.
• Although prox cards can be used to open the glass doors in the elevator lobbies, next to each glass door is an unlockable firedoor. Opening the fire door normally causes an alarm to sound, but the alarm can be disabled through the use of a physical metal key.
• There is no mechanical locking mechanism for the doors securing the Knight Lab; when locked, these doors can only be opened using prox cards.
• There exist several “master keys” at CSAIL—metal keys that have the ability to open multiple doors on a floor or in an area. Some of these keys were used in construction; other keys are being used on a daily basis by the cleaning staff.
• Some physical keys, including some master keys, may be unaccounted for.

Regarding system policies, we found:
• There was concern among some administrative employees that the prox card system might become a kind of automatic time card, keeping track of employees that arrive early or leave late. We found no policy statement from any part of the Institute that would preclude this use of the system, nor did we find evidence that such tracking was being practiced.
• We were told in June 2004 that the MIT Card Office holds a record of all uses of the MIT Card (both approved and denied) for 90 days. In May 2007 the MIT Card Office Privacy Policy stated that card use information is only retained for 14 days before it is erased. The policy may have been changed in the past three years, or the website may be inaccurate.
• The Card Office Privacy Policy further states that information may only be used for system troubleshooting or at the request of the MIT Police Department when accompanied by a request signed by the Chief of Police. We found that employees in the Card Office generally have unrestricted access to this database and that their accesses are logged but that the logs are not useful, because somebody generally logs into the system and then leaves themselves logged in for the whole day. An MIT student project that issued its report in December, 2004 reached a similar conclusion.3
• The MIT Card can also be used to enter and exit the Stata Center Garage. Entrances and exits to the garage are retained for three years by MIT Parking & Transportation in a computer system that is not physically connected to the computer operated by the Card office.

Recommendations:

Based on these findings, we make the following recommendations:

In order for CSAIL to have a prox card system with privacy practices that are good enough for everyone to live with, these basic requirements must be met:

1. The system must have a clearly-stated privacy policy with a reasonable retention period. We believe that the 14 day period currently proposed is acceptable. To this end CSAIL should verify that the MIT Card Office stated retention policy of 14 days is in fact being implemented. Specifically, CSAIL should verify that the database is being purged of transactions older than 14 days, and it should also verify that the database is not itself being backed up in a way that would allow transactions older than 14 days to be recovered in violation of the stated policy.

2. In order to assure adequate accountability to system policies, there should be regular (no less than annual) audits for compliance, based on comparison of the access logs with logs of approved access requests from Campus police.

3. There must be adequate data security practices in place for the data being stored.
Until these conditions are met, Lab members people should be able to opt out of the system by using metal keys so that they can gain access to their area without the need to utilize the prox card system.

- We have not discussed whether the expense of these keys should be borne by the requesting individual or the laboratory, nor what the procedure should be in the event that a key is lost.
- We have also not discussed whether there will be a record of the names of those requesting metal keys or the conditions under which that list will be made available to campus police, other officials, or the public.

4. The committee finds that the privacy questions raised by the prox card system are just a small subset of the larger privacy questions raised by other surveillance technologies we have documented (wifi access points, video systems, etc.) in use at MIT. There is an important class of technology and policy research questions that could be fruitfully addressed on the MIT campus. We note the general lack of practical policies at many institutions that deploy prox-card-like systems, and also the need to do privacy research in new network environments. We believe that such research could make a valuable contribution to our technical and social understanding of the impact of sensor networks and many other new technologies developed at MIT but likely to be used around the world.

2 http://web.mit.edu/mitcard/privacy.html
3 http://swiss.csail.mit.edu/6.805/student-papers/fall04-papers/mit_id/mit_id.html#cardofficeprivacy