The MIT ID Card System: Analysis and Recommendations

Priya Agrawal

Neha Bhargava

Chaitra Chandrasekhar

Al Dahya

J.D. Zamfirescu

December 10, 2004

Contents

List of Figures

List of Tables

Introduction

The MIT ID Card serves as a primary form of identification for all members of the MIT community. Advances in technology have made it possible to expand the functionality of the MIT ID Card over the years to provide many conveniences, including access to various facilities and the use of TechCash for purchases. However, these added comforts have come at a price: the security and privacy of MIT Card users. Technical problems - such as the theft of information on an MIT Card and the ease with which the card can be duplicated - have already been demonstrated, and seriously compromise the security of the card. The privacy of individual card-owners is at also a serious concern with the current card system, which has the ability to track users by keeping information on every transaction, including entries and exits to and from campus buildings. Our report aims to analyze how these issues affect the MIT ID Card system and the MIT population as a whole. In order to understand the system and the issues and concerns that influence it, we conducted interviews with administrators, faculty, lab directors, the police, and relevant committee members. To ensure student participation in the process, we conducted a survey of the student body to assess the awareness level, security and privacy concerns, and opinions of the current system.

Having studied the current system and policies, other available technologies and systems, MIT student body opinions, and the facts presented by and the opinions of other players, our group has identified several areas for improvement. Our recommendation can be broadly broken into three categories: technology, policy, and oversight. In terms of technology, we found the encryption offered by the current RFID system to be inadequate, therefore the widespread use of RFID technology should be shelved until the security of the system can be confirmed. Policy-wise, we have found MIT's current method of storing data on all card swipes with no restrictions to be excessive. We also find that the policy is not clearly stated and the cardholders are not appropriately informed. We recommend that entry data be kept only for those labs and dormitories who request it. In general, entries to public spaces will not be tracked; however, tracking of these areas may be turned on at the discretion of a committee we describe. Finally, we believe that an oversight board is required to ensure that access to information resulting from card use is regulated by a clear and easily available policy and that this policy is consistently enforced. This will ensure the accountability of those who can access the logs and the privacy of users, at the level decided by the oversight board.

In analyzing the MIT ID Card system we endeavored to follow three guiding principles in building a system that is beneficial to all users.Ê The first of these principles is the protection of privacy for cardholders. To the greatest extent possible, we believe that MIT community members should be free to use their card without fear of being tracked.Ê The second guiding principle we have followed is to maintain campus security. Therefore, while privacy is important we have also tried to remain cognizant of the fact that entry logging can serve as an important tool to combat crime on campus. Third, we seek to ensure that the MIT Card is both convenient and able to provide expanded services to cardholders. We believe that the expanded functionality currently offered by the MIT Card is of real value to the MIT community and should be maintained wherever and whenever possible. In many ways, these three principles are contradictory, with greater security often meaning less privacy and reduced convenience; our goal here is to balance the three competing demands and achieve an acceptable and maintainable equilibrium between privacy, security, and convenience.

Methodology

This section describes in detail 2.1 the methodology of our research into the MIT ID Card and its associated privacy implications and 2.2 outlines what this report is meant to achieve.

Our Research

Our main goal in studying the MIT ID Card system was to talk to everyone and get as many first-hand accounts as possible: we gathered opinions from undergraduate and graduate students via a survey, and we interviewed administrators, former administrators, the Card Office, Enterprise Services, MIT Police, lab heads, members of old committees charged with a similar mandate as our own, current members of the Card Advisory Council, vendors of the current system, a few faculty members, and a few generally outspoken members of the community. In addition to our primary sources, we also consulted a number of secondary sources: *Tech* news articles, system specifications, IS documentation, internal websites. We used these articles as launching points from which we found a number of faculty members, administrators, and committee members with whom to speak.

Survey

In order to discover how the student body feels about the MIT ID Card and its associate policies, we conducted a survey over a period of one month beginning November 1. We advertised our survey on the undergraduate dorm mailing lists, which combined reach a very large fraction of undergraduate students and also many graduate students. We also advertised our survey to certain graduate dorm lists, and also one or two ILG lists, but it is safe to say that our survey as a whole represents more the opinion of undergraduates

living in dorms than any other particular group: of 513 respondents, 63 do not live in on-campus dorms, and 403 had not spent any time as graduate students (i.e., were undergraduates). The principal reason for this skew in representation is distributionary, and unfortunate: neither the Inter-Fraternity Council nor the Graduate Student Council replied to repeated requests to forward our survey to their members.

Our survey was online, available at `http://privacy.mit.edu`; it took on average 5-10 minutes to complete, and consisted of 9 ``main'' survey questions, 4 demographic questions, and a comments box. We offered respondents to leave their username to enter a drawing for a $20 gift certificate for one respondent, as an incentive for participation. We justified this incentive by realizing that we were more likely to hear from students who did not have a very strong opinion on the matter if we included an external incentive.

The default response for all questions was ``decline to respond'' (and an empty box for the one main question that involved text entry). All questions were optional, and 18 respondents declined to respond at least one main question. An additional 60 respondents declined to answer the one main question that involved text entry;[1] the other 8 main questions involved only selection from a menu.

We were interested to know whether students knew that the MIT ID Card contains an RFID chip in it, and whether they were comfortable with it. We were also interested to know how students felt about the current policy of keeping logs of entry data. Finally, we were also interested to know student opinions on some of the policies we were considering recommending.

Appendix A contains a full copy of our survey as it was presented, as well as a description of the distribution of responses for each question. The conclusions we drew from the results of our survey are spread throughout the rest of the report.

Interviews

To find the opinions of the various groups on campus who might potentially have an interest in the MIT ID Card, and in order to be able to take their thoughts into consideration in our report, we conducted numerous interviews with community leaders:

Current and Former Administrators

Dan Michaud
: Head of the MIT Card Office. Mr. Michaud was very helpful in describing the current system; he provided us with many contacts throughout campus who have interests in the MIT Card system. He is also concerned about successors to the Card Office and stresses on the importance of an audit process.

Larry Benedict
: Dean for Student Life. We discussed with Dean Benedict issues related to dorm access and the MIT Card. He was unaware of the tracking policy of the MIT Card system. He felt that MIT gave more autonomy to students than other institutions.

Arthur Smith

Former Dean for Undergraduate Education and Student Affairs; Former Chair of MIT Privacy Committee. Professor Smith was the first chairman of the Privacy Committee which was formed in the wake of the Vietnam War. It was an era of change with the Buckley amendment and co-ed dorms at MIT. This ad-hoc presidential committee compiled a report about the handling of information at MIT. Policy issues required approval by the Dean (who was also a faculty member). He believes that education and awareness is a very important component of a successful system dealing with privacy issues.

Harry Lewis

Former Dean of Harvard College. Professor Lewis was very helpful in providing an external viewpoint. At Harvard as Dean, Lewis was the gatekeeper for entry data to the undergraduate dormitories; his thoughts on the Harvard system were invaluable to our analysis of the MIT system.

John McDonald

Associate Director, Enterprise Services. Mr. McDonald gave us valuable input on decisions made about the MIT Card. He views the Card Office as a guardian of confidential information similar to the registrar, bursar and HR. He welcomes the involvement of student and faculty in the process but would like to have consistent involvement over time.Ê

Faculty

In addition to the faculty mentioned above, we spoke with:

Joseph Ferreira, Jr.

Professor of Urban Studies and Planning; Former Head of MIT Privacy Committee. Prof. Ferreira gave us extended input on the working of the former committee including the lack of adequate representation from all sectors and the reasons for dissolution. He also said that the MIT Card was an example of how progress could be hindered by privacy concerns. He thinks an audit trail should be traceable.

Hal Abelson

Class of 1922 Professor of Electrical Engineering and Computer Science; Member of CSAIL Prox Card Privacy Committee; Professor Abelson pointed us towards great resources and was also an invaluable guide in directing and helping us work on our paper.

Lab Directors

Anthony Garratt-Reed

Principal Research Scientist, Department of Materials Science and Engineering. Mr. Garratt-Reed stated that they had their own RFID system in place before since they needed localized access control. After the incorporation of RFID in the MIT Card and the capability for client access stations, they moved to the MIT system. He is fairly concerned about the duplication of cards to gain access into

the labs but he is not significantly concerned about the fraudulent use of other people's cards to gain access to the labs.

Lissa Natkin

Assistant Director, Computer Science & Artificial Intelligence Lab. Ms. Natkin helped us determine what labs need from the MIT ID Card system, and also mentioned the cost savings in using the card. She also mentioned that card tracking was not useful during the times when doors were open to everyone and thefts happened more frequently.

Gregory Tucker

Director of Facilities of the Media Lab. Mr. Tucker mentioned that the main use of alternate RFID card systems in the lab was for limited access to hazardous regions. They hope to upgrade to the MIT system in the future for convenience and ease of administration. Their legacy system stores data for 18 days and used only in the case of theft.

MIT Police

Jay Perault

Detective, MIT Campus Police. Detective Perault gave us input about the police's perspective on the Card system. He said that the tracking data had been useful in investigations and should be continued. He also spoke about the Cori Law in Massachusetts, which ensured that privacy concerns were considered while looking at government data and similar high standards they set for privacy issues.

Albert Pierce, Jr.

Lieutenant, MIT Campus Police. Lieutenant Pierce addressed many of our concerns about the MIT Card. He concurred that the tracking data had been useful in the past. He was not able to reveal details about the cases or the number of times of usage. He said the data used was very case-specific and all requests had to be approved by Chief DiFava.Ê

System Vendors

MagnaData

Representatives from the firm. The representatives gave useful information about possible future systems and what considerations need to be taken into account.

Indala

Sales representative at the firm.Ê The representative spoke about the FlexSecur system but would not go into details about the security. When faced with the question about the vulnerability shown by Winstein, Roach, & Mandel, he would not give a comment and stated that he had not heard about it.

Committee Members

In addition to those committee members listed above, we spoke with:

Manisha Manmohan

Member of the Card Advisory Council. As the newest member of an infrequently meeting committee, Manisha has only been to one meeting.

Hector Hernandez

Member of the Card Advisory Council. Hector was very helpful in giving a first-hand account of how the Card Advisory Council operates. He spoke about the representation, operation, and motivation of the council.

Amy Bruckman

Member of the former MIT Privacy Committee. Amy gave us an account of the different parties involved with the then Privacy Committee and the committee's pro-privacy orientation. She also felt that raising awareness was an important aspect of the problem.

Members of the MIT Community

Richard Stallman

Mr. Stallman is a very vocal critic of governmental tracking and sees MIT as an extension of the U.S. government. He also believes MIT, as an academic institution, should be a model of openness.

In addition to the people we spoke with, there are a number of community members we wanted to speak with but were unable to: Chief of Campus Police John DiFava; any members of the former Card Steering Committee; and any members of the former Card Privacy Committee. We were able to find almost no information beyond a single *Tech* article on the Card Privacy Committee. It is possible that this committee did not exist, and was merely proposed, or that it simply produced no discussion or recommendations.

What is this report?

Our report contains three foci: a description of the current system, including limitations and flaws; a description of the ideal system; and necessary changes to the current system that can be implemented at low cost. Our recommendations throughout are heavily influenced by the individuals we spoke with and take into consideration to the greatest extent possible the differing views of all parties with interest in the MIT ID Card system.

The Current System

We present a thorough history of the current MIT ID Card system, as well as a discussion of the technical flaws and the questionable practices and policies currently employed. The current system is imperfect in many ways; we identify these ways. We also consider input from as many campus groups as we have spoken with to discover their opinions of the current system and how it might be changed.

The Ideal System

We also present a recommendation for the ideal future system. Our system addresses as many of the technical flaws of the current system as we believe is possible with currently available technology. Our technical recommendations are heavily influenced by our policy decisions, which we believe will result in a system that is acceptable to as many members of the MIT community while still within the bounds of implementability and while being useful to those who require the information available by virtue of having a campus-wide access system.

Necessary Changes to the Current System

We are not blind to the fact that any new implementation will take a substantial amount of time, money, and effort. Many of the administrators we spoke with were not optimistic about the likelihood of an entirely new system being implemented from scratch, especially since many of our ``ideal system'' recommendations are not being offered by vendors as an off-the-shelf solution. To address this problem, we present a set of changes we believe is it imperative be applied to the current system to address our serious privacy concerns.

History

Historically, MIT had used a person's social security number (SSN) as their primary identifying number across MIT systems. In fact, the SSN would be the ID number that appeared on an MIT identification card. However, as more records were stored on computer systems and access to these systems become more widespread, concerns about privacy became more acute. The use of a person's SSN as the common institute identification number was quickly singled out as being both dangerous and unnecessary. In response to these concerns, the Institute began to restrict use of a person's SSN, declaring it part of a person's personal data and thus protected by the MIT policies on privacy and disclosure of information. In tandem, MIT's Data Administrator, Scott Thorne, issued the Tech Info document ``People Related Projects: 37707'' to MIT Information Systems on August 17th, 1994. The document outlined the creation of a new common MIT ID numbering scheme and the system to support the lookup and assignment of this ID.[23]

According to the initial 1994 document, the MIT ID required the following four attributes:

Unique
: Each MIT ID must be unique to only one individual.

Distinct
: Each person should only have one MIT ID number and that number should be used to across the institute to identify the person.

Random
: There should be no implied or derived meaning encoded within the MIT ID. No personal information should be identifiable simply by looking at the MIT ID.

Public

> The MIT ID should be considered public data that can be openly and freely used. Therefore, the MIT ID alone should not be considered sufficient to authenticate an individual.

In August 1995 development of the central computer system necessary to support the new MIT ID was completed and over the years this ID system has been adopted by the following campus groups:

- Athletics
- Project Athena
- Personnel
- Card Office

Concurrently with the developments of the MIT ID, the Institute was also endeavoring to create a more flexible and useful ID card. On September 29th, 1993, MIT started experimenting with consolidating the functionality of its meal card and ID card. The new ``student services card'' was to be the first phase in a process that, as then Director of Housing and Food Services Lawrence E. Maguire put it, would create a ``one-card system that [met] the fundamental needs of the Institute as a whole [for] identification, access, and purchasing.'' [5] The process initially went through some growing pains as a proper system was fleshed out that would allow ID card, meal plan access, door access, and other functionality to exist on one card. In fact, the 1993-1994 academic year almost seemed comical to MIT students as they were issued no fewer than three cards over the course of the year. A column in *The Tech* perhaps best summarizes the incredulity that some regarded MIT's attempts to create a new card. In columnist Mark P. Hurst's self-styled ``*Cards in Review''* he notes that:

> In September we all affixed our registration stickers to our Old Card, the ID card we've used since freshman year. Magnetic stripe, photo, and a spot for the athletic sticker.
>
> Things soon got better when we got the New Card (at this point, the ``Old New Card''). This winner had the notable improvements of not containing a photo, registration sticker, or athletic sticker. The Old New Card was much better than the Old Old card, since it could be used for unlocking some doors some of the time (for mine, none of the time) and for buying lots of overpriced food on its New Magnetic Stripe. It also had the value added service (for you ARA types, a ``Val-U-Service'') that students could use stolen Old New Cards without that hassle of photo identification.
>
> Jump to the present: the New New Card. It has a New New Magnetic Stripe, which can be used to open more doors more of the time, and a New Photo, which is really an Old Photo, having been taken from the Old Old Card, but no athletic sticker, which is still on the Old Old Card. So if you want to buy an overpriced lunch and then work it off in the gym, you have to carry the Old Old Card and the New New Card.

> ...You may be saying to yourself, ``The real reason we got three cards this year is because we're in a transition period to a new card." Could be, but can't we have foresight of more than a week to cut down on new versions of the same old magnetic stripe? Besides, next year won't be much different. Look at your New New Card. On the front is an expiration date - in September. That's right: get ready for the New New New Card next fall. The fun never ends! [15]

As Hurst astutely noted, the next installment in the evolving MIT Card was issued towards the end of September 1994. The new card endeavored to combine the various functionality of the many cards from the previous year. In this case, dormitory access, parking access, meal purchases, and library card services were all included in one card. A feature new to this card was the introduction of a declining balance account that allowed students to make cash purchases using their ID card. This card was used for the entire year and is the first in the line of cards now known at MIT as the MIT Card.

From early in the process it was noted that security and privacy issues would dominate the introduction of this new MIT Card, however for the first few years little was done to formally address these issues. On November 3rd, 1993, the Undergraduate Association (UA) appointed a task force to investigate privacy, security, and convenience concerns surrounding the introduction of the proposed MIT Card. Also as early as 1993, the different offices within MIT that were planning on making use of the new MIT Card began stating what policies they would be following regarding the usage data that would become available to them. Assistant Director of Housing and Food Services Kenneth R. Wisentaner told The Tech that despite having the capability to track student use of card readers to gain access to MIT buildings, there was no intention of actually using this feature. Chief of Police Anne P. Glavin reported that parking lot usage data would be recorded and stored for 2 years for parking and traffic enforcement and for long range planning. Finally, Wisentaner noted that meal transactions would be stored for about one academic year. [6]

In this mess of policy declarations and preliminary investigations by the UA, it is very striking that no overarching body was acting to coordinate and oversee the creation and implementation of privacy and usage polices for the new ID card. At the time, no committee existed whose mandate specifically covered the MIT Card and its associated policies; instead, all privacy issues fell under the purview of the Faculty Committee on Privacy. However, as if to exacerbate the existing problem with lack of oversight, the Committee on Privacy ceased to meet between May 1994 and November 1995 because there was no one to act as chair of the committee. What is more, as observed by Amy S. Bruckman - then Graduate Student Union (GSU) representative to the Committee on Privacy, the committee itself ``had no authority or resources, and its recommendations were often ignored or laxly enforced." [17] This lack of cohesion and oversight is apparent in an anecdote recounted by Bruckman. According to her, a few months after use of card swipe access to dormitories was activated, a student called the security guard of her dormitory to report that her card was not working and had never worked. The security guard, in response to this complaint, responded by saying that indeed the card

did work because it was used to gain access to some building X at a previous time. In the end, it turns out that, despite the assertion by the Office of Housing and Food Services that it would not be tracking students, they had forgotten to switch off the tracking feature on the system.

During the early phases of the introduction of the MIT Card, privacy took a back burner to the sheer number of complications that surrounded the implementation of the new ID system. It was not until 1995 - after the new MIT Card was better established - that serious attention was drawn to the security and privacy implications. In September of 1995 MIT issued yet a new ID card. The new MIT Card's biggest change was that it no longer displayed the student's SSN, instead using a randomly generated ID number created using the system proposed and implemented by MIT Data Services. This marked the convergence of the programs to develop a more private MIT identification scheme and a more functional ID card. Also of important note, this new ID card was, for the first time, issued to MIT employees, thus replacing an older ID issued by the Personnel Office.

Very shortly after the introducing the new ID card for the 1995-96 school year, Senior Vice-President William R. Dickinson announced the creation of the MIT Card Steering Committee. The committee had no standing agenda and was instead tasked with addressing any issues regarding the MIT Card as they arose. One of the first issues that came to the forefront of attention was the security of data contained on the MIT Card's magnetic strip. It was realized early on that, if someone could gain access to a person's ID card, the information stored on the card could be easily read by any card reader and used to steal the person's identity. On March 28th, 1995 André DeHon published a paper entitled ``Security Assessment of the M.I.T. Card.'' Through the course of this paper, DeHon proceeds to make an argument that that ``the level of security provided by the card is laughable.'' His analysis walks through several scenarios in which an ID card could become compromised and ultimately leads to several recommendations that essentially suggest that the MIT Card was not sufficiently secure to be trusted for use with financial transactions. [7]

On the heels of DeHon's paper and the controversy it caused, the Office of Housing and Food Services instructed that the MIT Card should no longer be used as collateral for items loaned to students. This referred to the common practice of requiring a student to give their card away whenever they took items, especially from dormitory desks, on loan. When the student returned the borrowed item, they were given back their ID. The main concern here was that while a student's card was held as collateral it could be read by a rogue reader and its information stolen.[4] In possession of information stolen from an ID card, a person could create a new card and make purchases or access restricted areas under this new identity. In response to questions about DeHon's report, Associate Director of Food Services John T. McNeil noted that, ``We [at the Office of Housing and Food Services] were certainly aware of the faults that [DeHon] points out. I don't really know of a system that would be foolproof.'' Carrying on, McNeil states that, ``we knew [when] putting [the new MIT Card system] together that the system is only as good as the people who use it. We were aware that copying was a possibility, but really it's a felony to do that.'' In many ways, McNeil's reaction summarized the sentiment at the time. Yes

there were legitimate concerns and yes the card system was not perfect; however a lot of time and money had been sunk into the system and, frankly, it would be impossible to develop a perfectly secure yet convenient and flexible solution for the MIT ID Card. Therefore, faced with this reality it seems that the overwhelming choice was to go forward with the system on hand and accept the increased risks as the cost of having a more functional card system. [8]

This is not to say that no effort was made to improve the security of the MIT Card. In fact, the Office of Housing and Food Services took some of DeHon's recommendations to heart and made some of the technology changes he suggested.[5] In fact it could be argued that it was DeHon's paper which prompted then Dean for Undergraduate Education and Student Affairs Arthur C. Smith to instruct that a committee be created to oversee the MIT Card. It is as a direct result from this request that the MIT Card Steering Committee was formed. However, as time progressed and the new MIT community became more familiarized and comfortable with new ID card, these questions of security and privacy again fell from the focus of people's attention.[6]

For the next couple years following 1995, few major changes were made to the MIT Card and controversy over the card fell to a minimum. At the onset of the 1996-97 academic year uses for the MIT Card included: identification, meal plan access, library book borrowing, access to dormitory entrances, entry to parking lots, and access to various buildings across campus. At this point time, Maguire characterized the services offered by the MIT Card to be in the ``upper middle'' segment in comparison to those offered by other schools; and while other ways to expand the MIT Card were being explored, nothing firm was in the pipeline. Also in 1996, MIT changed its policy on the expiration of ID cards. Prior to 1996, cards were valid for only one year and were replaced each September; however, in order to cut back on printing costs, card expiration was extended to a four year period.

The 1997-98 academic year occurred without major event for the MIT Card, but in the summer of 1998 a major reorganization of both the Office of Residence and Campus Activities and the Department of Housing and Food Services led to the creation of an independent MIT Card Office. The new MIT Card Office reported to the Dean of Students and Undergraduate Education and was to be headed by former director of Housing and Food Services Lawrence Maguire. From this point forward, the MIT Card Office became responsible for development and expansion of the MIT Card system, distribution of ID cards, and maintenance of MIT Card infrastructure and software.

During the summer of 1999, the MIT Card office began an upgrade of the MIT Card system. The upgrade occurred in two parts, the first occurring in the summer of 1999 when the card office installed Diebold Corporation's CS Gold application.[7] The next phase involved the installation of a Windows NT server and porting over to an Oracle database and would actually not be entirely complete until the 2001-2001 academic year. With an estimated price tag of $350,000, this purchase represents the largest change to the MIT Card system since the upgrades it under went from 1993 to 1995. [9][8]

In 2001, the MIT Card office moved again within the Institute to fall under the supervision of Director of Enterprise Services (headed by Steve Immerman) of the Office of the Executive Vice President. Along with this move, a three person team was commissioned to study the existing MIT Card Office and MIT Card. Led by Interim MIT Card Office Director Kirk Kolenbrander and with Greg Anderson and Matt Brody from MIT Information Systems, the team researched practices at MIT and at universities across the United States and concluded that the MIT Card Office was outdated and irrelevant to the MIT community. According to the MIT Card Office 2000-2001 report to the President, the team established the following principles to guide the policies and structure of the office:

- One card will serve as the only card that individuals need to carry for routine personal use, on or off the campus.
- That card will function as the primary platform for the identification, access, individual purchasing, and Institute services needs for all members of the MIT community (students, faculty, staff, and affiliates).
- The office that administers that single card will be a fully self-supporting business enterprise that obtains its revenue stream through card swipe transaction fees, reader connect fees, interest earned on debit card balances, and replacement card fees.
- That office will feature fully centralized control of the card platform, hardware, and software, but will allow highly decentralized control of the specific business applications to the array of business users.
- Card functionality will be built upon a principle of customer service. With a particular focus on the needs of our resident undergraduates, the card will offer superior, responsive service to individual card users and those services that leverage the card. Extended service hours will characterize the effort, with replacement card services at locations across the campus throughout the day and night.
- Through the proactive leadership of the office director, card services will inspire confidence among the users and will forge productive relationships among users and the service providers and vendors. Through the director, the office will implement a rich communications plan to insure service and accuracy of information.

The full set of recommendations made by the team was compiled into a report which was then adopted by the Dean for Student Life, Vice President for Information Systems, the Director of Facilities, and the Director of Enterprise Services. Final approval for the recommendations in the report was given by the Executive Vice President and the Chancellor. [10]

The period of 2002 to present the MIT Card Office has overseen two interrelated efforts in addition to the implementation of the recommendations from the report adopted the previous year. These were a push to ``effectively and efficiently absorb some of the smaller, independent card access systems on campus into its campus-wide system;" and to make the jump to proximity access technology for the MIT Card. [10] The effort to

absorb other card access systems came from both the belief that a single ID card controlling access to all campus facilities was preferable to multiple disparate systems and the successful completion of upgrades to the MIT Card system which gave it the capability to handle an expanded system. To realize this ambition, the Card Office went to the various groups on campus and pitched the idea of using the MIT Card for their access requirements. The concept was extremely well received and, according to the current Director of the MIT Card Office Dan Michaud, at present the 34 locations have MIT Card client stations installed with over 20 to be deployed before next spring.[9] As a result of the extremely strong response the MIT Card Office received to this new program, it was forced to reevaluate its policies for privacy and security. Acknowledging the wider impact that any decision made by the MIT Card Office would have on the MIT community, a special committee, dubbed the MIT Card Advisory Council, was convened in 2002 to help develop policies and procedure for the MIT Card. The council is still in existence and is comprised of representatives from the MIT undergraduate and graduate population as well as key players in the MIT faculty and staff.[10]

The other big initiative for the MIT Card Office was the rolling out of MIT Cards equipped with RFID chips. According to Michaud, the addition of RFID technology came largely at the behest of MIT labs who were interested in expanding into this technology. There are few firm justifications for using this technology except that it is a new and interesting toy. The most compelling reason for RFID technology is that it will save on maintenance costs because readers and cards are less likely to be worn down. The new cards are rolled out in the summer of 2003 and the newly minted STATA center is equipped with proximity card readers. The use of RFID technology drew quick outcry from members of the MIT community who questioned the security of such a system, one of the most outspoken of whom is Richard M. Stallman, founder of the GNU project and now resident in building 32.[11] Stallman questions both the security of RFID cards against rogue readers and the dangers to privacy that could arise from tracking RFID cards. Despite the concerns raised by community members, RFID chips are now included standard within all cards issued by the MIT Card Office.

Perhaps, the final important event that brings us to the present state of affairs is the summer 2002 decision by the MIT Card Office to activate the tracking feature of the MIT Card system and keep logs of all card access incidents for a period of two weeks. The decision to start tracking was done without notification to members of the MIT community. News of this change in policy was finally released to the MIT community in a January 29, 2003 article in The Tech. According to both Daniel Michaud and John McDonald, Associate Director of Enterprise Services, the decision to enable tracking was made in response to requests from a large number of labs and departments for such a feature if they were to use the MIT Card system for access control. According to McDonald, when Enterprise Services took a survey of groups across campus on why they had bought their own access systems the three most common replies they received were: audit logs, local control over doors and people with access, and the ability to use proximity readers. Therefore, the move to enable tracking was part of the larger program to attract these groups to use the MIT Card system. At its own discretion, the MIT Card Office implemented its own policy governing access to tracking logs. This policy stated

that all logged data would be kept for a period of two weeks and would only be accessible by written request from MIT Chief of Police John DiFava. To date, logs have been accessed in only a handful of instances in response to thefts and missing person cases.

Thus we arrive at the current state of the MIT Card, MIT Card Office, and all associated policies. The evolution of the technology, vision, and policies guiding the development of the MIT Card has been far from perfect. However, what we now find ourselves with is a system that provides many conveniences upon which we rely and, in fact, expect. Many questions have been raised over our ID, and perhaps only a handful of these questions have even been answered; however, many people to whom we have spoken view the development of the MIT Card as a tradeoff between the cost of action (lessened privacy, security, and identity theft) and the cost of inaction (decentralized and expensive access control across campus and few conveniences for cardholders). It is many of these unanswered questions that we endeavor to answer in this report and we hope to provide reason and guidance for the further evolution of our MIT Card.

Current Policy Practice & Our Policy Recommendations

This section discusses in detail the current policies and procedures concerning the MIT ID system, our recommendations for changes and improvements, and why these recommendations are optimal. These policies address issues such as the collection of tracking data, permissions to access tracking data, situations in which access to tracking data is appropriate, and an auditing process for all policies and procedures.

The current policy for the MIT ID Card is a result of multiple policy changes over the years, which were outlined in great detail above. The current system tracks all types of entries from all locations on campus, including in the classroom buildings on the main campus, dormitories, and laboratories. The current magnetic stripe system does not record failed attempts, which will be described in the Tracking section below, to enter a building. It should be noted in reference to this blanket tracking policy that according to Daniel Michaud, the head of the Card Office, the current technology system of the card can only support tracking all entries at all locations or recording no entries at all locations. All of the data is then stored in the system for viewing by the gatekeeper of the data two weeks after recording.

The data that is recorded is under the control of the head of the Card Office. There are three other employees of the office that are also able to access the information freely. According to the MIT ID Card policies that are posted online, the tracking information will only be used for trouble shooting and police investigations. [18]

The troubleshooting occurs at the Card Office by the employees. As far as police investigations, the chief of Campus Police, currently Chief John DiFava, must send a signed written request to the head of the Card Office to obtain any tracking information. No other outside group is allowed to request the data.

When an access to this data occurs, then there is a log that is updated to record who viewed what data at what time. The current system does include a log that could be used for auditing information. This computer also includes the log files of who has accessed the database. However, it is speculated that Mr. Michaud leaves his account logged into his computer during the day for other employees to use the database system. Aside from the speculation, the log is also useless for auditing the head of the office if he can easily delete any evidence of accesses that he has made of the data.

The tracking policy in terms of uses, locations, length of record storage, and who has access to the data is all available online at the card website. There is part of the policy that is not readily available to the public, which is the information regarding the Card Advisory Council. This body meets quarterly to review and advise on current and potential policies regarding the MIT ID Card. Current members of the council include Dan Michaud, Assistant Deans from several different offices, and representatives from the Faculty, Graduate Student Council, the Undergraduate Association, MIT Campus Police, MIT Enterprise Services, Athletics, Human Resources, Registrar's Office, Alumni Association, and MIT Libraries. Overall, the current policy has its strengths and weaknesses that will be discussed in depth below.

Policy Recommendations Summary

There are several major changes to policy that we recommend for the current and future MIT ID Card system. Our most urgent recommendation for the policy surrounding the card is that those recommendations that can be implemented with the current system technology should be implemented as soon as possible. These recommendations include the implementation of an auditing policy, and changes in who the gatekeepers are for the access log.

The policy changes we recommend are:

1. The creation of a stronger, more permanent Card Advisory and Oversight Board
2. Approval of accesses to dormitory tracking info is now done by that dorm's housemaster.
3. Tracking and privacy policies must be made public and well known.
4. Students are allowed access to their own tracking data, and are provided with a copy of any of their data which is accessed by other parties.
5. The entire process of accessing tracked data is audited by the MIT Audit Division.

Introduction

There are several model laws and paradigms in place at the state and government level which regulate access to certain records and help to maintain the privacy of the public. These include the Family Educational Rights and Privacy Act (FERPA), a federal statute, and the CORI Laws, state laws of the Commonwealth of Massachusetts.

FERPA, also known as the Buckley Amendment, allows for students above the age of 18 to access educational records kept by educational institutions. For post-secondary information, these rights to access are passed solely to the student if he or she is over 18 years of age. Students are entitled to view their educational records within 45 days of making such a request to the institution that keeps these records. Disclosures of information to third parties by the educational institution can be done only with student consent with some important exceptions. These exceptions include disclosure of information without student consent to ``court subpoenas, requesting information, federal audit requests, law enforcement requests regarding missing students, and requests from health departmentsÉappropriate parties in connection with a health or safety emergency if knowledge of the information is necessary to protect the health or safety of the student or other individuals." [20]

The FERPA laws apply to all public institutions and those private institutions which receive public, including MIT. Much of the financial aid that students receive at MIT is through federal funding, and many of the research programs on campus are also funded by the government. According to Professor Arthur C. Smith and Danny Weitzner, tracking data that MIT records is considered to be educational data, and is subject to the guidelines of FERPA. MIT and the tracking data it maintains are then subject to the rules of FERPA because MIT is a partially government funded private educational institution. In our policy recommendations, we will adhere to the guidelines that FERPA lays out for the usage and disclosure of educational information.

In addition to the disclosure rules outlined in FERPA, we have strived to adhere to the Fair Information Principles of the U.S. Department of Health, Education, and Welfare. These five principles that guide the legislation enacted by these departments were developed in response to the computerization of medical records and a desire to maintain the privacy of the public in light of new technology. These principles are:

1. Collection limitation.
    - Data should not be collected on systems that are very secret. Students must be aware of what systems are in place to record their educational information.
2. Disclosure.
    - There must be a way for an individual to find out what information about him is in a record and how it is used. The system should allow for the full disclosure of information to the student.
3. Secondary usage.
    - The individual must have a way to control the usage of his or her educational data beyond that of the collecting institution.
4. Record correction.

    - If the information located in the record is incorrect, a student or family member should have the right to have the correct changes made.
5. Security.
    1. Any organization or other entity that uses data obtained from the MIT Card Office must be able to protect that information as well.
    2. One of the pertinent protections that must be offered is the protection against misuse of the data. This includes the student's rights to privacy. [19] [21]

The CORI Laws are state laws intended to protect the privacy of those who have criminal records when those records are accessed by other parties. These are laws that MIT police must follow when attempting to access anyone's criminal record for investigative purposes, and surely serve as a reminder of the kinds of privacy protections that students are entitled to in light of the protections guaranteed to those with criminal records. The penalty for non-compliance with the CORI laws is a $10,000 fine, or 1 year in prison for offending officers, according to Detective Jay Perault and Lieutenant Albert Pierce of the MIT Campus Police. The laws set an important and high standard for police actions when accessing the personal records of any person including the tracking data of students.

Based on these principles and laws, it seems that much of the data that is recorded by the current system falls subject to FERPA and should be that policy formulations should adhere to the Fair Information Principles, as they are national standards for privacy protection. Tracking data is identifiable data in that card swipe data can be traced back to the user of a card given the right records of id numbers. Although the state and federal realms contain many laws concerning the protection of privacy, and accesses to state and federal records, such rigorous processes do not exist within the confines of MIT. The following policy and technology recommendations were created by taking the guiding principles and model laws from the state and federal domain into account. It is our goal that the following recommendations, if adopted, would prevent theft and other crimes while preserving a high level of privacy protection. An attempt has also been made to keep the policies as straightforward as possible so that they are accepted by the entire community as logical and necessary policies and not as cumbersome processes designed to make simple tasks relatively difficult.

Tracking

The initial planned role of the MIT ID Card was to provide a secure method of restricting access for a building to the correct individuals. When an individual wishes to enter a building, he must present reliable identification to prove that he should have access to that location. Access to a building varies on the desired population, as general campus areas are accessible to all MIT associated individuals, whereas individual departments often limit the access to their own members. Since the device that checks the user's card will have to check the individual's identification to see if they have the correct permissions, the system has a choice of saving the information from this transaction. Saving this data is tracking at the most basic level. The questions arise of what

information to save from a single transaction and at which locations this information should be stored.

When an ID card is scanned by a card reader, one of three things can happen: the reader identifies the card as valid and grants permission to the specific location, the reader identifies the card as valid but denies access to the particular door, or the reader fails to identify the card as authentic. These different scenarios occur depending on the card owner's access privileges and if the reader is functioning correctly. If the user does not have permission to enter and the reader is working correctly, the attempt is called a denied entry. The second type of entry, where the reader is not working properly, is a termed a failed attempt and does not depend on the status of the user. If the card owner has permission to enter the building, the reader is working correctly, and the user is allowed in, the access is a successful one. These three types of attempts to enter create three different categories of data that could be handled differently in recording.

Denied Entries

Denied entry data gives information of which people tried to unsuccessfully gain access to a certain location. If this happens, then the individual may be trying to enter where he actually should be allowed but the system for whatever reason is not granting access or where he thinks he should be allowed but does not in reality have permission. In the first case the individual will most probably want to have the problem looked at if it happens repeatedly. To properly analyze the problem, the data stored needs user identification. If the data contains a specific identifier that lets the authorities know who was trying to gain access and at what time, the authorities can look at this information and act accordingly. To meet these motivations, if the database administrator is not able to identify the denied entry as belonging to the user, the user is not able to show a problem. If denied entries are recorded into the database, the duration that they remain in the database should be long enough to provide ample amount of time to the user to visit the card administration for help. If the data is used to show problems in the system, then it is not disadvantageous to keep the data for anytime greater than a few days.

Another use of recording denied entries is to monitor individuals trying to gain access with ill-natured intentions. Depending upon how the specific tracking data is pinpointed in the database, the level of usefulness for crime investigation varies. If the Campus Police are investigating a crime and find numerous denied entries in the record close to the time of occurrence, the data could help the police find a potential suspect. On the other hand, if the Campus Police find the information ``accidentally'' while aimlessly looking through data, then this would be a breach of students' privacy rights. According to Pierce and Perault of the MIT Campus Police, the data with a user identifier attached should be stored for shorter periods of time to reduce the possibility of ``fishing'' for data. Additionally, shorter periods of time would lessen the ability of the database administrators to browse through data as a past time, since it would be there for less time. If the Campus Police look through denied entry data randomly, the user identifier will hurt the privacy rights and a lack of identifier would therefore be preferable. However, the privacy rights can only be upheld if there is an effective database access protocol,

which will be discussed in the Database Access Section. If there is proper security of the database and the administrators do not use it to ``fish'' for data, then the user identifier on denied data is not a problem. The two cases have one key component that differs: the reasons of why the data administrator found the data.

In general, if denied entry data is stored with a user identifier, then it should only be investigated when there is a specific reason, such as a complaint from a card user of a system failure or a crime investigation. Assuming that the data access is properly restricted, then denied entry data should be recorded at all locations.

Failed Attempts

Failed entries occur when a person tries to gain access to a building by using the card system, but the reader does not recognize the card as one in the system. In this case, the reader does not have any other data about the event, except the time and location that some card failed to be read. A failed entry attempt would indicate either a broken reader or an outsider trying to gain access.

If there is a broken reader, then the record of failed entries would be extremely useful in finding a problem. The system could keep track of the number of failed entries in a certain location over a certain time period. If the number of failures exceeds a certain limit, then a warning could be raised to the database administrator to warn of possible card reader failures. A further discussion of a possible alert system appears in the Data Access section later on.

The other possibility is an outsider attempting to break into a building on campus. However, a large number of failures at the same reader has higher chances of indicating, is a hardware system problem rather than an ill intentioned outsider. Regardless of the cause, the counter for number of failed entries would still be triggered in the case of an outsider and warn the database administrator of a possible problem.

Failed entry data should be kept for a long enough period to allow the database administrator to discover a problem. Hence, the data must be kept long enough such that on a normal basis, if a card reader was not working at a certain location, then enough failed attempts would accrue and warn the administrators of the database. Keeping this data for too long does not pose a privacy threat, since it does not have any personal information identifiers, but rather only a time stamp and location.

Successful Entries

When a successful entry occurs, then the information of who entered what building at what time can be easily recorded into the database. This information can be very useful especially for the purposes of a crime investigation or analysis of foot traffic through an area finding individuals that entered a building at a certain time.

While considering solutions for fulfilling the above requirements, a few principles need to be kept in mind Ð campus security needs and individuals' privacy rights. The policy created needs to provide the optimal amount of data for use in a crime investigation. At the same time, the recording of this data could infringe on the privacy rights of students, faculty, and administration. Individuals with access to this data could potentially use it for inappropriate reasons, such as monitoring the number of individuals of a certain demographic that enter a building at a certain time or to track the whereabouts of a certain person.

Due to the possible contradicting goals, each potential solution will need to be evaluated in terms of how well it fits each motivation and in turn how well this fits the needs of the campus. In particular, the policy of the successful entries in the tracking system focuses on location of tracking and lifetime of records.

Locations Tracked

The policy concerning which locations should be tracked can be in one of three: a uniform policy covering all entrances on campus, a blanket policy where nothing is recorded, or only specific places are tracked. On one hand, if tracking data is collected, it would obtain information that can be valuable for the Campus Police during investigations. On the other hand, if data is collected, there is the possibility of misuse of records, ``Big Brother'' theories, and overall privacy infringement concerns.

According to Lieutenant Albert Pierce and Detective Jay Perault of the MIT Campus Police, the data currently recorded by readers at building entrances is useful in their work, though how it is used varies by case. In general, they were not able to inform us of how the data is used or how frequently it is used due to the confidentiality of investigations. However, they did mention that the information is very useful in the cases of missing students, since the information helps to recreate where and when the individual has recently been. The data garnered from tracking could be useful to prove an alibi of an individual's location or to piece together information about a crime, such as witnesses or suspects. The representatives of the Campus Police did mention that the tracking records merely suggest possibilities, rather than using the data as stand alone evidence, that need to be verified in other ways. In relation to the privacy issue, a survey of the student population indicated that two thirds of the individuals were not opposed to tracking, if the data was kept for a reasonable time period, if they were aware of it beforehand. In conclusion, tracking could occur without excessively infringing on privacy rights, if the lifetime of the records and access to the records, which will be discussed later, are properly restricted.

While tracking is important to the MIT Campus Police for investigation purposes, it can possibly jeopardize individuals' privacy rights. The stored data could be looked at by authorized individuals, but for inappropriate reasons. Authorities could look through the data for entertainment or look specifically at people of a certain demographic. These possible misuses hurt the principal of student privacy rights that should be upheld. Therefore, tracking at any locations would be possibly harmful to privacy rights.

Furthermore, the tracking data is not always helpful for solving crimes. For example, currently, according to Lissa Natkin, the Assistant Director of CSAIL, most thefts from CSAIL occur during hours when the card is not needed for entrance. This fact indicates that there are problems in the security system of the building and not a result of a problem in the current card system. Therefore the tracking could not have helped solve these crimes. Though this may be a more specialized case, it shows that while the tracking records do offer the possibility of greater security and investigative power, tracking and investigative power do not always correlate.

Another possibility is to track only at specific locations, especially where more expensive crimes can occur and the privacy rights are not as problematic. Laboratory areas with expensive equipment would not have the same sort of privacy rights associated with them as more personal spaces such as dormitories. In this way, tracking could vary throughout the campus depending upon need.

According to Lieutenant Pierce and Detective Perault of the MIT Campus Police, theft is a big problem at MIT since the members of campus are very trusting of others and do not always lock up their possessions. Theft is a bigger problem in dorms, where students often leave their doors unlocked, and in labs, where there is very expensive equipment. To this end, tracking could be helpful in assisting in crime investigations and should be performed in dormitories and laboratories.

As Former Dean of Harvard College Harry Lewis suggested, this scheme presents a few problems. It would lose some of its potential use and be more complicated than a uniform policy. Professor Lewis pointed out that individuals on campus should be fully aware of the policy and would then be more likely to approve it if it is simple and the same for all locations. However, the proposed policy is simple enough such that individuals can easily remember it and if the policy did get more complicated, then some sort of picture icon could be placed next to each reader that tracks the card swipes.

Lifetime of Data Record

The data recorded by the system when a card is read can be kept for a variable amount of time Ð never, eternally, or a limited amount. The different lengths of time would provide different amount of utility to the police force as an investigative tool and still protect privacy rights. Not recording any data would be the same as tracking at no locations, which hurts the police from gathering possibly valuable information about future crimes but at the same time protects privacy rights. This issue was evaluated above in the same regard as not performing any tracking, which was decided to not be optimal for security reasons.

On the other hand, if the data is kept eternally in the database, then the police would be able to utilize the information maximally. If they needed information on who was at a certain location at a certain day and time, it would be useful to simply look at the records as a starting point. The Campus Police expressed the important role that the tracking data is able to hold in investigations. For police utilization, the data should be recorded and

kept. However, if the records are kept indefinitely, then the problem of inappropriate usage becomes more severe. If authorities have access to unlimited amounts of tracking data, then it is a privacy threat. Individuals may fear that the people holding these records could use it for ``Big Brother'' type of activities. While eternal recording of data could be more useful to police, it threatens to infringe on the privacy rights of individuals.

If the record was kept for a limited amount of time, then a balance could be reached such that all of the principles of security and privacy were optimally upheld. The longer time period allows for better utilization of the records on the part of the Campus Police. But the shorter time period helps protect the students' rights for privacy. Lieutenant Pierce and Detective Perault of the MIT Campus Police explained in an interview that the current limit of two weeks was set such that it prevented authorities from ``fishing for data'' or monitoring an individual's records without specific reason. Student opinions from the survey showed that most individuals were comfortable with the current policy of holding the data for 2 weeks. It also showed that these one third felt unfavorably towards tracking was because of the amount of time that the data would be stored and these individuals were in favor of keeping the data between two and seven days. However, this short of a time period would probably drastically decrease the value of the records to the Campus Police. Therefore, the recommendation is to keep the data for a two week period.

Public Awareness of Policy

The policies regarding tracking can only be fully utilized if these policies are known to the entire campus. The student survey showed that 73% of students were not aware of the current tracking policy and this lack of knowledge was one reason that they did not like the policy. This should not be the case, because everybody involved has the right to know what the policies are and how they work.

There are a few ways of implementing the policy such that all of the members of campus will be aware of the policy and be able to find it when necessary. The members of campus should be aware of the policy from the time that they arrive. One way is to give out a flier in the welcome packet when a new student, faculty, or administrator joins the campus. This will help make all individuals aware of the policy. However, a person may lose it during their years at MIT. For this reason, the policy needs to be available by some other route, like the web. The web would make the information easily accessible to campus members at any point in time. Public awareness of the policy is important to help protect privacy rights of people on campus.

Access to the Tracking Database

Another important feature of the tracking database is the process by which tracked door entry data is accessed. The entire system is vulnerable, if the two key procedures to keep tracking data secure are not met. The data access protocol decides who can access what data and by what procedure. A secure access protocol needs to be strict enough such that

it enforces the policies regarding tracking location and the lifetime of the record, while still allowing for efficient and convenient use for investigative purposes. If a tightly secure access system is not created and implemented, then the privacy rights of individuals are vulnerable and there should be no tracking of entries at all.

An efficient access protocol should be created, while still trying to uphold the keystone principles, particularly, protection of student privacy rights and efficiency of investigative security tools. Access paths should be created only when there is a specific reason. If the tracking data is accessed by unauthorized individuals, then there could be numerous security issues and the privacy of the students would be compromised. Deciding which individuals should have access to which types of information and how they access it depends upon their role on campus.

Anonymous Data

Tracking data information is useful for numerous reasons, including police criminal investigation, system checks by the card office, solving individual student card issues, and general traffic data. Some of these motivations, specifically some system checks and traffic information, do not require that the analyst be aware of the card holder's identity. It would be useful, however, to know the type of entry, the location, and the time. To reiterate, if unneeded identity information is given to the individual that views the data, then it will greatly increase the chance that the data use will infringe upon the card user's privacy rights. Therefore, for those parties for whom anonymous data is adequate, it should be easily accessible.

Facilities

The tracking of ID cards can be useful for facilities to learn about the traffic patterns in certain buildings. This data can be useful for a department to figure out cleaning schedules, estimated amounts of traffic, and other such information from data regarding the number of people that accessed a building by using a card reader. This information, however only requires knowing how many people used the reader and at what time. It does not require any other sort of demographics, such as sex, race, or class. Any extra information that is given, but is not pertinent to performing the project at hand, could perhaps lead to misuse of data. For this reason, it would be better if this anonymous data that was completely stripped of all identification data was available to facilities.

On the other hand, this data could potentially be used for supervisory purposes. For example, suppose a worker is supposed to be at his job at some exact time and other people very rarely enter this building around that time. If the anonymous tracking data is available to the facilities head of a lab and subsequently the boss of the worker, the boss might be able to tell exactly when the employee arrives to the work location. The card tracking system should not be used for these purposes. Very precise information regarding the number of individuals that entered at a certain location at a certain time is unnecessary to the purpose of analyzing traffic data.

Yet, this anonymous tracking information could be helpful to the facilities department in their work. Calculations could be made from this data such that it has lower resolution. For example, one way to lessen the precision of the tracking information is for facilities to specify a twelve hour period of the day. The data for this twelve hour period is averaged for the last two weeks and then rounded up or down to the nearest integer person per twelve hour period. This type of formula would make it harder for a third party to make stipulations regarding the whereabouts of specific individuals, which protects the privacy rights of the card users, but at the same time, it helps illustrate the traffic patterns in a certain location.

Card Office

The main function of the Card Office is maintenance of the card system, which includes proper functioning of all of the readers and successful access to the correct locations for individual card holders. The employees of the office need information to pinpoint broken readers. For example, if a reader is not functioning properly in a certain building, the problem will not be found until the office is alerted by an individual that tries unsuccessfully to gain access at this location and calls the office to let them know of the failure. Then one of the Card Office employees that have access to this data can find the information. Since viewing the information is currently not restricted, the employees could look at other recorded data while looking for something specific. This presents another possible situation of infringement of privacy rights.

The worker at the Card Office should be able to use his own computer to check how many failures have occurred or if there have been any successful entries in the past few hours. The workers of the Card Office are supposed to make sure that the system is running properly. This does not necessitate the worker knowing the identification of the card users unless it is in regards to a specific individual card holder. In this case, the student, faculty, or administrator would be present at the Card Office and could give permissions to the employee to view his or her account at the time of trouble shooting. More information on student access rights is in the later Student Access section of Personal Data. The Card Office employees can fulfill this role with regular access to anonymous tracking data.

Furthermore, there are certain card trouble-shooting situations where other solutions could also provide quicker solutions. When a reader to an entry is broken, then attempting to use a valid card may result in a failed entry. If the reader remains broken, then more individuals will attempt to use the reader to gain access and more failed attempts will occur. The database is already recording these failed attempts, so the information should be used. An automatic counter is recommended that alerts the maintenance team when a broken reader is suspected. The automatic nature is important in that if the system is able to check these possibilities internally, then there is no human contact or possibility of privacy rights infringement. This counter could base its alert system on the proportion of failed entries versus successful ones or the number of failed entries that have occurred over a set period of time. Setting these tolerances at reasonable values will quicken the process of pinpointing and fixing broken readers, while not

encouraging Card Office employees to casually search through campus members' personal tracking data.

Personal Data

All data that contains a user identifier in the tracking record is limited to successful and denied entries. The user identifier is the major reason that tracking poses such a huge threat to personal privacy rights. While the personal identifier does pose a threat, it is also essential part that allows the tracking data to meet the motivations. This personal data helps to pinpoint any problems regarding an individual campus member's card, investigate crimes, and allow for easy missing person checks.

While considering these possibilities, only one gatekeeper of certain information should be picked. A second gatekeeper would add a layer of security to the system, but it will also make the system more inefficient. The second gatekeeper would need to be an individual on campus that has student's interests in mind, such as faculty members or deans. Deans, for example, work on a daily basis on confidential student matters. However, the police may need data quickly for a time sensitive issue and making it mandatory that one of these individuals be present for any data access would slow down the process greatly. A quicker and more efficient option is to rely partially on an efficient auditing system, designs of which will be further discussed in the Auditing section below. If there is only one gatekeeper and a good auditing system, the security still remains intact and efficiency high.

Student Access

Students may need to demonstrate to the Card Office that they are experiencing a particular problem with the functioning of their card. Currently, when there is a problem of this sort, then one of the three employees with access will look up the information and act accordingly. With the current recommended architecture all Card Office employees except for the head have the permissions to only access the anonymous data. With this setup, students should have access to their own information. If the students hold the privileges to their own account, their privacy is protected the best. On the other hand, if desk workers at the Card Office have access to this information, it would be easy to track a student and follow the student's routes. Furthermore, if the student realizes that they can access their own data and the desk worker cannot, the students will trust the system more to uphold their privacy rights. The easiest authentication method for students would be to require entry of their Kerberos username and password. The Kerberos password is already secure enough to do other transactions that require privacy and it is already in place. The student being able to access their own information is important to protect privacy and maintain any principals that were put into place from all of the other sides of policy.

One reason that we have to provide information to students is that it counts as educational data. This kind of information must be provided to students under the Family Education Rights and Privacy Act (FERPA). There are a few ways to provide this information in an

easily accessible, but in a secure and efficient way. One possibility is to offer it on Websis, where private academic and financial information is stored for students to view. The Websis system is fairly safe and reliable, as the campus trusts it to store their other personal information. It is also easily accessible from anywhere, as long as the user has a personal certificate. However, setting up the system on Websis requires a data system that will update the system regularly and for the entire database to be on the web. Limiting the data to one computer in the Card Office will make it more secure and less easily obtainable by an outside third party. While having this information on Websis would be a novelty, it is not really necessary. Most students will need this information more often for solving problems associated with the card, for which they would need to visit the Card Office anyways. If students are interested in viewing their records, they should be able to visit the Card Office. Having student records accessible to the individual at the Card Office would ensure security of the information and meet the requirements of FERPA.

One of the additional provisions for student privacy protection is that students will be provided with a copy of their data if their data is specifically requested for any reason. This policy has been adopted by Harvard University, and we feel that students should be entitled to know when their personal records have been requested. Such a procedure follows in the spirit of disclosure, one of the Fair Use Principals, and the disclosure guidelines of FERPA.

Campus Police

The Campus Police find tracking data valuable in investigations, as was noted earlier. If they do not have access to the data, then the security importance of the tracking is not fulfilled. Therefore, the Campus Police should definitely have access to tracking data in some way or form. The Campus Police currently gain access to the data by requesting it from the head of the Card Office and putting it into the case file for storage. This system restricts the power that the police would have if they have full access to the database. According to Lieutenant Pierce and Detective Perault of the MIT Campus Police, the current system is flexible to the time constraints of an investigation, as they are usually able to get the data within a day and even sooner if needed. Furthermore, they noted that if the Campus Police need the information and the two week storage period is almost ending, then the Card Office can save it for the police until the paper work is completed.

On the other hand, more police power could be useful in cases where there is extreme time sensitivity. The information as an investigative tool is one of the key motivations of tracking. Police are supposed to uphold citizen's rights, as according to Pierce and Perault, they face a $10,000 fine and a year of jail time if they violate any of the privacy laws. The police are aware of the consequences of invading an individual's privacy and already deal with this on an everyday basis. Speeding up crime investigation is a strong reason to make the police as the gatekeeper of the data and there is also already infrastructure in place to hold them responsible for upholding privacy rights. However, the police's domain should be limited when it comes to dormitories, which should be part of the housemaster's, as discussed below.

Housemasters

Police have the permissions to view student and faculty tracking information. However, privacy rights need to be protected more in the dormitories and for this reason there needs to be an extra precaution to protect the dormitory tracking data. Larry Benedict, Dean of Student Life, suggested that the housemaster of a dorm should have access to his or her dorm's tracking information. The housemaster of a dorm is supposed to be one of the key individuals involved in a student's life, especially when there are any problems. Current MIT policy specifies that housemasters ``should be knowledgeable about the resources that exist at MIT for responding to crises and should be quick to call upon them when needed." [24]

Numerous duties of the housemaster require that the housemaster maintain the student's privacy rights and act in the student's interest, including representing the student in front of the Dean's office. For these reasons, the housemaster is a good choice as the gatekeeper for their own dormitory records. The housemaster should need to agree to any police accesses of tracking entry data from that housemaster's dormitory.

Housemasters deal with numerous crises that they need to investigate themselves. According to Julian Wheatley, the housemaster of East Campus, most housemasters prefer keeping these type of investigations internal so that they can still hold control, rather than making the information external. For the motivation of internal house investigations, Wheatley was in favor of housemasters being the gatekeeper for dormitory information, especially in the case of a possible missing person case. Under this recommendation, housemasters can at any time access data regarding their own dormitory at the Card Office, where the data is stored.

Since the data will be centralized in a certain location and not be placed online, the housemaster will need to visit the office to view data. There should be a secure authentication process for login, for which the Kerberos system can be used. The housemasters have two roles for taking care of student data: they can view the data to investigate internal house matters and they need to act as the gatekeeper for the data anytime someone else wants access to it, especially the Campus Police.

Miscellaneous

Any other individual on or off campus should not usually need access to the tracking data. Again, if access to the data is too easy, then the privacy rights of the students and faculty are at risk. However, if any other party does need information, such as outside government agencies, then they could be directed through the Campus Police. One possibility is through the Campus Police, which would make sense due to the hierarchical nature of the jurisdictions. The current policy for outside government agencies is that they need a subpoena for any information, according to Pierce and Perault of the MIT Campus Police. However, these individuals also mentioned that requests from other groups are usually rejected unless it's a criminal investigation. If any one on campus has a reason that they want to access the data, they can go through one of two channels: the

Campus Police or the Housemasters. Which group an individual approaches should depend upon the type of concern.

Location of Database

It will be easiest to have one central database that holds both the anonymous and personal data. The location of the database is important such that it is central for all of the groups that we are giving access to and such that it does not burden the holder. In terms of frequency of usage, the Card Office employees will use it regularly to troubleshoot the system, whereas the Campus Police will use it rarely for investigations. However, in terms of urgency, the Campus Police will need access as quickly as possible for investigation. On the plus side, placing the database in the Card Office would add another barrier that would deter the Campus Police from making random accesses of data or leaving the computer logged in during the entire day to allow other people to use it. No individual at the Card Office has the permissions to view the private tracking data, so Card Office employees browsing aimlessly through data would not be problem. Overall, the best location for the database in accordance with the rest of this policy is in the Card Office. One issue that could arise with the Card Office hosting the database is that it is only open during normal business hours. Yet, there are situations that would require the data as quick as possible, even on the weekends. If the reason is an extreme emergency, the police could potentially gain access to the Card Office, even when it is closed. This would enable necessary accesses to the database to occur, even though the Card Office is not always open.

Card Policy Making and Reviewing Bodies

One of the recommendations of this report is to expand and strengthen the mandate of the current Card Advisory Council, and to rename the council the Card Advisory and Oversight Counsel. In formulating this recommendation, we considered information gathered from interviews with current members of the Card Advisory Council, and members of past versions of the same committee, and combined our findings with our own concerns, and those of other users of the MIT ID Card.

The Card Advisory Council

One of the main functions of the Card Advisory Council is to formulate policy recommendations for the card, devise new uses for the card, and in general to think about the implications of card use for the entire MIT community. Members of the card council represent the different sub communities within MIT and include those who are directly involved with the function of the card as well. Current members include representatives from the Faculty, Graduate Student Council, the Undergraduate Association, MIT Campus Police, John McDonald Ð from MIT Enterprise Services, Assistant Deans from several different offices, representatives from Athletics, Human Resources, Registrar's Office, Alumni Association, and MIT Libraries and Dan Michaud Ð Manager of the MIT Card Office and current chairperson of the Card Advisory Council.

One of the main problems with the current committee is that although there are ostensibly members from all parts of the MIT community on the council, not everyone is always present at the meetings. Most importantly, undergraduate attendance at these meetings is relatively low, as it is across many institute committees with undergraduate representatives. Low attendance by undergraduate representatives is problematic because undergraduates make up a large portion of the MIT community and should have proportional representation on the committee. If undergraduate representation at the policy reviews meetings is low, then the policy recommendations and reviews will probably not accurately the undergraduate interests as well. As demonstrated by our survey of the student body, there is widespread ignorance of the card and its policies. For such a large portion of the community to be completely ignorant of these policies is intuitively disturbing.

The Council's main function at present is only to review changes and additions to the MIT Card policies; it does not currently have any power to make decisions. Herein lies another flaw with the construction of the current council. These policy discussions and reviews are nothing if they don't have the power to actually enforce any of those recommendations. One way to understand why the lack of decision making power of the council is problematic is to imagine the function and purpose of congress without lawmaking powers: Congress would exist to discuss and review the policies and laws of the administration, but would not have any power to change those policies. The actual laws would be completely controlled by the administration, and there would be no way to ensure that the laws took into account the interests of all the people the law would apply to. This is the case with the current council: It meets to discuss policies of the card, and how those policies might affect the MIT community, but they have no power to enforce any of those policies, or to make sure that the policies in place really look out for the interests of the groups they represent.

When the tracking function of the MIT ID Card system was turned on in 2002, recommendations of previous card advisory committees were disregarded. Previous incarnations of the Card Advisory Council had decided that maintaining records of successful card accesses was undesirable. It is unclear how much effort was made to make sure the tracking policy was acceptable to the entire community. From information gathered from John McDonald, Associate Director of Enterprise Services, it seems that the change was made to accommodate labs and offices on campus that wanted local access control, access to audit logs, and RFID technology. The accommodation was made to help bring more labs and offices under the card office umbrella to improve convenience for the labs.

It was assumed that this change in tracking policy was generally desired by the entire MIT community when in fact a large portion of the community Ð the student population Ð had no knowledge of the feature until an article in The Tech described the launch of the tracking policy some 6 months afterwards. This change in system operation flew in the face of previous policy decisions to not keep record of card access. A policy review of the change in tracking was never conducted at this time. This seems to have been a major breakdown in the way that these processes were ostensibly supposed to work. Such

a decision which affects all users on campus should have been approved by the representative committeeÑthe care advisory council.

Despite the inabilities of the council to effectively steer policy, the Card Council does have some very important merits. According to Hector Hernandez, a recent addition to the Card Advisory Council, the committee is composed of all the right players. Discussions between members of the council are genuine roundtable discussions in which no person's opinion is more important than another member's, and the discussions that occur at meetings are fruitful ones in which many important issues are discussed.

Many of the members are highly cognizant of the implications that the card's functions have for privacy; some members of the council, such as Hector Hernandez, are on the council because of a strong interest in the larger privacy and security concerns surrounding the card.

Card Advisory and Oversight Board

We recommend the creation of a new, more powerful council that will serve as a policy creation and oversight board, named the Card Advisory and Oversight Board (CAOB) which will replace the current Card Advisory Council. They will help to create the policies to be employed by the MIT ID Card system, and also to be responsible for enforcing the policies of the system in much the same fashion as other Institute committees act. As new technologies are developed and new methods of providing ID services are introduced, the policies of how card information is handled will need to be changed. It is important to have a policy-making board with the MIT community's interests in mind in place to handle these changes as they arise. This board must also find new uses and efficiencies for the card in order to use its strengths to provide better service to card users. Policies approved by this council, which will have the same representative makeup as the current Card Advisory Council, will be enforced after approval by the administration.

The CAOB will be in charge of dealing with all other problems that may arise as a result of keeping tracking information. One such situation that is likely to arise is when 3rd parties subpoena the tracking information, perhaps in relation to a criminal investigation. Third parties may want to serve the subpoena to anyone with access to the data. For example, the state police might serve the manager of the card office with a subpoena for tracking information. At this point, the card manager has two options according to Hal Abelson, a professor at MIT who has previously received a subpoena for information: He can consult directly with MIT general counsel to determine whether or not he must comply with the subpoena and provide the information, or he can pass the subpoena on to some other authority to consult general counsel. Our recommendation in this situation is to pass the subpoena up to the card advisory council to handle compliance issues with the subpoena. The CAOB will be in charge of consulting MIT general counsel about whether or not they must comply with the subpoena. If general counsel advises the CAOB to comply with the subpoena, then the CAOB will provide the requested data to the party serving the subpoena.

It seems that it is important to at least make the committee carry more weight, and to use this weight to get its proposed policies approved and implemented. One requirement for this is to make the committee more permanent and less easily dissolved. In the past, Committees on Privacy seemed to be formed whenever privacy concerning the card was a salient issue in the community. By making the Card Advisory and Oversight Council a stronger Institute committee, we can ensure the continuity of the committee. Over the past several years, card committees, and privacy committees, other various committees have been formed and dissolved. In the process of forming and dissolving committees, much of the accumulated knowledge seems to have been lost and is difficult to find unless one speaks with former members of those committees, who may not remember all of the discussions and findings in the desired detail. When interest in the topic died, or the current issues were resolved, the privacy committees disbanded, or discontinued. Our recommendation entails making the Committee a more permanent institute committee so that issues of security, privacy, and the MIT ID Card can be dealt with proactively and counter problems before they become widespread.

In the event that dissolution of the CAOB can not be prevented, a process for dissolution should be followed. This process should ensure that the findings and the policies of the committee are kept intact and archived for future use, when the Council might be reincarnated.

Auditing

This section describes the auditing mechanism we feel is necessary to protect against abuse of data collected by the MIT ID Card system.

Audit Mechanism

One of the most important parts of a policy recommendation is the creation of a mechanism for enforcement of the policy. Although the people currently responsible for administering the system and granting access to data are reputable people, there is no way to guarantee that future office holders will be as trustworthy. There must be a system in place to monitor accesses and other transactions to ensure proper use, and to also hold accountable those who misuse the system. Without the threat of enforcement, the act of accessing data logs without authorization would seem like less of an offense. Most people would think that the greater the penalty associated with a particular action, the more unacceptable and wrong that action is considered to be.

Possible misuses of the tracking data include discriminatory, supervisory, and random tracking. Discriminatory tracking would entail the distillation of entry/exit data of different groups on campus. Supervisory tracking is the tracking of employees by their superiors to aid in enforcing employment rules and regulations. Random tracking is more of a voyeuristic activity that people might engage in just to see whose card is being used where. Random tracking might also include stalking. Additionally, it is important not to

give just one party complete access to the data as this party could abuse its power, even with accountability mechanisms in place. Auditing procedures will prevent parties from illegally accessing data and/or altering data without proper consent. Auditing also ensures that data is only being used in accordance with the principles under which access data was being collected in the first place.

In reality, though the current policy requires that all requests for card tracking data be approved by the chief of police, many accesses to the data occur without ever coming to the attention of the MIT Campus police chief. Additionally, there is no written audit policy, nor evidence of a mechanism used to audit the practices of the MIT Card Office, and other MIT ID Card activities. It is these unauthorized accesses which we intend to curtail, and nebulous policies that we hope to define more precisely.

Needs for Auditing System

We recommend a system that creates a log file of all accesses to entry and exit data at the central Card Office database, as well as a corresponding procedure to review these logs and hold accountable those who deviate from the official policy. The entire auditing process will contain a series of checks and balances that will not burden those who carry the responsibility, but will still provide a high level of privacy protection for members of the MIT community.

The technical design of the log of data accesses will be discussed in later sections. Rather than logging accesses to data manually, the new system will log them automatically to further streamline the audit process. Currently, there is no real system in existence for auditing all accesses to the tracking databases. Although the current policy stipulates that the Chief of MIT Campus Police must sign off on all requests to use student data, there have been many instances of accesses to the database that have occurred without the proper authorization. Additionally, there seems to be no real record of when such accesses have occurred; the closest semblance to a database access log is a manually maintained log of such accesses.

While protecting the privacy of individuals by including an audit process in data access procedure, we would still like to preserve the speed at which data can be accessed when necessary. The purpose of the tracked data is to aid in maintaining security on campus, and the auditing process should not impede this goal as much as it should aid in ensuring that this goal is effectively and efficiently achieved.

Information Stored for Auditing

The information stored in the proposed access logs needs not be extremely detailed. The three main pieces of information that need to be recorded for each access are the identity of the user who is accessing the database, when the access occurred, and a description of what information was accessed. As discussed later in the technical system description, this can be accomplished by recording username, timestamp, and database query commands used.

First, record of the username will allow for auditors to know exactly who was responsible for accessing certain data, and who to hold accountable in case of any deviations from policy. Auditors will also need the timestamp and knowledge of what data was accessed in order to determination whether or not a violation of policy occurred.

Auditing and Those With Access

According to Professor Joseph Ferreira, users of the logged data should be aware of the existence of an audit trail. If a person accesses the tracking data at any point, he should have notification or other knowledge that his operations within the database are recorded for auditing purposes. Knowledge of the existence of such a process would be enough of a deterrence to prevent many from misusing the data, simply from fear of repercussion. If a party is to access data, that party should also be aware of what sorts of permissions it has to access the data, and why it has those permissions. These disclosures can oftentimes be a deterrent to those who might have unknowingly attempted to access the ID card database. Currently, someone can access the tracked data without knowing exactly what his or her level of access permission is. Professor Ferreira also believes that it is necessary for users of the card database to be aware of the different levels of permission, the different rationales regarding the levels, and what level they possess. This awareness will create a sense among users of certain responsibilities they have when accessing such data, and will also act as an enforcement mechanism for policies that are intended to optimize privacy and security.

Along the same vein of responsibility among users, those who are auditing the system should have a vested interest in providing a quality auditing procedure to ensure that auditing is carried out properly. If the auditing process breaks down, then so does the integrity of the privacy protection built into the system.

One key question which arises in formulating an auditing policy is the designation of an auditing authority. We recognize that auditing the card access procedure with an outside auditing source could be costly, and that costs are one of the main limiting factors to the MIT ID Card system overall. However, the risks to privacy that misuse of tracking information poses are so great as to justify the additional costs of auditing the entire procedure. One of the main requirements of our policy, supported by undergraduates and other members of the community is that tracking information should only be kept if there is an auditing or procedure in place to ensure that the data collected is not misused. Guaranteeing that the data is not misused also means that all accesses to the data follow the procedures outline in our policy recommendations. Without such checks and balances in place, it would be impossible to prevent misuse of the tracking information from going undetected.

There are several options for which on or off campus entity should have the authority to responsibly audit card data access logs. This entity should be a trustworthy, on campus body with a vested interest in the card, and with a concern from privacy of card users.

According to Professor Arthur C. Smith, one of the first members of the MIT community to head a privacy committee at MIT, it is better to keep faculty in charge of many of the functions of card oversight. The primary reason to do so is that they are by far the most permanent members of the MIT community. Students, the MIT police force, and other offices on campus have very large rates of turnover, relative to the turnover in faculty. Because of low turnover among faculty, putting a faculty member in charge of auditing creates a position of influence for a faculty member who has an interest in maintaining rights on campus, and who will maintain that position for many years; another method of preserving institutional memory.

Auditors

Auditing of the card access logs is one of the most important procedures in the card system as it adds a net of accountability to force all those involved with the card to comply with procedure. We have two options for entities who will actually conduct the audit. The first option is some combination of faculty, staff, and students, and the second option is to give the auditing work to the MIT Audit Office.

The first office that comes to mind as a potential auditor is the card office itself. One of the primary reasons for instituting and auditing policy is to ensure that the card office follows the policies and procedures to which it is subject. It is not feasible to allow this office to audit itself, as it would be inclined to find as little fault with its actions as possible. Also, audits should be conducted by an outside source that will not be biased in its findings.

Another option for auditing is to give this responsibility to enterprise services, the office which oversees the card office. Because this is the office which oversees the function of the card office, it would be one of the more logical choices for an auditing authority. Additionally, because enterprise services is the office in charge of dealings with outside vendors, they would also be able to use their access powers to perform system checks, and to make sure that the system was performing as promised by the vendor.

Campus police, which is responsible for approving accesses to student information, would most certainly be responsible in performing audit checks. In conducting criminal investigations, the MIT police are required to follow strict rules and regulations when accessing personal records, as regulated by the CORI laws. However, like the Card Office, the Campus Police would then be auditing many of their own actions.

The more practical yet costly solution to auditing is to hire a third-party auditing agency to review the access logs to make sure that policies and procedures are being followed by parties involved in card data access operations. One such third-party is the MIT Audit Division. MIT's Audit Division is an in-house office that can be used as an auditing resource for the tracking data access process. MIT Audit is an internal auditing office that performs audits and reviews for labs, departments, and centers across the Institute. The assessments performed by this office include reviews of compliance with Institute, financial, operational and information technology policies and procedures. Additionally,

MIT Audit will provide follow up assessments of offices they have audited to make sure that any necessary changes that were needed to be made were made and that the changes were effective in remedying the problems they were intended to solve.

Existing Access Technologies

In this section, we give an overview of some of the major technology options available for ID card systems. One method of classification of the different technologies is according to whether the card is a contact card or a contactless card. Contact cards primarily in use are magnetic strip cards and contact smartcards. Among contactless cards, the two most popular options are contactless smartcards and proximity cards. In the discussion below, the different types of cards are described in detail according to the technology that they use: Magnetic strip, RFID, or smartcard.

Magnetic strip

A magnetic strip is a plastic-like film containing tiny iron-based magnetic particles on the back of many transaction and access cards. The strips are written by magnetizing the particles in the required orientation. There are three tracks (each 0.11 inches wide) on the strip. According to the ISO/IEC 7811 standard, the tracks contain information as described in table 5.1.

Table 1: The tracks of a magnetic strip

Track	Bits per inch (bpi)	Number of Characters
1	210	79 six-bit plus parity bit (read-only)
2	75	40 four-bit plus parity bit
3	210	107 four-bit plus parity bit

Usually only tracks 1 and 2 are used. On track 1, either of two formats may be used. Format A is proprietary use by the card issuer. Format B is a standard representation as shown in table 5.1. Table 5.1 also shows the standard format that is used for Track 2.

Table 2: The contents of tracks 1 (if format B is used) and 2 on a magnetic strip

Content	Chars on Track 1:B	Chars on Track 2
Start sentinel	1	1
Format code=``B''	1	-
Primary ID number	less than 20	less than 20
Separator	1	1
Country code	3	3
Name	2-26	-
Separator	1	-
Expiration date or separator	4 or 1	4 or 1
Discretionary data	remaining (to add up to 79)	remaining (to add up to 40)
End sentinel	1	-
Longitudinal Redundancy Check (LRC)	1	1

Magnetic strip technology is mainly used for transaction processing and access control. The strips come in two main varieties: High Coercivity (HiCo) and Low Coercivity (LowCo).[12] HiCo provides highest protection against damage by magnetic fields, but it is harder to encode due to the higher power required to encode it. Most cards that are used for access control are HiCo, so as to provide greater protection against accidental modification and to survive repeated use.

Radio Frequency Identification

Radio frequency identification (RFID) [11] technology comprises two main components: the tag and the reader. The tag acts as the identifier in the system; it contains a microchip with a coiled antenna, and can transmit the information held in its microchip's memory by sending radio waves to a reader, which also contains an antenna. The information is interpreted by the reader and relayed to a main computer system. These tags can vary in size, shape and form depending on the needs of the application, but the antenna has to be of the specific size required by the transmitting and receiving frequency.

The mechanism for communication for a typical RFID system works as follows:

1. RFID reader transmits a radio wave.
2. A tag in the vicinity of the reader is powered or activated by the radio wave.
3. The tag selectively reflects energy back to the reader containing some identification data.
4. The reader, now acting as a receiver, receives and processes the identification data.

The most common way of categorizing RFID tags is based on the power source, classifying them into three main categories: passive, semi-passive and active.

1. A passive tag is activated by the reader: the reader sends out radiowaves that energize the tag. Passive tags are the mostly widely used form of RFID due to their lower cost, but the lower tag cost comes at the expense of computational performance.
2. A semi-passive tag has a battery built in to the tag for better performance leading to an increase in operating range. The battery powers the internal circuitry but is not used for radio wave generation.
3. An active tag broadcasts its signals to the reader using its own power in the form of a battery in the tag. Battery power is used for the entire operation and hence active tags can work and transmit even without the presence of a reader. Active tags are usually much bigger than passive tags due to the presence of an internal power source.

The transmission range of a tag depends on the frequency and power used; different antennae are used depending on the required communication frequency. Tags can be broadly categorized into three operating frequency bands: low-frequency tags (20kHz - 500kHz), high-frequency tags (13.56MHz) and ultra-high-frequency tags (850MHz - 900MHz). The read ranges vary according to frequency. The low-frequency tags can be read from up to about a foot away. High-frequency tags can be read from up to about three feet away. UHF tags can be read from 10 to 20 feet away. The low-end tags have very basic functionality emitting a static 64-to-256-bit identifier, while the higher-end tags may have the capability to perform active encryption.

Security in RFID systems

One of the biggest problems with RFID technology is the lack of security in the system. RFID tags have very little computation power: they have a few thousand logic gates and no cryptographic functions are available for the passive tags. However, there have been a number of proposals for providing security. RSA Laboratories has provided two approaches: the minimalist cryptography approach [13] and the blocker tag approach [14] described further in this section. Other schemes that have been proposed include the Kill Command feature described by the AutoID center, the Hash Lock Scheme and Randomized Hash Lock Scheme by MIT, and the Anonymous ID Scheme by NTT DoCoMo, Inc.

Minimalist Cryptography: This approach uses a method of ``pseudonym rotation." The basic idea behind this mechanism is that each tag has a list of cryptographically unlinkable pseudonyms computed externally by a trusted verifier. This would require limited storage - around 10 pseudonyms; the tag cycles through these pseudonyms. The pseudonyms are coupled with a throttling mechanism that strengthens the restriction on adversarial queries. On the reader end, a valid reader provides new pseudonyms. These pseudonyms are protected against eavesdropping and tampering using encryption

(readers have enough power to do this even though the tags do not). The pseudonyms are encrypted by the interleaving of one-time pads.

Each of the pseudonyms stored on a tag consist of a list of triplet-values. With the current restrictions on the size of RFID chips, this list would have about 10 entries. Each triplet contains three values a, b, c. a is sent to the reader by the card on query, and b is the value that the reader responds with; c is the final authentication value sent by the tag. In this protocol, the reader has the capability of updating the triplet values on a tag. The update is made using one-time pads that have been transmitted across multiple authentication protocols (to prevent malicious reader attacks).

This method is based on the fact that RFID adversaries are different from the usual adversaries in other systems. An adversary with full system access can easily break the system. But in the real world, the adversary must have physical proximity to the tag and, in this case, a valid reader. An adversary could use an invalid reader but the throttling mechanism would prevent them from getting all of the pseudonyms. Also, they would need access to the reader to gain the reader component of the pseudonym. The threat model for RFID tags supports the hardness of this method; it is not a foolproof cryptographic solution, but can be argued to be enough for most security purposes.

Blocker Tag Approach: A blocker tag simulates all (billions of) possible tag serial numbers. A `tree-walking' protocol for identifying the tags asks the tag what the next bit is; a blocker tag always says both 0 and 1. This makes it seem like all possible tags are present and stalls the reader. Blocker tags move can be selective and move tags to privacy zones, blocking certain ranges of RFID serial numbers. This type of tag is useful for protecting consumer privacy when RFIDs are placed on many items. After purchase, the tags can be transferred to privacy zones. The approach is not very useful for ID card systems that require repeated use and no change of zoning (or moving into privacy zones) is required, nor is it useful for authentication, however, it is useful for keeping the data on an identifying card secret when the card is not being used.

Smartcards

A smartcard is a card that has an embedded computer chip which is either a microprocessor with internal memory in it or a memory chip alone. Due to the presence of the embedded microprocessor, smartcards have the ability to store large amounts of data and carry out many functions including encryption and acting as digital signatures. The card connects to a reader in one of 2 ways:

1. Direct physical contact: Contact smartcards
2. Through an electromagnetic interface: Contactless smartcards

The above classification method is based on the means of communication. Another way of categorizing smartcards is by the hardware on the card:

1. Integrated Circuit (IC) Microprocessor Cards: These are cards that have a microprocessor on them. The microprocessor allows for the addition, deletion, and manipulation of information in memory, and for a variety of applications and dynamic read/write capabilities. The programmable nature of the processor makes it useful for many operations including cryptographic functions.
2. IC Memory Cards: These cards come with a memory that can store data, but cannot perform the additional processes that require a processor. Memory-only chips are functionally similar to a small floppy disk. They are less expensive than microprocessor cards, but they also offer less security due to the lack of processing capabilities.
3. Optical Memory Cards: These cards have optical storage and can only store data, but they have a larger memory capacity than IC memory cards.

The international standard for smartcards is ISO[13] 7816. Among their many uses, smartcards are very useful for physical access as ID cards to open doors, gates or other controls. Many physical security systems today use a protocol called ``Wiegand'' to communicate with door locks and other security devices.

Contact smartcards

Figure 1: Contact smartcard

Contact cards[14] require insertion into a smartcard reader or card acceptor device (CAD) with a direct connection to a conductive micro-module on the surface of the card. When the contact smartcards are inserted into the reader, the pins attached to the reader make contact with pads on the surface of the card and can read from and store information on the chip via this interface. The ISO 7816 series of standards provides the standard for this type of card. One of the disadvantages of contact cards is that they have been shown to suffer some degree of wear, limiting the life of the card. They are used in a wide variety of applications, including network security, vending, meal plans, loyalty cards, electronic cash, government IDs, campus IDs, e-commerce, and health cards. They have very strong security capabilities.

Contactless smartcards

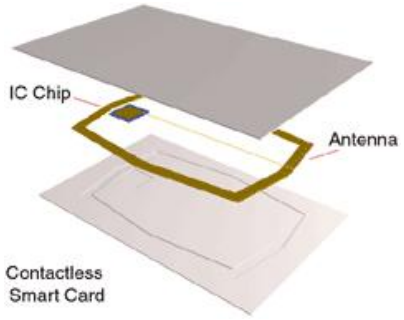

Figure 2: Contactless smartcard

Contactless smartcards or non-contact smartcards have chips that communicate with the card acceptor device through wireless self-powered induction technology (106-424kbits/sec). The card acceptor device is also called a reader. Standards for the contactless protocol are specified by ISO/IEC[15] 14443 (type A and B) from the year 2001. There are proposals outstanding for ISO 14443 type C, D, E and F that have not yet been accepted by the ISO standards committee. An alternative standard for the contactless smartcard is ISO 15693. These standards are focused on microprocessor-based cards. These cards have at least 1 kilobyte of memory.[16] The cards need to come within close proximity of the reader. Typically the range of operation varies from 2.5 to 3.9 inches (63.5 to 99.06 mm) depending on the reader.[17] In order to communicate, the cards contain an embedded antenna that can be used for reading and writing information.

The advantages of contactless smartcards include expanded flexibility, more memory, higher security (than most other options), faster transactions, lower maintenance, and published standards. They provide both convenience and security. All the secure cryptographic capabilities that were previously available in contact cards are now available in contactless smartcards. Examples of widely used contactless smartcards are Hong Kong's Octopus card, Malaysia's Touch 'n Go smartcard (1997), Paris' Calypso card[18] (October 2001), and London's Oyster card[19] (January 2004). Other areas of growing use include student identification, electronic passports, vending, parking and tolls.

Other smartcard options

Smartcards also come in different varieties depending on the combination of required capabilities. Hybrid cards and combination cards are two such varieties. Hybrid cards contain two or more embedded chips - for example, a contactless smart chip with antenna and a contact smart chip with contact pads, and/or a prox chip with an antenna. The contactless component would be used for applications with fast transaction times and the contact chip could be used for higher security requirements. The combination cards (also called ``combi'' cards or dual-interface cards) has one smart chip embedded in the card that can be accessed through either contact pads or an embedded antenna. This type of

smartcard is growing in popularity because it provides ease-of-use and high security in a single-card product. Mass transit is one of the growing areas for the combination card. Here, the contact chip could be used to add cash to the card and the contactless interface can be used to deduct a fare from the card. An example is Malaysia's multi application smartcard identification called MyKad that uses both contact Proton and contactless Mifare (ISO 14443A) chips.

Security of Smartcards & Cryptographic Techniques

This section gives an overview of the making of a smartcard leading to a discussion of the security. Each chip has an operating system which usually contains a manufacturer identification number (ID), type of component, serial number, profile information, etc. The system area may also contain different security keys, such as a manufacturer key or a fabrication key (FK), and a personalization key (PK). All of this information needs to be maintained secret.

One of the main benefits of smartcards is the ability for most cards to support on-board cryptography. Since the actual cryptography is done on the card, the keys do not have to leave their storage place. smartcards have the capability to perform both symmetric and asymmetric public/private key cryptography. They provide support for the following: Symmetric cryptography is when two parties share a secret key that no one else knows. This key is used to both encrypt and decrypt messages (hence ``symmetric''). If the key is compromised, then the cryptographic method breaks. Asymmetric cryptography works using a pair of a public and private keys. The public key is freely available and can be used by anyone to encrypt a message that the owner of that public key later decrypts with their private key, which is safely stored on the smartcard. Symmetric cryptography is much faster than asymmetric due to the lesser amount of computation time required. Common symmetric key algorithms are DES (Data Encryption Standard), 3-DES, and AES and the most common asymmetric cryptographic technique is public key RSA (Rivest-Shamir-Adleman's algorithm). DES, 3-DES and RSA use 56, 168, and 1024 bit long keys, respectively. Often a combination of symmetric and asymmetric cryptography is used. A usual method of doing this is as follows: if you want to send a message to user A, encrypt a new key K (usually small and fixed-width) using A's public key. Then use K to encrypt the message. A then finds K by decrypting it using her own private key (takes time) and then uses K to decrypt the message (taking less time). The self-containment of smartcards makes them resistant to attack as they do not need to depend upon potentially vulnerable and exploitable external resources. Hence, they are useful for strong security protection and authentication. In order to examine the security of smartcards, we will consider the following four areas:[20]

1. Communication
2. Hardware
3. Operating System (OS)
4. Software

Communication with the outside world: A smartcard and reader communicate via small data packets called APDUs (Application Protocol Data Units). The sophisticated protocol, low bit rate (9600 bits per second), bi-directional transmission line, and the fact that the data only travels in one direction at a time makes it harder to attack the system. A mutual active authentication protocol is used for authentication. The card generates a random number and sends it to the reader, which encrypts the number with a shared encryption key before returning it to the card. The card then compares the returned result with its own encryption. The pair may then perform the operation in reverse. Once communication is established, each message between the pair is verified through a message authentication code. This is a number that is calculated based on the data itself, an encryption key, and a random number. If data has been altered (for any reason, including transmission errors) message must be retransmitted. Alternatively, if the chip has sufficient memory and processing power, the data can be verified through a digital signature. Some of the algorithms used on these cards have been found to be breakable. [12]

Hardware Security: All data and passwords on a card are stored in the EEPROM (electrically erasable programmable read only memory) and can be erased or modified by an unusual voltage supply. Therefore some security processors implemented sensors for environmental changes. However, since it is difficult to find the right level of sensitivity and there is a voltage fluctuation when the power is supplied to the card, this method is not widely used. Other successful attacks methods include heating the processor to a high temperature or focusing UV light on the EEPROM, thus removing the security lock. Invasive physical attacks are the most destructive when the card is cut and processor removed. Then the layout of the chip can be reverse engineered. Differential Power Analysis (DPA), is a statistical attack on a cryptographic algorithm which compares a calculated guess with a measured outcome and can often extract an encryption key from a smartcard. Simple Power Analysis (SPA), which is the direct analysis of the recorded power data to determine actions and data, can also break some smartcards. Several solutions to these problems have been implemented. Technologies that have been developed for protection include the following: [12]

- Technology barrier: Advanced 0.6 micron technology greatly reduces the size and power consumption of cards as well as the relative variations in their operating parameters. It becomes very hard for external SPA/DPA methods to distinguish between normal card fluctuations and data-related fluctuations.
- Clock fluctuation: This is a special Clock Software Management facility, which when properly used, results in highly variable software timing when the embedded application program is executing to prevent voltage attacks.
- Unpredictable behavior. A built-in timer with interrupt capability and an unpredictable number generator is used to impose unpredictable variations on software execution behavior, with consequent changes in the pattern of power consumption.
- Robust design: Ensuring that the design is modular, allows for a robust design. Modularity makes it easier to do hardware variations, including customized variations, thereby allowing fast response to new attack scenarios.

- Memory control for multi-applications: An enhanced memory access control system provides secure operating system support for multi-application cards.
- Security mechanisms and firmware functions: An enhanced set of security mechanisms and firmware functions allow the application to detect and respond appropriately to the occurrence of conditions that might indicate an attack. These conditions include invalid operating conditions, bad opcodes, bad addresses and violations of chip integrity; the possible responses include interrupts, program reset, immediate erasure of all RAM data and flash programming of the entire EEPROM array.[21]

OS Security: Data on smartcards is organized in a tree hierarchy. There is one master file (MF) which behaves as the root directory. The root contains elementary files (EF) and dedicated files (DF). EFs are files and DFs are sub-directories (which can also contain more EFs), similar to any common operating system. The main difference is that DFs can also contain data. DF's, EF's, and MF's headers contains security attributes resembling user permissions associated with a file/directory. Any application can traverse the file tree, but it can only move to a node if it has the appropriate rights.

Attributes (Access Rights): There are five basic levels of access rights to a file (both DF and EF). Some OS provide further levels. Basic levels can be categorized, increasingly in security, as follows:

Always (ALW)
: Access of the file can be performed without any restriction.

Card holder verification 1 (CHV1)
: Access can only be possible when a valid CHV1 value is presented.

Card holder verification 2 (CHV2)
: Access can only be possible when a valid CHV2 value is presented.

Administrative (ADM)
: Allocation of these levels and the respective requirements for their fulfilment are the responsibility of the appropriate administrative authority.

Never (NEV)
: Access of the file is forbidden.

CHV1 and CHV2 correspond to the two security PINs stored in the card:

CHV1
: is a common user identification PIN.

CHV2
: is a specific unblocking PIN pre-stored in the card.

The PINs are stored in separate elementary files. When a wrong PIN is entered several times, the OS blocks the card. The number of times is fixed and depends on the OS. Once blocked, the card can only be unblocked with a specific unblocking PIN stored in the card. The unblocking PIN can become blocked in the same way. If this happens, card is said to be in irreversible blockage and may have to be scrapped for security reasons. If the PIN is

blocked, the attribute of every file is changed to require CHV1. After the unblocking PIN is presented, the file attributes are returned to normal, the counter for the PIN is set back to its maximal value and the counter for the unblocking PIN is decremented. If the latter counter reaches zero, it cannot be used for unblocking the PIN any more. This provides additional security for the card. This PIN structure is used for advanced authentication.

Software Security: Software security is also important. Properly encrypted data and transfers are required which are done using hardware-based or OS-based instructions and libraries supporting advanced cryptographic algorithms.

Most attacks today are classified as class 3 attacks, which means that either the costs associated to break the system are far more than the cost of the system itself, or that the cracker has to spend several or hundred years of computing power to break into a single transaction. Technology is developing faster than cracker methods. Therefore, each new generation of technology usually prevents attacks that the previous generation was vulnerable to.

The Current MIT Card Technical System

As can be seen from the discussion of ID card technologies in sectionrefextech, an ID card system is generally made up of three components:

- The actual card containing identifying data.
- Readers that read the information on the card and interface with the back-end.
- Back-end databases for storing and correlating the data.

The MIT ID Card system has all these three components.

The MIT ID Card

The current MIT ID Card consists of a double-layered strip of PVC with a magnetic strip and an RFID chip. This card will also be referred to as a ``proximity card'' or ``prox card'' later in this paper. The front face of the card has the MIT logo and owner's name, MIT ID number, photograph, and an expiration date. The back face of the card has a magnetic strip, a serial number, the status of the owner (explained below), the MIT logo and contact information for the MIT Card Office, and a disclaimer. There are three types of card based on the status of the owner: student, affiliate (including spouse or partner), and alumni. Temporary cards can be issued for residence access, parking access, summer conferences, retirees, athletic center access, and other non-picture cards. Specialty cards can also be issued such as those for the Emergency Response Group, for Campus Police, and for Facilities. Currently, there are over 27,000 card records in the MIT system. [22] The integration of the card into the existing MIT infrastructure was done by MAC Systems of Avon, Massachusetts.

Card Specifications

Indala Corp. of San Jose, California is the vendor who provided the card technology to MIT. It is part of their range of solutions for card systems. The type of card used for the MIT ID Card is the FlexISO Proximity Card.[22] According to the Indala website, the FlexISO card is a credit card-thin identification card that is ISO 7813 compliant. ISO 7813 is a standard for identification cards that are used as financial transaction cards. The card has a graphics-quality surface on both sides of the card and can contain multiple ID technologies including a magnetic strip, Wiegand code strip, bar code, a multitude of smart chips, and MIFARE. Currently, all MIT ID Cards has a magnetic strip and an RFID chip but some of the newer cards have a bar code also. Information is printed on the card using a dye-sublimation printer. Figures 3 and 4[23] show the ISO standard specification for ID cards.

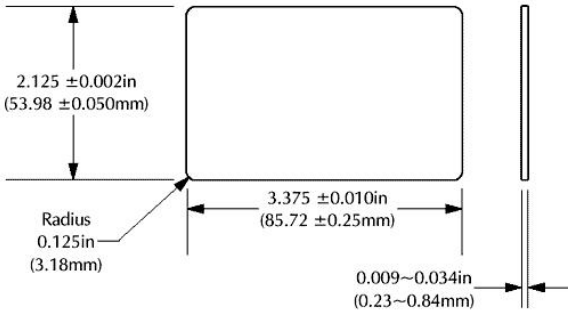

Figure 3: Plastic card size and dimensions

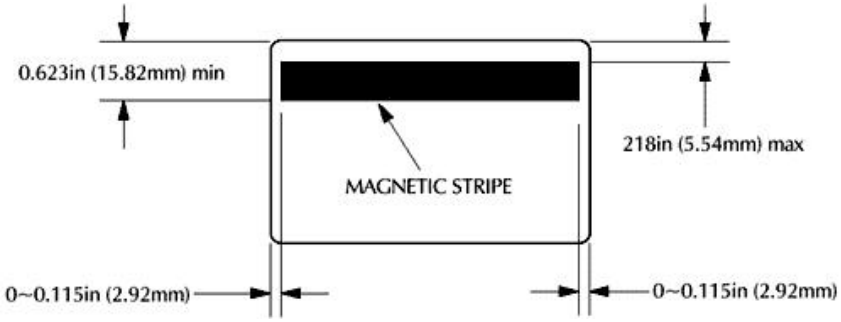

Figure 4: Magnetic strip positioning

The Indala card in particular complies with these specifications. The card has the ability to include either a contact smart chip, a prox chip or a contactless smart chip. The MIT Card, in particular, contains the 125 kHz proximity antenna and chip, and a 3-track high-coercivity magnetic strip. The magnetic strip follows the standard described in section 5.1. Figure 5 shows a typical card from Indala, but this was slightly modified for the MIT ID Card when it was seen that excessive use of the magnetic strip led to the wear of the tag that lay directly beneath it. [22]

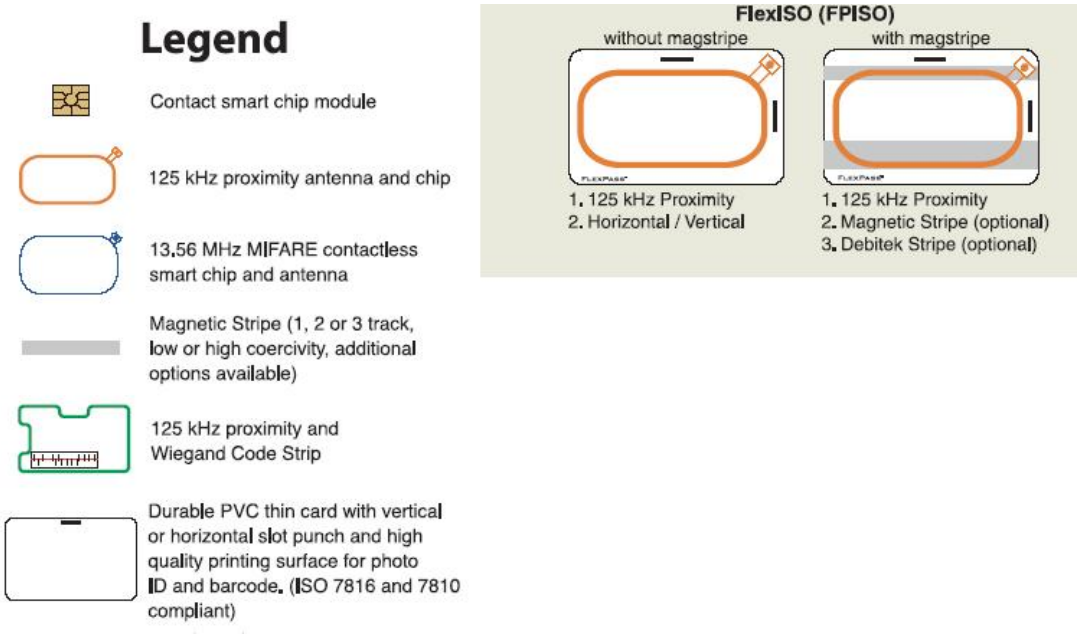

Figure 5: Type of card from Indala

The read range of the card depends on the reader. According to the company specifications, with a mid-range reader (like most of the readers on campus), the read range is up to 12 inches (30.5cm). Informal measurements by members of our group have shown that campus readers can read cards from approximately 5-6 inches away. in experiments conducted by Mandel, Roach and Winstein, the cards could be read remotely at a distance of several feet.

Each card has an identifier that is a randomly generated 6-character string that is different from the owner's MIT ID number. This is the ID number stored on the magnetic strip. A new number is generated for every card, both new cards and replacement cards. This same number is used for the RFID chip on the prox card. The chip is passive and thus has no power source. The card is powered by a 125 KHz sine wave. [25] It responds with an AM broadcast of bits that can be received with a modified AM radio or with an oscilloscope. The broadcast contains 224 bits that are repeated. There are 30 zeros, 22 constant bits and 172 user bits. Out of the 172 user bits, 32 bits seemed to vary from card to card while the others remained constant between cards.

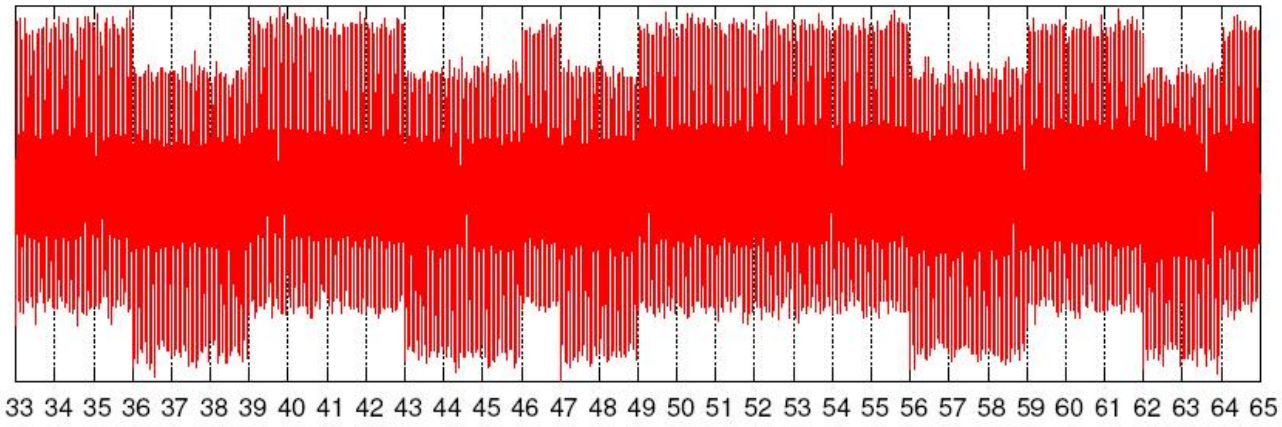

Figure 6: Example broadcast recorded from an MIT Card. [25]

Card Security

The security of the card is based on the Indala FlexSecur [26] system. This proprietary technology performs a type of verification at the reader level before sending data to the host system. In essence, the reader screens out unauthorized cards before sending out its programming data. This verification enhances security in the following 3 ways:

1. The data on the card is scrambled prior to the programming of the card. Hence the data stored on the card cannot be decoded to find the actual information on the card.
2. The information stored on the card is locked and only the reader has the key necessary to unlock the data. The programming data is translated by matching the reader key with the lock. This is the mechanism that prevents non-MIT Card data from being transmitted to the host system.
3. The reader can be programmed for each site, thus making each site unique for the reader as well as the card.

Since Indala's is a proprietary technology, we were not able to obtain any other information directly from them. [27]

Process for Lost, Stolen or Revoked Cards

When a card owner loses his or her card or has his or her card stolen, he or she reports it to the Card Office and the card will be deactivated immediately, though the deactivation make take some time to propagate to all the campus readers. In order to obtain a replacement card, the owner must go in person to the Card Office with another form of identification. A card is revoked if a card holder so requests.

Reader System and Access Control

Currently, the MIT campus has a combination of magnetic strip readers and proximity readers. There are about 700 card readers on campus. [22] The proximity readers are being incrementally installed around campus. The magnetic strip readers are still used for points of sale. Each reader is connected to a panel that is in turn connected to the centralized MIT Card system database.

Reading Mechanism

When a prox card is presented to a prox card reader, some data is received by the reader. The data is verified to be an MIT ID Card by the Indala FlexSecur system, as described in section 6.1.2. This data is then sent to the panel that is connected to that reader. The panel contains all the ID numbers that have access to enter through that door. After verification of the ID number, access is granted to the owner.

Specifications

As mentioned before, the currently installed readers were provided by Indala. The type of reader[24] is the Mid-Range Arch Reader, using an excitation frequency of 125kHz. The approximate read time is 200 ms from read to data output. The reader has a read range of up to 12 inches, according to the specifications. In actuality, most cards cannot be read beyond a distance of 7 inches, using this combination of card and reader technology.

The panels were provided by SonicWALL, a provider of integrated network security and identity solutions based in Sunnyvale, California.[25] They are part of the network described in the data management section. The panels can be connected to the MIT Card Office system allowing the card office to control access or they may be controlled by the department whose control that panel falls under. On request, the Card Office will help set up a client station that gives the department control over access. The department also needs to provide a PC, a network jack, and a lock-box. CS Gold 4.1 by Diebold, Inc. is responsible for the access control at the client stations; the software offers controlled access, electronic payments, and identification. Currently, there are 34 client stations spread across the MIT campus. There are plans to deploy over 20 more stations before Spring 2005. [22]

Data Management and Network

The management of the card data is done through a centralized system. A new card computer system was set up by Diebold Inc., a provider of integrated delivery and security systems based in North Canton, Ohio, in the summer of 1999. The system included a central server in building E32 operated by the MIT Card Office. For the new prox card system, MIT uses technology from SonicWALL. The card system has a virtual private network (VPN) that is used to transmit secure information from the main electronic card systems to the individual client stations around campus. The network has two firewall and VPN concentrators (SonicWALL PRO 330s). These are used to manage

the main access point of the card system. All the data is stored in the central server in building W91 with a backup server in Building E32. In addition to this, 80 appliances were deployed at key client stations and point-of-sale locations in January 2004; 50 more were installed through this year. These appliances are part of the VPN and they transmit access approvals to the central server using a secure, encrypted tunnel on the VPN. The software for the back-end system was provided by SoftwareHouse. The front end is custom-built for preparing MIT IDs which hands off the data to the CCURE backend. [28] CCURE is the system provided by SoftwareHouse that is used for making the IDs, entering new user data, configuring the servers, and monitoring the data on the servers.

The data from the panels are all sent to the centralized server and access logs are made. The access data are stored for a period of two weeks. The two kinds of data stored are

Card read
: ID number, access, and timestamp for when an access is attempted

Door state change
: State, and timestamp when a door is locked or unlocked

Both normal and denied entry data are stored. In the case of a successful entry, all the available data are stored. In the case of a denied entry, if it was an MIT ID that did not have authorization that information is stored. If it was not an MIT ID, then the ID number is not stored. An Oracle database is used on the server.

After the data are stored on the server, they can be accessed by a request that must signed by the police. The CCURE system has an audit log so that every time someone runs a report of card usage, the system stores the user as well as the parameters of the report. These requests are maintained on file. [23] Only Dan Michaud of the Card Office has access to the log of changes to the entry log. [22]

Limitations of the Technical System

The MIT ID Card is not secure by any stretch of the imagination; both the magnetic strip and the RFID tag portions of the current card are vulnerable to identity theft. A 1995 *Tech* article on a report submitted by André DeHon to then-director of Housing and Food Services (which is now separated into two different departments) Lawrence E. Maguire and several other administrators quotes DeHon as writing ``the level of security provided by the card is laughable." [8]

Magnetic Strip Vulnerabilities

DeHon discovered that anyone with an appropriate magnetic strip card reader can readily extract the information from a card and make a copy, onto an old ATM card or the like. Says DeHon: ``Equipment to duplicate or synthesize MIT Cards can be readily obtained for less than $500 and requires no technical expertise to operate. The technically inclined

can put together suitable equipment at a much lower cost." [8] As noted in section 6.1.1, the magnetic strip on the card contains the owner's MIT ID number and a 42-bit code identifying the owner.[26]

Unfortunately, a magnetic strip does not allow much in the way of flexibility in terms of how data is stored on the card. The data may be encrypted, for instance, but anyone can still copy the card's contents without knowing the key. The best security possible for this type of hardware, then, is ``security through obscurity,'' that is, security by preventing others from gaining physical access of your card and by preventing others from reading the contents of your card while the data is being transferred between the card reader itself and the access panel as described in section 6.2.1. While the problem of eavesdropping on reader-panel communication is more of a physical access issue than a technical limitation, and even so might possibly be solved by encrypting that communication, the problem of preventing others from accessing your card is more difficult.

On MIT's campus there is no more universal identification card than the MIT ID Card. The card can now be used to purchase food from campus vendors, is used to enter buildings, as an identification scheme by the Student Services Center and most other MIT administrative groups, as collateral for borrowing videos and keys at student dormitory desks, for parking, and so on. While not all of these uses require that the ID change hands, the use of the MIT ID for collateral does require surrender of the card. While surrendered, the owner has no control over whether the card is copied. And once copied, due to the wealth of services available with the card, not only is the owner's identity compromised but he can also lose monetarily. In his report, DeHon suggests not using the card as collateral precisely because the card is so easy to duplicate. In fact, this recommendation became policy shortly after his report was published, but the policy reverted back to the original shortly thereafter.

Because of its many uses, and because of the tendency for the MIT ID to be given to others for sufficient time for copying as a form of collateral, the security provided by the magnetic strip is not acceptable.

RFID Vulnerabilities

Unfortunately, the new MIT ID Cards that contain RFID tags only make the problem worse. Because the type of RFID used by the card, so-called ``passive'' RFID, always transmits the same data to the reader, the acquisition of the data sent in a single session can be used to make a duplicate of the card.[27] This data can be read by a third party in two ways:

1. By reading the waveform emitted by the card when it is activated by one of MIT's readers.
2. By exciting the card and reading the waveform emitted by it.
3. By getting access to the contents of the magnetic strip.

Method 1 above is difficult because the excitation range for card's particular RFID implementation is not very great, and your presence is likely to be noticed. Method 2, however, is not very difficult to accomplish with a little technical skill or an RFID reader. Because the range of the card's RFID tag is great enough to pass through a wallet or bookbag, the extraction of the RFID tag's data can be done without the owner's knowledge or even suspicion - affording the attacker a greater likelihood of escaping undetected and able to use the information he or she has gleaned.

Method 3 relies on the fact that the same information is kept on the magnetic strip as in the RFID tag. According to Dan Michaud, the rationale behind this decision was to avoid having to upgrade the access panels. Currently, the access panels have room to store about 20,000 identifiers. The card office has issued over 10,000 ID cards. If each card had multiple identifiers there would not be enough space on most access panels to keep all of the identifiers. In light of this limitation the card office decided to use the same identifier both on the magnetic strip and in the RFID tag. Unfortunately, this decision led to a serious vulnerability as well.

When MIT first contracted with Indala to bring RFID on campus, Indala assured them that the data stored on the cards was ``encrypted,'' however this was not the case. [22] As mentioned in section 5.2, only ``active'' cards are capable of real encryption, as real encryption relies on being able to perform computationally expensive (relative to the power used) tasks. ``Passive'' cards simply rebroadcast the same data each time they are activated, and are not capable of real encryption. This is not to say they are not useful, of course: in a system where there are no adversaries there is no need for strong encryption. If there is no incentive to spoof the system, there is no need for encryption. If you are counting cattle, the cattle are not going to impersonate each other; there is no need for strong encryption. Members of the MIT population are not cattle; we need strong encryption. The Indala system uses passive RFID tags, and thus cannot provide strong encryption. Under these circumstances it stands to reason that it would only be a matter of time before the ``weak'' encryption scheme were broken.

Keith Winstein, Austin Roach, and Josh Mandel showed in Spring 2004 that there is a trivial relation between the pattern of bits stored on the RFID tag and the identifier used on the magnetic strip of the same ID card. Now that this information is public, anyone who has access to the magnetic strip data of an ID card can recreate an RFID tag that emits the sequence of bits that the original card would have produced. Thus all of the issues surrounding the magnetic strip and its use as collateral apply even more so to the RFID portion of the card.

But even without this third method of gaining access to the data stored in the RFID tag, the passive tags used by the Indala system are vulnerable to replication and theft of identity simply by recording the signal they emit and playing it back. Winstein, Roach, and Mandel did this with $30 worth of hardware available at MIT's introductory electrical engineering laboratory. If MIT wishes to continue the use of RFID in the card, other options for secure transations need to be explored such as those mentioned in section 5.2.1.

Technical Recommendations

Our main technical recommendations can be broken down into two parts. In addition to changes we feel are required for the current system...

1. Stop the expansion of RFID readers on campus until a secure RFID technological infrastructure can be implemented.
2. Change the client stations so that only the most recent hour's worth of data can be viewed.

...we also present what we feel would be an ideal new system for a future implementation:

1. Use a secure card technology based on challenge-response authentication.
2. Keep localized access control through client stations (this is already present in the current system).
3. Allow client stations to view only the most recent hour's worth of entry data.
4. Maintain centralized access logs subject with restricted access enforced by...
    1. ...a two-tiered database that restricts access to sensitive username information.
    2. ...cryptographic mechanisms that require multiple keys held by distinct individuals to access sensitive data.
5. Provide a technical infrastructure to facilitate the keeping and reviewing of audit logs.

This section is broken down by which part of the system that a given recommendation affects.

1. Cards and Readers
    - Insecurity of RFID chip in the ID card
2. Access Control
    - Localized control of access for departments and labs
3. Data Management and Network Issues
    - Maintenance of MIT ID Card access log data
    - Protected and audited access to log data
    - Automated checks and balances in place to prevent fraud

Card and Readers

As we have already seen, the current implementation of RFID on the MIT ID Card is not secure and magnetic strip technology has fundamental properties that are irreconcilable with present uses of the MIT ID Card.

To summarize section 6.4, the two main liabilities of the RFID tag in the MIT ID Card are:

1. The encoding provided by Indala can be broken to reveal the contents on the card.
2. The card uses passive authentication and hence can be copied easily.

Solutions

We discuss here four possible solutions:

1. Revert back to using magnetic strip for all applications and continue the use of existing cards
2. Revert back to magnetic strip for all applications and reissue cards with no chip for card-owners with a proximity card
3. Recall all proximity cards and rewrite them with different IDs for the magnetic strip and RFID chip
4. Halt the expansion of the RFID readers on campus until such time as a secure RFID technology is in place.
5. Issue new cards with alternate technology that provides both security and convenience

The first option is the cheapest and only restricts new deployment of RFID. The main advantage of this option is ease of implementation. Restricting the use of RFID means that, over time, the RFID readers on campus will be replaced with magnetic strip readers; any new cards will only have a magnetic strip, and so all members of the MIT community will eventually be reissued non-RFID cards. The main disadvantage is that since the RFID tag contains the same information as the magnetic strip, the presence of RFID in the card is still a vulnerability, even though it is not used.

The second option solves the latter vulnerability by doing away with RFID in the entire system altogether. This option has the obvious advantage that the added vulnerabilities of RFID are not present in the system.

The third option is more complex because it requires the replacement of a large number of access panels. This option has the advantage that the RFID tags and magnetic strip data are divorced of each other, so that reading one will not tell you anything about the other. This can be useful for things like TechCash, which only uses the magnetic strip for the moment: even if an attacker gains access to the RFID tag (easier than the magnetic strip contents, since no physical access of the card is required), he or she will not be able to use the victim's TechCash account.

The first three options, while relatively inexpensive and implementable over the current system, still have many of the vulnerabilities that the magnetic strip and RFID tag have individually. Of these three, only the third is likely to be accepted by the MIT community. In our survey of the student body, approximately 41.7% felt that the convenience of RFID is worth the security risk. Now that RFID technology has been introduced, it is unlikely that (the student body, at least) will respond well to its withdrawal.

The fourth option is what we recommend for now. The MIT Card Office has already expended considerable effort in implementing the current system of prox card readers; students, faculty, and lab directors have all voiced the opinion that RFID is a generally useful tool, and they would probably not respond well to a removal of RFID. However, to eliminate the extra cost of installing a poor RFID system and needing to replace it later, we strongly recommend that expansion of the current RFID system be stopped.

The fifth option - the contactless smartcard - is ideal for a new system. The MIT ID Card's ``Passive'' RFID's intrinsic vulnerabilities are based on the fact that the tag emits the same data each time it is activated. However, ``active'' tags do not necessarily suffer from this vulnerability. In fact, ``active'' tags have been in use for authentication throughout the world since 1997, when Hong Kong implemented what is widely regarded as the first implementation of ``contactless smartcard'' technology, the ``Octopus Card.'' The ``Octopus Card'' can be purchased locally with cash, totally anonymously or with personal information recorded so the card can be revoked if lost. Because of the quantities of capital involved, the designers of the Octopus Card needed a system they were confident could not be broken into - imagine having the money in your pocket or wallet stolen through the very walls of your pocket or wallet! Clearly an unacceptable vulnerability.[28]

At the time when the designers of the Octopus Card were deciding on a system to use for authentication, the most secure mechanism available was the smartcard, a card with a little chip on it capable of performing strong encryption. When used, the smartcard receives power from the reader it is inserted into and with this power is able to have a secure conversation with the reader. As discussed in Sectionrefsmart above, smartcards ensure the integrity and privacy of the key data it stores (through various mechanisms) and perform challenge-response authentication with a reader.

Preferring a contactless solution, however, the designers of the Octopus Card designed a way to supply a card with enough power via induction coils to allow the card to perform strong encryption. In this manner, the designers were able to produce what is now commonly known as the contactless smartcard. Described in sectionrefclsmart, the contactless smartcard is an ideal solution to the problem that visibility of communications between a passive RFID tag and a reader leads to the ability of an eavesdropper to emulate the tag.

Access Control

The current system of providing client stations to departments that request it must be continued because many of them require expedited access control. The important addition that needs to be made to the current system is the option for a lab to request to turn on the feature of access logging. There are some labs that absolutely require tracking due to sensitivity of information, high value equipment or protected equipment stored within the building. In order to ensure that these labs will always have the option to control what happens to their property, it is important to allow for them to request this option. This would require a change to the existing software as described in the technical discussion of

the current system. If a new system were to be developed, local access control would need to be a key requirement.

Another minor loophole that was identified in the current system, is the possibility of someone sitting at a client station to be able to see realtime data of entries and exits. This is made possible by keeping the client machine's screen turned on with a window of the access entries that are being sent to the central server. The number of entries that can be seen with this method depends on the buffer size of the window. The number of days worth of data that can be gathered is dependent on the amount that the readers served by that client station are used. The more frequently they are used, the lesser number of days worth of data will be shown on the screen. We recommend that this be changed so that client stations only show the most recent hour's worth of data. Our understanding is that this can be implemented easily, and we suggest that it be implemented as soon as possible to allay fears that administrators might use this information to track the movements of members of the MIT community.

Data Management and Network Issues

Maintenance of MIT ID Card access log data

The card access log data would be stored on the server in a similar format as it is now. Restrictions on accessing this log are described in section 4.

In light of the more frequent need for access the log of general entry and other system data that is *not* user-specific, as well as the need for accountability regarding access that *is* user-specific, we recommend that the MIT Card Office keep a two-tiered database: the first level is a relational database with all the columns it already contains, except the username field is replaced with an ID string - unique to each entry in the database - that maps into a second database; the second database is simply a secure mapping between usernames and unique IDs that can only be accessed by the parties discussed in section 4.5. The two-tiered nature of the database allows the Card Office to access the data it needs on a daily basis without restriction, but only anonymously or in the presence of the individual whose data will be accessed. Of course, in the case of a request from the MIT Chief of Police, approved by the dorm housemaster in the case of dorm log data, the individual in question need not be present.

Protected and audited access to log data

In order to enforce accountability of the policies set forth in section 4, we recommend keeping detailed logs of all the accesses made to the entry log data; the information kept about such accesses must include information about who accessed the log, who requested the access, and any other details about due process.

We recommend having two separate audit logs - an automated one and a manually created one. The first log is an automated one that automatically records every access that

is made to the central database. This must be programmed into the system. Every time a connection to the database is initiated, the following details must be recorded:

- Username of the person accessing the log
- Query timestamp
- Query contents
- Type of access (whether it was for troubleshooting or for gathering information)

This gives an automatic log of events that can be used for audits and corroboration. The log can be accessed by only one user account and the user account would be controlled by the Card Access and Oversight Board (CAOB). This would decouple responsibility for policy from the Card Office, ensure independence, and prevent changes to the audit log by unscrupulous elements.[29] The second log must be stored at the Police Station and contains physical, documented evidence of requests that were made and granted by the Chief of Police. Whenever a request goes through the Chief of Police, it must be recorded here. The details of the request must include

- Name of the person requesting the data
- Time of request
- Result of request
    - Whether the request was approved or denied
    - Reason for approval or denial
- Requested Data
    - Type of Data
    - Data format requested
    - Exact fields requested
- Reason for request

This would provide the more comprehensive log of the request made. The CAOB would have access to these audit logs, but the auditing itself will take place as described in section 4.8.

Comparable Systems: Harvard

There are other schools that encounter many of the same privacy and tracking data issues that MIT faces. The closest analogy to MIT is Harvard University, located in Cambridge, which experiences the same external threats to the students and members of the community, as the MIT community does because Harvard is located in the same city and the same urban environment. Actual uses for tracking data have occurred in situations and criminal investigations that are very similar to those which have occurred at MIT. These cases have included missing persons, vandalism, theft, and sexual assault. In some cases, students have requested their own data to aid in self-conducted investigations, but these requests for information have been denied. The existence of the card swipe logs has also helped to spur students guilty of academic fraud to admit to their crimes.

Harvard University currently operates a magnetic stripe card system similar to the one previously employed by MIT; the university has yet to switch to an RFID system. Like the MIT Card system however, data from card use is kept in logs, which can be accessed according to a policy that has never been formally distributed. This policy is described in an article that was first published in the Harvard Crimson Newspaper in 1993. This article is the only record of the policy which was created by student members of the Harvard University Civil Liberties Union and the Dean of Harvard College at the time, Fred Jewett. All of the information in the following sections on the ID card system used at Harvard was gathered from the article in the Crimson which described the policy, and an interview conducted with former Dean of Harvard College, Harry Lewis. Much of this information remains otherwise undocumented.

The Harvard system

Harvard's magnetic stripe card system was implemented in 1994, at roughly the same time a similar system was introduced at MIT. The system keeps a record of entries and exits to dormitories and other buildings, although the amount of time for which such records are stored is not well documented among policies and procedures laid out on the Harvard University ID services website.

Policy in Theory

Harvard University's policy on access to tracking data is not well documented. The only mention of such a policy appeared in The Harvard Crimson in an article published in 1993. In response to the implementation of the card system, the Civil Liberties Union of Harvard (CLUH) objected to the college's ability to track students, and felt that a stringent policy regarding the use of such data should be formulated to prevent the possible misuse of recorded information. The student leaders of CLUH collaborated with Fred Jewett, Dean of Harvard College at the time, to develop a policy that was acceptable to both the administration and the students. This policy was passed by the Administrative board in early April of 1993.

According to a Former dean of Harvard College, the actual policy has never been formally described anywhere although it was officially adopted by the Administrative Board. Upon discovering this fact as a result of inquiries for this report, Former Dean Lewis has advised his successor's to post the University's policy on card swipe data access on its website.

The policy stipulates that information can only be released with permission from the Dean of the College, or by the student whose information is to be released. Any data that is to be released to Harvard University Police will be released only ``under circumstances when the information is important in the investigation a crime or other incident related to campus security." Whenever information is released to any party, a copy of the released information must also be provided to the student. The CLUH felt that this policy struck the right balance between preserving information because it was useful and preserving the information simply because it was possible.

Policy In Practice

Since the policy was adopted, the question of whether it has been strictly followed is debatable. It is certain that the general spirit of the policy was followed, but strict enforcement has not occurred. During Dean Lewis' tenure as Dean of the College, all requests for information by the police or any other party were directed to him. The Harvard University Police Department (HUPD) knew to contact him whenever it was necessary to request card information. The Dean's jurisdiction, however, was limited to information of entry and exit from any of the University's dormitories. In one case, where the police requested entry/exit information from the dining hall, the Dean was asked for permission even though his jurisdiction did not extend to the dining halls. Those who requested information generally understood that the policy for making such requests required the permission of the dean. Dean Lewis felt that the provision of requested information to students was one of the requirements of the policy that was not always followed.

The data access policy only applies to dormitories because most students do not have access to other campus office buildings and labs after about 6 pm. This policy is beginning to change as students require more access to buildings on campus, such as labs and computer clusters, to complete work. Once card access is expanded to these areas, the policy for accessing data about students will also change as the data collected will include students not under the watch of the Dean of Harvard College, such as graduate students.

In most of the cases where card entry data was needed to help solve criminal investigations, most of the data was corroborated by witness accounts; the card swipe data did not serve as the primary piece of evidence. In these cases, the police requested very specific data from different locations during a fairly narrow time window on the order of a couple of hours. One of the provisions of the original policy allowed for student authorization for the release of data, but it seems that this was largely ignored over the years as student requests were often denied by the Dean of the college.

Comparable Systems: Stanford

Another system that is similar technologically to MIT's is the Stanford ID card System. The Stanford Campus Card serves as identification, library card, electronic key, and debit card for the StanfordCardPlan, an account system similar to MIT's TechCash. Users can actually take out cash from their StanfordCardPlans using their ID cards. The Stanford Campus Card also contains both a magnetic stripe, and an RFID chip. Like the MIT RFID card, the RFID chip on Stanford's card can be activated within 12 inches of the reader, and tracking data can also be stored. Access to campus buildings, elevators, and dormitories is granted by the Stanford card. Access control is not technically described in too much detail on the Stanford Campus Card website. However, the site does say that access can be restricted according to day of the week or time of day, and can be granted on an individual basis or through departmental and class lists.

Data storage

The reason for presenting the Stanford Campus Card System here is that although the technology of the Stanford and MIT systems is extremely similar, the policy surrounding the Stanford system is different from MIT's in one very major way: tracking data is stored indefinitely, and in effect, forever. Initially tracking data is stored for one month on the active card database system. Each day, the data is backed up on optical disks as a precaution against system failure. These backup disks are reused every seven days, so 7 backup disks with data exist at any given time. After the one month active data period is expired, the data is transferred to optical disks which are then stored indefinitely: they are neither destroyed nor erased.

The data on these disks is recorded in a proprietary encrypted format, which prevents the misuse of the data therein by parties without access to the encryption methods or the Campus Card System Software. This software is apparently the only software that is capable of reading data from the storage disks. Stanford's Card system, much like the Indala system at MIT, is a completely proprietary system and the software and hardware employed are completely devoted to card operations. Registration information from the Stanford Axess system, equivalent to MIT's Websis, is fed into the card system, but all other records are kept separately from the card system. No other personally identifying information is given to the Card system from Axess.

Access to Data

Authorization for access to the data by people other than the Manager of Campus Card Services is also granted differently at Stanford. Whereas the current system at MIT allows the police to grant requests for data, Stanford grants access only with student consent, or a subpoena for that information. The Stanford ID services website clearly lists the exceptions to this rule as well. These exceptions include disclosure of information in compliance with regulations imposed by federal law on card issuers and providers, and disclosure without card user consent in the event of a safety or health emergency, or a criminal investigation. There are other exceptions to the rule, however. Computers in several libraries, the bursar's office, and dining services can also access certain unspecified types of data from the card services office. [16]

Feasibility of the Proposed System

In this section we hope to explore the feasibility of our proposed system. The recommendations we make above we have broadly classified as technical and policy recommendations. On the technology side of the card issue, there are three main factors to consider: security, convenience, and cost. On the policy side of the issue, the main concerns are privacy and accountability. With the continuation of an access logging system, the privacy of all members of the MIT community is at stake. Our proposed

recommendations deal with these two issues by addressing both of them to the greatest extent possible and by ensuring that there are as few loopholes in the system as possible.

Our discussions with John McDonald of Enterprise Services have indicated to us that substantial changes to the current system are not feasible in the short term. To address this concern, we have ensured that out most important recommendations are inexpensive and easy to implement. We hope that the ideal system we have described in this document will be used as a template for any future system should MIT decide at some point to upgrade its current system to the state of the art.

Security

Security on campus is a very important issue. MIT is an urban campus that has a comparatively open access policy. It is therefore extremely important to ensure that areas that are not as public as others are not made open through a compromise of the access mechanism - the MIT Card. Along with the access policies that are in place for private and/or restricted areas, we need to make sure that the card itself is secure. The technology that is used should not easy to fake or duplicate. It should also not reveal private information about the cardholder. Our proposed system is secure. It uses a very secure card technology: contactless smartcards with enhanced cryptographic functionality. The already existing virtual private network ensures that the data is transported securely to the central database. On the other end of the spectrum, in certain cases, such as on-campus thefts, access log data have proven to be useful in the past - so there is an airtight system in place to obtain this information for investigative purposes only. The data is stored for the required period of time and is available with due process.

Convenience

The recommended system maintains the convenience of cutting edge technology for card systems. The contactless smartcard works at the same range that the current proximity card does and allows for ease of use without handling at access points.

Cost

The changes to the current system that we recommend must be implemented as soon as possible. To this end, we have ensured that those particular recommendations have very low cost. In contrast, the construction of an entirely new, secure system is much greater. A thorough investigation of the costs of implementing such a system will be necessary before such a system is implemented, but we do not expect the cost of implementation to exceed the cost of the first MIT ID Card system completed in 1995.

Privacy

The new system has a transparent privacy policy in place along with a representative council to review and ensure the updating of the policy as required. The manpower and representation required is feasible and, in our opinion, necessary.

Accountability

One of the most important new additions to the system will be the auditing procedure. Access to personal tracking data needs to be monitored very carefully. The auditing procedure is in place to ensure that the system is doing what it is supposed to do. This will ensure that all the concerns, especially those related to privacy, are being addressed. We strongly feel that an auditing procedure is worth the added expense.

Conclusions, Summary of Recommendations, and Contributions

We have presented here:

- A description of the current MIT Card System in nearly as much detail as is available,
- A set of short-term recommendations for the MIT ID Card:
    1. Policy, to be implemented as soon as possible:
        1. The creation of a stronger, more permanent Card Advisory and Oversight Board
        2. Approval of accesses to dormitory tracking info is to be done by that dorm's housemaster
        3. Tracking and privacy policies must be made public and well known
        4. Students are allowed access to their own tracking data, and are provided with a copy of any of their data which is accessed by other parties.
        5. The entire process of accessing tracked data is audited by the MIT Audit Division
    2. Technical, to be implemented as soon as possible:
        1. Stop the expansion of RFID readers on campus until a secure RFID technological infrastructure can be implemented.
        2. Change the client stations so that only the most recent hour's worth of data can be viewed.
- A set of technical recommendations for a future MIT ID Card system:
    1. Use a secure card technology based on challenge-response authentication.
    2. Keep localized access control through client stations (this is already present in the current system).
    3. Allow client stations to view only the most recent hour's worth of entry data.
    4. Maintain centralized access logs subject with restricted access enforced by...
        1. ...a two-tiered database that restricts access to sensitive username information.

    2. ...cryptographic mechanisms that require multiple keys held by distinct individuals to access sensitive data.
5. Provide a technical infrastructure to facilitate the keeping and reviewing of audit logs.

In order to develop fair and balanced recommendations, we consulted the thoughts and concerns of many different members of the MIT community, including students. To our knowledge, this report is the first report on the MIT ID Card to consider input from a large section of the student body. Considering that the MIT ID Card is almost 10 years old, this fact both surprises and concerns us, however, we are happy to announce that it has now been done. In addition to our survey, we have also collected the opinions of the many who have written on this topic before into a comprehensive collection.

We hope that our short-term recommendations are implemented in a timely manner, and that our long-term recommendations are seriously considered for any future system.

Appendix

Survey

This appendix contains our survey questions and available responses, as well as how our survey respondents answered those questions.

The full contents of the survey page are given here, and each possible response is followed by the total number of respondents who selected that response and what fraction of total respondents this total represents (percentages may not sum to 100% due to rounding). In total, we received 513 responses.

This survey is designed to discover the privacy concerns of MIT students with regard to the MIT ID Card system. Our goal is to propose a system that will address the concerns of students and members of the faculty, lab directors, and the MIT campus police.

We appreciate your contribution.

The following questions are to gauge current opinions toward the MIT ID Card system.

1. Were you aware that the MIT ID Card contains an RFID tag in it? *(RFID stands for Radio Frequency IDentification; the tags are small, cheap radios-on-a-chip*

that emit identification strings when activated by a reader. The MIT ID uses a form of RFID that is entirely passive, and can be read from 2-5 feet away.)

1. Decline to respond *0 (0%)*
2. Yes *269 (52.4%)*
3. No *244 (48.6%)*

2.

Are you comfortable with the current level of security offered by the card and associated reader technologies?

1. Decline to respond *3 (0.6%)*
2. Very comfortable *80 (15.6%)*
3. Somewhat comfortable *171 (33.3%)*
4. Neutral *89 (17.4%)*
5. Somewhat uncomfortable *68 (13.3%)*
6. Very uncomfortable *22 (4.3%)*
7. I was not aware of any security concerns with the current system *80 (15.6%)*

At present, the MIT Card Office records when an individual enters a building or lab using their card and keeps these records for 2 weeks. This policy came into effect in the Summer of 2002.

1.

Were you aware of this policy?

1. Decline to respond *2 (0.4%)*
2. Yes *134 (26.1%)*
3. No *377 (73.5%)*

2.

How do you feel towards this policy?

1. Decline to respond *2 (0.4%)*
2. Very favorably *51 (9.9%)*
3. Somewhat favorably *106 (20.7%)*
4. Neutral *189 (36.8%)*
5. Somewhat unfavorably *135 (26.3%)*
6. Very unfavorably *30 (5.9%)*

3.

In your opinion, how long should MIT keep these records?

- Responses here varied widely. Many students felt that 2 weeks was an acceptable amount of time, some thought that the data should be kept for months, while others preferred days.

The current system does not allow for different areas of campus to be treated differently for the purposes of tracking entry. The following questions refer to a hypothetical future system.

One group has suggested a policy of only recording unsuccessful attempts at entry, that is, only record a card swipe when entry to a location is denied.

1.

How would you feel about such a policy?

1. Decline to respond *6 (1.2%)*
2. Very favorably *27 (5.3%)*
3. Somewhat favorably *113 (22.0%)*
4. Neutral *119 (23.2%)*
5. Somewhat unfavorably *184 (35.9%)*
6. Very unfavorably *64 (12.5%)*

The current 2 week policy may have been implemented in part because of on-campus labs' desire for increased security. As such, one suggestion is to limit tracking of entry to those areas alone.

1.

How would you feel about a policy that restricts tracking to those labs that specifically request it?

1. Decline to respond *5 (1.0%)*
2. Very favorably *109 (21.3%)*
3. Somewhat favorably *226 (44.1%)*
4. Neutral *87 (17.0%)*
5. Somewhat unfavorably *71 (13.8%)*
6. Very unfavorably *15 (2.9%)*

2.

If such a policy were implemented, how much should lab members' input be considered in the decision to track entries/exits? (In contrast with letting the decision be up to lab directors alone.)

1. Decline to respond *8 (1.6%)*
2. Very much *138 (26.9%)*
3. Somewhat *155 (30.2%)*
4. Don't know / Up to the labs *173 (33.7%)*
5. Not much *31 (6.0%)*

6. Not at all *8 (1.6%)*

Getting back to RFID, the current system allows cards to be read by a card reader in close proximity. This means that, hypothetically, someone can read your ID card's RFID identifier by walking near you with a reader (readers can be quite small). With this ID, they can access wherever you can access, can use your TechCash acount, and can discover your MIT ID number.

However, many argue that the vastly increased convenience of RFID (not having to take a card out of a wallet) outweighs the risks associated with reading-at-a-distance.

1. What is your opinion on this matter? Is the increased convenience of RFID worth the risk of someone getting your ID number?

    1. Decline to respond *4 (0.8%)*
    2. The convenience of RFID is very much worth the risk *32 (6.2%)*
    3. The convenience of RFID is worth the risk, but I am concerned *182 (35.5%)*
    4. Neutral / Doesn't make much of a difference *38 (7.4%)*
    5. The convenience is not worth the risk, but not by much *116 (22.6%)*
    6. The convenience is definitely not worth the risk at all *125 (24.4%)*
    7. I don't know *11 (2.1%)*

The following information is for demographic purposes. If you feel comfortable providing this information, we would appreciate it.

1. Do you live on campus?

    1. Decline to respond *7 (1.4%)*
    2. Yes *450 (87.7%)*
    3. No *56 (10.9%)*

2. Which Living Group do you live in?

    1. Decline to respond *26 (5.1%)*
    2. Baker *69 (13.45%)*
    3. McCormick *54 (10.53%)*
    4. Burton-Conner *38 (7.4%)*
    5. MacGregor *3 (0.6%)*
    6. New House *25 (4.9%)*
    7. Next House *69 (13.5%)*

8. Simmons *1 (0.19%)*
9. East Campus *54 (10.5%)*
10. Bexley *19 (3.7%)*
11. Senior House *25 (4.9%)*
12. Random Hall *23 (4.5%)*
13. Ashdown *2 (0.4%)*
14. Eastgate *0 (0%)*
15. Tang *2 (0.39%)*
16. Warehouse *0 (0%)*
17. Sidney-Pacific *53 (10.3%)*
18. Westgate *0 (0%)*
19. Edgerton *1 (0.2%)*
20. Green Hall *0 (0%)*
21. Other / FSILG *49 (9.6%)*

3.

How many years have you been at MIT as an undergraduate student?

- $0 < years \leq 1$
- *139 (27.1%)*
- $1 < years \leq 2$
- *115 (22.4%)*
- $2 < years \leq 3$
- *86 (16.7%)*
- $3 < years \leq 4$
- *90 (17.5%)*
- $4 < years$
- *1 (0.2%)*
- total *431 (84.0%)*

4.

...as a graduate student?

- $0 < years \leq 1$
- *29 (5.7%)*
- $1 < years \leq 2$
- *12 (2.34%)*
- $2 < years \leq 3$
- *15 (2.9%)*
- $3 < years \leq 4$
- *8 (1.56%)*
- $4 < years \leq 5$
- *5 (1.0%)*
- $5 < years$
- *2 (0.4%)*
- total *71 (13.8%)*

If you have any comments about this survey or privacy at MIT in general, please share them with us here:

If you would like to be entered in our drawing for a $20 gift certificate to the Cambridgeside Galleria, please provide your username for us to contact you. Your username will not be associated with your responses in any way.

@mit.edu

Submit Query

Thank you for participating!

Priya, Neha, Chaitra, Al, and J.D.

If you have any questions, please send e-mail to privacy *at MIT.edu*

Bibliography

1

By *name* Year: Publisher.

2

Jonathan A. Ives, *The HIstory of the MIT ID* 1998-1999: `http://web.mit.edu/mitid/www/history.html`

3

MIT Policy and Procedures: Privacy and Disclosure of Information 1997: `http://web.mit.edu/policies/11.0.html`

4

Scott Thorne, *People Related Projects* 1994: `http://web.mit.edu/mitid/www/t_info.admin-arch.37707.TXT`

5

Charu Chaudhry, *MIT Card Replaces Meal Card, Keys* The Tech Vol 113, No 45, Pg 9, 28 Sep 1993

6

Ifung Lu, *MIT Card Raises Issues of Privacy, Security* The Tech Vol 113, No 55, Pg 1, 5 Nov 1993

7

André DeHon, *Security Assessment of the M.I.T. Card* 1995: http://www.ai.mit.edu/people/andre/mit_card/security_assessment/security_assessment.html

8

Jeremy Hylton, *MIT Card Security Is ``Laughable''* The Tech, Vol 115, No 16, Pg 1, 7 Apr 1995

9

Dana Levine, *MIT Card Upgrades Lead to Expansion* The Tech, Vol 119, No 47, 5 Oct 1999

10

MIT Reports to the President 2000-2001: Dean for Student Life - MIT Card Office 2001: http://web.mit.edu/annualreports/pres01/07.00.html#card

11

S. Hodges and M. Harrison *Demystifying RFID: Principles & Practicalities* 2003: MIT Auto ID Center

12

Oliver Kömmerling and Markus G. Kuhn, *Design Principles for Tamper-Resistant Smartcard Processors* 1999: http://www.cl.cam.ac.uk/ mgk25/sc99-tamper.pdf

13

Ari Juels, *Minimalist Cryptography for Low-Cost RFID Tags* October 2003

14

Ari Juels, Ronald L. Rivest and Michael Szydlo, *The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy* 2003: In Proceedings of 10th ACM Conference on Computer and Communications Security (CCS 2003)

15

Mark P. Hurst, *Deal of Student Service Card Deck Reveals Jokers* The Tech Vol 14, No 12, Pg 5, 8 Mar 1994

16

Stanford University Information Technology Systems and Servies, *Campus Card Security and Confidentiality* 2003: http://www.stanford.edu/dept/itss/services/campuscard/security.html

17

Amy S. Bruckman, *MIT Card Holds Promise and Pitfalls: Questions of Privacy and Security* MIT Faculty Newsletter Vol 8, No 1, Pg 18, October 1995. Also available at http://www.ai.mit.edu/people/andre/mit_card/supplemental/asb-fnl-v8n1.txt

18

MIT Card Office, *Privacy Policy* http://web.mit.edu/mitcard/privacy.html

19

Privacy Rights Clearinhouse, *A Review of the Fair Information Principles: The Foundation of Privacy Public Policy* 1997-2004: http://www.privacyrights.org/ar/fairinfo.htm

20 Massachusetts Bar Association, *Mass Law Help: School Records Law* http://www.massbar.org/lawhelp/legal_info/index.php?sw=236&vt=3#schoolrecords

21 U.S. Department of Education: *Family Educational Rights and Privacy Act (FERPA)* http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

22 Dan Michaud, head of MIT Card Office, *Unpublished Interview and/or Electronic Communication* Sep-Dec 2004

23 John McDonald, Associate Director of Enterprise Services, *Unpublished Electronic Communication* December 2004

24 SLP, *Housemaster Roles* http://web.mit.edu/residence/hm/roles.htm

25 Josh Mandel, Austin Roach, Keith Winstein, *MIT Proximity Card Vulnerabilities* 2004: http://web.mit.edu/keithw/Public/MIT-Card-Vulnerabilities-March31.pdf

26 Indala, *FlexSecur* http://www.indala.com/products/flexpass/flexsecur.html

27 *Unpublished Conversation with Indala Sales Representative* November 2004

28 CSAIL Prox Card Privacy Committee http://proxcard.csail.mit.edu/ 2004

About this document ...

The MIT ID Card System: Analysis and Recommendations

This document was generated using the **LaTeX2HTML** translator Version 2002-2-1 (1.70)

The command line arguments were:
latex2html `-split 0 mit_id.tex`

The translation was initiated by J.D. Zamfirescu on 2004-12-11

Footnotes

... entry;[1]

This question was ``In your opinion, how long should MIT keep [entry data] records?''

... ID.[2]

This history of the MIT ID is highly indebted to [2], a draft document maintained by MIT Information Systems. The MIT policy for protection of personal data can be found in chapter 11 of [3]. The Tech Info document entitled ``People Related Projects'' is [4].

...2[3]

Taking after the document that outlined its creation, the new database that would manage the new MIT ID system was called the ``People Database.'' This represented version 1.0 of the MIT ID storage and lookup system. It was not until version 2.0 in the fall of 1997 that the system received its current name, MIT ID Database.

... stolen.[4]

To this day, dormitories and some other places on campus require students to leave their ID card as collateral for items borrowed. Likewise, it is still the stated policy of the MIT Card Office that students should never agree to leave their card as collateral.

... suggested.[5]

DeHon discovered that when a card was reported stolen and a new one reissued to a student, the only difference between the stolen card and the new card was that a counter encoded on the magnetic stripe was incremented by one. Therefore, it would be trivial for someone to steal a card and use it even after the card was reported stolen. To address this issue the counter was replaced with a randomly generated number.

... attention.[6]

1995 was indeed a focal point in the debate over the MIT Card. It was during this year that most objections to the proposed technology and policies were raised and it was during this year that campus-wide interest reached a noticeable peak. The number of issues raised by member of the MIT community in 1995 are too numerous to be listed in full here. For an excellent synopsis of this early period in the MIT Card's development, see [17].

... application.[7]

CS Gold is Diebold's solution for campus card systems and supports a wide range of features from access control to meal plan access. There are many features in the CS Gold application that proved desirable for the MIT Card, particularly its Y2K compliance and support for an Oracle Database. For a description of the current version of CS Gold offered by Diebold, visit the products website at: `http://www.diebold.com/opccsol/Products/CSGold/CSGoldSoftware.htm`.

...levine[8]

[9] article makes general reference to some of the changes implemented by the Card Office in addition to some of the key benefits. The Card Office itself reported its progress towards these upgrades in its annual Reports to the President. Reports to the President from 1994 to 2003 can be located at: `http://web.mit.edu/annualreports/`. One of the key benefits of the 1999

upgrade outlined by the card office was the ability to connect card readers to the central computer system via the MIT network. Prior to this ability, a wire had to connect each reader to the server in E32.

... spring.[9]

A client station is the computer system that connects to the MIT Card system to authenticate access. The client system allows for local access policies to be set. A full description of this system and other details necessary for a department or lab to setup use of the MIT Card for access control can be found on the MIT Card Office website at: `http://web.mit.edu/mitcard/department.html`.

... staff.[10]

To date the MIT Card Advisory Council has made no known recommendations or reports. In fact, the council has no web site and minutes from its meeting are not published in any easily accessible location.

... 32.[11]

The details of RFID technologies and the particulars of MIT's implementation are discussed in section 6.

... (LowCo).[12]

Coercivity is the measurement of the strength of the magnetic field required to affect data encoded on the strip.

... ISO[13]

International Organization for Standardization

... cards[14]

For more infromation see `http://www.idedge.com/ID_Card_Learning_Center/Smart_Cards/Contact_Smart_Cards.cfm`.

... ISO/IEC[15]

International Electrotechnical Commission

... memory.[16]

For more information, see `http://www.biocentricsolutions.com/media/Tokens.pdf`.

... reader.[17]

For more information, see `http://www.idedge.com/ID_Card_Learning_Center/Smart_Cards/Contactless_Smart_Cards.cfm`.

... card[18]

http://www.calypsonet-asso.org

... card[19]

http://www.oystercard.com

... areas:[20]

For more information see *Smartcard Technology and Security*, `http://people.cs.uchicago.edu/~dinoj/smartcard/security.html`.

... array.[21]

For more information, see `http://www.st.com/stonline/press/news/year1998/t138ma.htm`.

... Card.[22]

For more information see `http://www.indala.com/pdf/products/FlexISO_Imageable_Card.pdf`

...std2[23]

Figures are from `http://www.varo-inform.com/adv_poly_plasticcards_gost_eng.htm`

... reader[24]

For more information, see `http://www.indala.com/pdf/products/Arch_Data_Sheet.pdf`.

... California.[25]

For more information, see `http://www.sonicwall.com/General/DisplayDetails.asp?id=207`.

... owner.[26]

Under earlier versions of the card, this 42-bit code was merely incremented when a card was reported as lost or stolen - an obvious vulnerability. However, it appears that now a random value is assigned for the 42-bit code.

... card.[27]

A brief Google search reveals a number of websites with instructions for how to copy an RFID card.

... vulnerability.[28]

Since the MIT Card can also control monetary assets - in many cases more than the HK$250 that can be stored on an Octopus Card - it is vital that these assets be strongly protected.

... elements.[29]

Dan Michaud has discussed with us his concerns about possible his potential successors.

J.D. Zamfirescu 2004-12-11