RFID and Student Privacy

In modern times, technology is being used to accomplish things that were once impossible. Seemingly limitless information and data can be accessed any time and at any place around the world. Not only can doors be unlocked electronically, but they can also be restricted to only allow certain individuals. The latter is very common in places that require access control on buildings containing sensitive information, such as among students at universities. These usually have large populations, thereby making the control of traditional keys impossible. A common solution to this problem is the implementation of a computer readable ID card, the most notable being the Radio Frequency IDentification (RFID) card standard, and a large implementer of these: HID Global. However, there is still the question as to whether this technology is a violation of student privacy. Some people believe that students give up their rights to privacy as soon as they step onto campus, especially if it is a public institution. This is not true, the Family Educational Rights and Privacy Act (FERPA) affords much protection regarding student privacy, but is mostly aimed at the unlawful distribution of a student's grades (EPIC Student Privacy 2012). Other rights of privacy, such as daily movements on campus and access to the student's personal and financial data could be violated depending on what information is embedded within the ID card, and how well the data associated with the card is protected. In the strictest sense, universities are only compromising students' privacy, not violating it, but doing so would not be difficult. Another open question is the ethical dilemma of teaching by requirement the behavior of always carrying "official" identification.

The technology behind this access control, and many more services afforded students by universities such as the Georgia Institute of Technology (Georgia Tech), is an ID card that is an

RFID enabled HID proximity card, which is provided to Georgia Tech by Blackboard Inc. RFID prox cards are used by holding the card in the proximity of a reader, which emits a frequency that activates the card (Igoe 2012). Once powered, the card emits its identifier as a string of binary bits. The reader takes the identifier, and passes it to an access controller, which verifies the validity of the number, and then either approves or rejects it, unlocking the door if required. A drawback to this system, and a security feature, is the short read range (on the order of inches), which requires close proximity to the reader to facilitate a proper read.

Identifier formats are hard to pin down because there are many standards, and many different lengths. One common standard is the HID Corporate 1000, which is 35 bits in length. This is where some security is implemented, due to the contract between an organization and HID. The HID Corporate 1000 contract grants exclusive rights to the organization for the format in which they choose to encode the card's unique identifier (Understanding card data formats 2006). Legally, no other organization can use that format, and HID cannot discuss the format, nor sell cards encoded that way without written consent from the organization (required even when the order is from within the organization). Identifiers are generally broken into a Facility Code section, a Card Number section, and several parity bits, which are used to determine validity of the identifier. An example breakdown of the identifier includes 3 bits of parity, a 12 bit facility code, and 20 bits for the card number. As is clear by the basic format, there is no inherent security provided aside from the obfuscation of the numbers through the parity bits. To emulate any card, one would only need to know the facility code of the target (generally few per organization), how to generate the parity bits (can be found by brute force with enough known cards), and the card number to be emulated (which is generally printed on the card). Another way to get this information would be to simply read the card, and emulate the data resulting. While

there is no personal or sensitive data in this format, it is disconcerting to know that for a relatively small sum, one could make a device that can read any card of this type, and for little more, emulate a card as well (Igoe 2012).

If it is so easy to emulate an RFID prox card, what uses do Georgia Tech and other schools tie to this insecure medium? Access control is the most used feature of the prox card on campuses. The first thing to know, is that most universities have multiple tiers of access restriction based on the cards. Generic services, such as access to the library, are restricted to simply having the card; often students are required only to hold up their card for the security guard on the way by. This is clearly not secure, but is a decent model for non-sensitive areas such as the library, which requires those without cards to sign in. Other buildings maintain a list of cards, managed locally, that are authorized to gain access to the building. On top of that, some buildings that house more sensitive activities, such as the research buildings, also have 24/7 guards that ensure those without the cards cannot slip in with an unsuspecting person holding a door.

Another common use for these cards is the facilitation of a monetary transaction with funds from the student's account. On Georgia Tech campus, nearly all vendors, from commercial offerings to vending machines and dining locations, accept the card as payment. Additionally, several restaurants immediately off campus have partnered with Georgia Tech to allow students to use their card as payment. This is a convenience to the student, because it relieves them of having to carry several forms of payment, so long as they stay on campus. However, this can be a burden to transient entities and clubs who want to allow payments during events like fundraisers, because the equipment can be complicated to use and is sometimes difficult to get, since Georgia Tech rightly regulates its use.

Lastly, the cards are used as a proof of identity. This is generally used in cases such as access to the library and other buildings, but also at times such as proving student status when gaining access to an athletic activity. Most classes require that a student present their card when turning in their exam, to prove that they are the student whose name is on the test, and that they are on the roster for the class. This is a decent deterrent of identity based cheating (having another person take the test for you), but is only as effective as the diligence of the exam proctors in checking the cards. Other schools, such as John Jay High School and Anson Jones Middle School of Bexar County, Texas, have begun utilizing similar cards to track students' locations in school, as well as take attendance in the morning (Vara-Orta 2012). Reactions to this move by the school system vary widely, with some being outright disapproval from both students and parents.

Clearly, there is room between the technology employed, the company contracted to manage it, and the use-cases for the privacy of the students to be violated. But are the universities actually violating privacy? Weaknesses of the simple RFID technology being employed are widely known, and could be exploited fairly easily on campus. This compromises the use of the proximity portion of the card as a guarantor of the presence of the actual card, and the identity of the person using it. This is not a problem with guarded entry points to buildings, as they could still physically check the card. However, this does not apply to using the spoofed card to gain access, and then showing a legitimate, yet unauthorized, card to the unsuspecting guard. A breach such as this does not overtly violate the privacy of the student, but does violate the privacy and security that is supposed to be protecting any student or faculty member in the building that is accessed. Imagine the safety hazard and dangers of a student who is not trained on machinery that has non-approved access to the machine shops located within the Mechanical

Engineering building. By using the machines, the student could be exposing himself, and any other personnel in the vicinity, to danger. Similarly, a student could cause trouble by spoofing access to a restricted building and browsing notes and other non-public materials related to research or academics.

Despite its shortcomings, a benefit of the cards being based on RFID is the format of the identifier. Because it needs to be unique, but also uniform, the identifiers have no room to store information about the student. Additionally, because of the way the technology works, there is no way to change the identifier of the card after it is made. This is beneficial because the student's data is not compromised immediately if his card identifier is read or spoofed. However, the attacker could conceivably use the information combined with information gleaned by attacking the servers that link card identifiers to data about the students. Overall, the cards themselves have proven to not be a direct privacy breach to the students, but introduce ways to compromise the system and hence, students' information and privacy.

Another major area of concern is the company that has been contracted to provide the RFID based cards, as well as provide other services to many universities, including Georgia Tech. Blackboard Inc. supplies the HID compliant card-based access control system, along with some or all of the systems that interface with the cards, to more than 200 universities nationwide (Jenkins 2003). This includes the payment system used by campus entities such as clubs, dining halls, the student center, and even laundry machine fees, and non-campus entities such as the restaurants and stores near campus. One well-known security technique is to minimize the entities that have access to the information, and here that is directly at odds with the university's wish to provide an all-encompassing solution for payment and access control with the cards. A disturbing example of Blackboard Inc.'s policies was demonstrated in 2003 when two students

were forced to cancel an academic lecture they were going to give at a convention over the insecurities of the system (Jenkins 2003). The procedure to block this lecture is important, in that it involved Blackboard Inc. filing a temporary restraining order (TRO) in which many unfounded accusations were made, and claims that would not hold up in court were reinforced by the unbalanced amount of resources between the students and Blackboard Inc. The case attracted attention because they sent a cease and desist letter that threatened claiming rights under the Digital Millennium Copyright Act (DMCA) to the students in addition to the TRO, which had no mention of DMCA in it. This is significant because it suggests that Blackboard Inc. knew claims along those lines were unfounded and unable to stand up in court, and used them as a scare tactic. Additionally, the TRO was served the day before the students were to give the lecture, which gave them no time to respond to the accusations. Is a company that acts like this, one with which students should feel comfortable confiding in with their data?

The privacy concerns of the use-cases should also be considered. Many large commercial companies collect data on the purchases of their customers, under the guise of providing a better product. There are also quite a few companies that specialize in accruing this data, and selling it to companies who want this. The real goal of this data acquisition is the discovery of trends, and hence targeted advertising. There have been alarming occurrences in the past like one example where a teenage girl was sent advertising based on her trend of purchases that implied she was pregnant before the parents knew. This may not be as consequential on a college campus, but it demonstrates that surprising things can be learned from things as simple as purchase history. In this situation, there is no way to definitively know whether the universities or Blackboard Inc. are profiling students based on purchase history. This is a place where the university is not

violating student's privacy outright, but is compromising it by adding another area where data could be taken.

Another use-case concern involves when the actual read of a card occurs. The effective read range of some of the hardware (such as the handicapped accessible) is quite long (one or two feet) (Igoe 2012). Because of this, a student can expect at least one read every day that they did not intend to happen, due to being close enough to the reader for it to activate the card. This along with intentional reads, such as using the card to pay for something, or when gaining access to a building, can build a surprisingly complete picture of the student's movements. This data does not outright violate the student's privacy, but as soon as they look at the data, they would be violating the privacy. Another potential violation arises if there are people with access to the data, such as technicians or guards, who could then misuse the data. Blackboard Inc. also advertises an electronic voting system based on the cards. It was not discussed in detail, but the possibilities of data misuse are great in any sort of electronic management, and electronic voting systems are generally criticized for being "black box" type applications. The thought of trusting a machine to accomplish a critical task is always hard to accept, especially when viruses and other forms of malware are prevalent in the news.

Lastly, the broader implications of the presence of ID cards should be considered. Currently, the United States does not require a member of the population to carry an official ID at all times. This right to privacy is one of the freedoms that is being taken for granted as of late. The requirement by universities for students to carry ID cards (by the fact that they are needed for everything from payment, to classes, to building access) could be considered to be desensitizing the student population to giving up their right to anonymity. Proponents of this

viewpoint never fail to mention that students are still developing and are impressionable, and because of this are more susceptible to the influence.

Due to the security implications surrounding the use of these cards, there are several questions that would need to be answered before a verdict could be reached as to whether or not a specific school was violating their student's privacy: What data is stored on the magnetic stripe of the card, which is commonly present on such cards? Are there people who monitor the reads by the readers? If so, do they have access to the information of the students? How protected is the data, and also the servers on which it resides? What data do third-party vendors have access to once they are a part of the student account payment system? Because universities go through Blackboard Inc. to get HID cards, is the card identifier format unique to the university or to Blackboard Inc.? Additionally, who owns the right to the format, Blackboard Inc., or the university? The presence of this many questions in a research paper indicates that universities should at the very least inform their students, faculty, and staff of the technology being imposed on them, and the possible privacy concerns that they should be aware of while in possession of that technology.

As should now be apparent, the "safe" and "secure" promises made by the companies who sell these systems are not true because of the inherently insecure technology it is based on. When a card can be read, copied, and emulated in less than a minute (EPIC RFID 2012), a system becomes much easier to compromise, and the compromise of a system like this can lead to violations of other students' privacy. Recall that other concerns over possible privacy violations could happen through the location and financial tracking of a student, and the availability and security of the data which is linked to the card's identifier. Lastly, it is worrying that students are being forced to relinquish their right to anonymity by having to carry the card at

all times. In conclusion, while it is not possible to say that universities and schools are violating students' privacy, they are compromising the privacy by adding more points of vulnerability which could be exploited by a malicious entity.

Bibliography

EPIC RFID - Electronic Privacy Information Center. (n.d.). *EPIC*. Retrieved October 31, 2012, from http://epic.org/privacy/rfid/

EPIC Student Privacy - Electronic Privacy Information Center. (n.d.). *EPIC*. Retrieved October 31, 2012, from http://epic.org/privacy/student/

Igoe, T. (2012). *Getting started with RFID: Identify objects in the physical world with Arduino*. O'Reilly Media.

Jenkins, J. (2003, September 30). Blackboard erases research presentation with cease and desist. *Chilling Effects*. Retrieved November 14, 2012, from http://www.chillingeffects.org/weather.cgi?WeatherID=383

Unknown. (2006). Understanding card data formats. http://www.hidglobal.com/page.php?page_id=10

Vara-Orta, F. (2012, May 26). Students will be tracked via chips in IDs. *San Antonio Express-News*. Retrieved October 31, 2012, from http://www.mysanantonio.com/news/education/article/Students-will-be-tracked-via-chips-in-IDs-3584339.php