

Report on Physical Security of Facilities and Hardware

Andreas Koeller and Joseph Youn
Academic Computing Committee
Montclair State University

February 10, 2004

1 Introduction

In an effort to provide modern technology in the classroom, many academic institutions, including Montclair State University, invest heavily in valuable hardware that is deployed in publicly accessible areas on campus. Due to the high value (especially, resale value) of some of those hardware items, problems of theft are quite significant. Vandalism also exists. This report assesses the physical security situation on the MSU campus and makes recommendations for improvements.

2 Relevance to the Academic Computing Committee

The Academic Computing Committee typically deals with issues of the appropriate use of information technology in education. The core task of this committee is the recommendation of technological solutions to problems in teaching.

Ideally, the committee's recommendations, if adopted by the community, will lead to an increased use of meaningful technical solutions, such as (digital) data projectors, laptops, and "smartboards". Such technology can lead to improvements in the effectiveness and efficiency of teaching.

However, even if convinced of the advantages of information technology in the classroom, instructors will adopt new technology only if it is reasonably easy to use and permanently available. Availability and reliability are essential preconditions to the acceptance of technology by instructors, and are the factors most affected by the lack of physical security. If an instructor cannot rely on a projector to work or even to be physically present in a classroom, he or she will not be willing to use projectors as an integral part of the classroom experience.

3 Scope of this Report

It is not within the reach of this ACC subcommittee to conduct a study of physical security issues with any amount of statistical relevance. Therefore, the issues raised here are of an anecdotal nature. However, we believe that our concerns are valid and that our recommendations are reasonably easy to implement and will lead to improvements in security.

4 Security Concerns

The MSU campus is subject to a variety of physical security issues, some of which affect information technology. Those issues are detailed out below.

4.1 Room Access Control

Access to rooms is regulated by three different means: traditional cylinder safety locks using metal keys, combination locks, and swipe card locks. Each of those lock mechanisms is subject to security problems, as detailed below:

4.1.1 Cylinder Locks

The main problem is the availability of master keys, which enable a person to gain access to a large number of rooms. Loss or theft of master keys is a major concern. We have received numerous complaints from faculty about the perceived or actual abuse of master keys. One member of the faculty had laptop computers stolen from his locked office, while another professor reported a number of valuable books stolen in this way.

Publicly accessible documents (recently published by the IEEE [Institute of Electrical and Electronics Engineers]) contain documentation on ways to generate master keys from simple keys for the most common type of cylinder lock, such that the security of any cylinder lock is seriously in question.

4.1.2 Combination Locks

Combination locks are subject to problems of key sharing. If access to a room is allowed to a group of people, each person in this group must know the combination of the lock. Passing this combination on to friends or unauthorized colleagues weakens the lock's security. Frequent changes of the combination, in response to security breaches or other events, raise the problem of memorizing the code. Codes are often written down, compromising security further.

4.1.3 Swipe Card Locks

Swipe card locks are the safest of the three options. However, a security concern remains.

The current generation of swipe card locks uses off-line technology. Each swipe card in the system has a unique identifier (a number), while each lock maintains a database of accepted card identifiers (numbers). If a swipe card is lost or a swipe card owner leaving the university does not return his/her swipe card, that card's identifier must be physically removed from every lock that the card owner had access to. If a highly authorized card (such as a campus police officer's card) is lost, hundreds of locks have to be reprogrammed to no longer include this card's identifier. Such reprogramming currently requires a lock expert to physically access each lock. Only a small numbers of employees at MSU are trained in reprogramming swipe-card locks, which often leads to delays and omissions in lock programming.

4.2 Unlocked Rooms

Leaving doors open is one of the most common sources of compromised security. There are a number of reasons for open doors, most importantly the difficulty to lock a door and a lack of responsibility on behalf of the person who should lock the room.

Difficulties in locking doors arise from a number of sources. We have received reports stating that a number of cylinder locks and keys on campus are cut with high tolerances, such that some keys do not fit some locks in which they are supposed to work. The mechanical difficulty to even lock a door tempts instructors to ignore the lock and leave doors unlocked for extended periods of time (often overnight).

Furthermore, a common issue in teaching a class is that students take a significant amount of time to vacate a room after a lecture. Often, instructors leave the classroom without waiting for the last student to leave. Even if the last student to leave a classroom closes the door, many doors protected by cylinder locks will not lock automatically when closed. Even in rooms using swipe card locks, which do lock on closing, instructors often wedge the door open to accommodate students who are late. Such wedges are rarely if ever removed by the last student to leave, such that the security of such swipe-card-locked doors is also compromised.

4.3 Access Control inside Rooms

Once an intruder gains access to a room, theft of equipment becomes trivial unless the equipment is secured further. Expensive hardware (such as projectors, monitors, computers) that is left in open rooms is most affected by theft, but even cheap items like remote controls or cables are often stolen as an act of vandalism or simply due to the ease of stealing.

Such theft can be prevented by locking down the hardware itself (or locking items inside cabinets, even with simple mechanical locks). In the case of projectors, this can be partially accomplished by bolting the projector to the ceiling. This measure is not perfect since given enough time and resources even steel pipes attaching the projectors to the ceiling can be sawed off using an electric saw.

At MSU, recent technology investments are protected by fiber-optic alarm cables wrapped around projectors and other equipment. Cutting such a cable will trigger an alarm with the campus police. If the police response time is low enough, such a system can prevent theft even from unlocked rooms. However, such a measure does not prevent theft of remote controls, power supplies, cables, special “smartboard” markers, and other small but important items.

5 Recommendations

It is important to understand that physical security can never be perfect. The benefit of additional security lies in the fact that the cost (effort) that an intruder needs to invest increases. The goal of adding security measures is not to make intrusion impossible, but simply to raise the cost (to the intruder) to a level beyond the possible rewards gained by theft. Once it becomes too expensive to steal an item (for example if expensive tools are needed to break a lock or if the danger of detection and punishment is sufficiently high), the incidence of theft will decrease dramatically.

5.1 Status

MSU has begun to address some of the security concerns raised above. Most importantly, MSU is in the process of contracting with an outside vendor to implement a “one-card solution” for a number of services on campus. Those services will include parking, student registration, a debit card system for campus convenience stores, and most importantly, physical access control.

The one-card solution, once implemented, will extend swipe-card access to more classrooms on campus, and will therefore make those rooms more secure. The new card locks will have

networking capabilities, which means that the addition and removal of authorized swipe-card ID numbers can be accomplished from a central office. There will no longer be a need to reprogram locks by physically accessing the lock. If implemented, this feature will make it significantly easier to remove ID numbers from locks if they are no longer authorized.

In addition, swipe locks will be used on perimeter (building) doors. This new feature will add another level of security to the entire campus, since one more barrier needs to be breached by an intruder in order to access facilities.

5.2 Procedural Recommendations

Technical solutions (see below for some additional recommendations) will never be able to completely address security. Below is a list of procedural remedies to security problems that we identified in our study.

5.2.1 Patrols

Students and faculty must become more aware of the danger of leaving rooms unlocked. A solution implemented by a few universities (Cornell, Barnard) involves forming teams of two or three students who **patrol** academic buildings on a regular basis and identify open doors and other security problems. Such teams may simply shut a (self-locking) open door or alert the campus police or another entity to the security problem. If a security problem is found, students may leave a note (e.g., a PostIt-note) at the door in question or at the equipment that could have been stolen, alerting instructors and students to the potential danger. Patrols could be implemented on a work-study basis and could be a minor addition to the university budget with potentially high rewards.

5.2.2 Awareness

Another solution could be to inform students that their tuition is used to purchase hardware, such that theft will lead either to higher tuition or lower-quality instruction. This might raise the level of awareness among students, such that they might cooperate in closing doors and locking rooms. This is a cost-neutral measure that can reduce the incidence of crimes of opportunity.

5.2.3 Reporting

A further cost-neutral measure could be to implement an anonymous hotline (or email address) to which students can report information about ongoing or past thefts, which might lead to reductions in the theft rate.

5.3 Technological Recommendations

The new security features that will be implemented by MSU's contractor can be complemented by additional security. A few recommendations for additional technological security features are:

5.3.1 Lock Cables

Large and expensive hardware is currently protected by fiber-optic cables whose removal will trigger alarms at the campus police headquarters. A supplemental protection mechanism could be the locking down of large stationary equipment by steel cables or similar means. We recommend to require that newly purchased stationary equipment must be attached to tables or walls by steel cables or bolts. Laptops should also be protected inside faculty office by laptop locks.

5.3.2 Lock Maintenance

This issue is partially addressed by the above proposal: Users who are no longer authorized to enter a room must surrender their access key or card.

It must be noted here that MSU's future ID card contractor will *not* initially be required to replace *existing* swipe-card locks, such that the hundreds of non-networked card locks currently in place will remain in use for a significant amount of time. That means that even in the new system, if a card gets lost, stolen, or otherwise removed, the card's ID number must be removed from some locks. This removal must occur within hours or days, not weeks or months, of the loss of the card. Some additional staffing might be necessary to increase the speed of lock updates, until the centralized swipe-card lock system is ubiquitous on campus. This measure will incur additional cost unless lock maintenance can be improved with the available staff resources.

5.3.3 Equipment Identification

Permanent identification of equipment is a strong deterrent to theft. This is an open issue, since it is difficult to make recommendations on how to *permanently* mark a device. Stickers are an insufficient technology since they can easily be removed. For plastic cases, a heat-based stamp (which imprints marks into a plastic case by melting the material) might be used.

It can be expected that non-removable asset tags and a thorough and accurate device registration procedure will further reduce theft. However, the increased use of leased equipment at MSU might make the implementation of this recommendation difficult, since such equipment cannot be permanently marked as MSU property.

5.3.4 Universal Access Cards

In the process of enabling one-card access for many facilities on campus, a solution recently implemented by Rutgers University deserves some consideration. Rutgers announced that they will issue facility access cards to every person on campus, including one-time visitors, using a system similar to hotel room key cards. Such a measure could enable the university to permanently lock building doors, which will prevent unauthorized outsiders to even enter university buildings. High accountability of legitimate card owners due to card identification is an additional advantage.

5.3.5 Funding for Security Measures

Faculty who receive equipment or research grants often purchase expensive hardware that has to be protected from theft and vandalism. In order to provide small-scale funding for simple security measures protecting such equipment, MSU could require that for each purchase of theft-prone equipment from grant money, a fee has to be paid to the college's or school's technical coordinator, who will then provide physical security for the equipment. Such a measure will also increase awareness of security problems among faculty.

6 Concerns of Privacy

Most of the suggestions given in this report do not affect privacy. However, implementing our recommendation to use Rutgers-style Universal Access Cards would allow an observer to track a person's movement on campus. In the matter of such cards, we believe that since the academic buildings of a university form an office-type environment (as opposed to a home-type environment), some degree of trackability is acceptable.

Naturally, certain sensitive non-academic areas must be treated with care. For example, university health services, psychological services, and some other areas of administration must be accessible to students without requiring them to use their unique access card. Also, the possibility of tracking students' access to dormitories raises significant privacy concerns. Such tracking might become possible with the introduction of networked swipe-card locks, even if the actual transmission of data from the lock to the data center is encrypted (as the university requires from its future contractor). However, any recommendations pertaining to non-academic environments are beyond the scope of this report to the Academic Computing Committee.