A security analysis of the UBCcard (Nov. 2007)

Carlos Colon-Vonarx, Noriel Rilloma, and Taivo Evard

Abstract - **A security analysis of the UBC student card has uncovered several vulnerabilities, leaving it open to attack. Relatively easy exploits can give an attacker access to a student's assets. Our study began with a survey of student security habits, and found that the majority of students do not realize the value of their student cards nor the assets that they can access. Most students seem to be indifferent to card loss, and would present their cards to individuals who had no authority to view them. Next, we proved that it was possible to perform a replay attack with the UBC student card, using cheap and easily available technology along with a little social engineering. Our risk analysis showed that it was possible to profit from an attack. We conclude with a set of proposed countermeasures to reduce the vulnerabilities and prevent the possibility of attacks.**

Index Terms - **magnetic stripe exploits, student card vulnerabilities, student security habits, UBC student card security analysis**

I. Introduction

UBCcards are issued to all of UBC's 43,000 students and 2000 faculty. The UBCcard was introduced in 2003, and took over the functions of the AMS student card/library card. Since 2003 it has taken over the functions of a gym pass ID (replacing a previously separate "BirdCoop" gym pass card), residence meal plan cards (replacing the UBC Food Services card), residence key cards (Currently being used as a key replacement to access rooms in Gage residences, phasing out the usage of the previous magnetic swipe key cards), and most recently the Dining A La UBCcard program of 2007 (like the residence meal plan cards, it allows cardholders to place money on an account and use it like a debit card at UBC Food Services locations).

Figure 1. Four Generations of UBC Student Cards (1988, 1993, 2003, 2007)

Other residences (such as Place Vanier Residence) have considered using the UBCcard as an alternative to their own VIN cards, but have not done so yet. So far Gage Towers is the only university residence that uses VIN cards for full access (access to the tower, to the living unit/quad, and into individual rooms). The UBCcard is also used for the residence meal plan, available to Totem Park and Place Vanier residences. The card is used for a new pay-as-you-go meal plan , called the Dining A La UBCcard Plan. This plan allows money to be deposited onto a card's account and used at all UBC Food Services locations, and will serve as a prototype to add further debit card-like transaction capabilities to the card.

Figure 2. Four Generations of UBC Student Cards (rear)

As these services are consolidated into one card, so increases its risk of being copied and used with criminal intent. Cheap mail-order magnetic card writers and magnetic card blanks are easy to obtain, and a determined social engineer can quickly recoup his investment by gathering students' personal data and forging students' cards. A successful copy of the magnetic stripe on a UBCcard can be reproduced onto a blank card and used to access a student's assets associated with that card. In the most intrusive case, a student's home in residence can be accessed, resulting in a threat to both the student and his/her roommates' belongings and possibly even personal safety, depending on the threat agent. An attacker with personal knowledge of the victim could exploit this vulnerability even more easily.

As the UBCcard's growth in services continues to expand -- to become a debit-card substitute and a form of access to buildings and residences -- so does its potential for abuse. UBC staff does not appear to be trained to scrutinize ID presented for authentication. For example, UBC Food Services employees provide minimal scrutiny of whose card is being presented, as we were able to use another student's ID without incident. And UBC after-hours building access does not require any human verification.

UBC students do not appear to be practicing satisfactory security habits. Though many students rely on their card as a form of daily identification, less than half of the students that responded to our survey changed their default passwords, whose values can be easily deduced. Overall, the casual attitude displayed toward authentication by UBC staff and students alike pose risks for many assets that are now accessible through the new UBCcard.

II. Survey Results

A survey of UBC students' security habits was carried out with 196 respondents (53 paper respondents and 143 online

respondents). Ten questions were posed of issues surrounding the UBCcard, from which we were able to observe several interesting security-related statistics:

- Of the 89 respondents living in residences, 43 are using passwords for access to their residence and buildings, and 41 of these are using the default password (the default password being the user's date of birth).

- 77% (143 out of 185) students would consent to having their UBCcard swiped magnetically to improve after-hours security on campus.

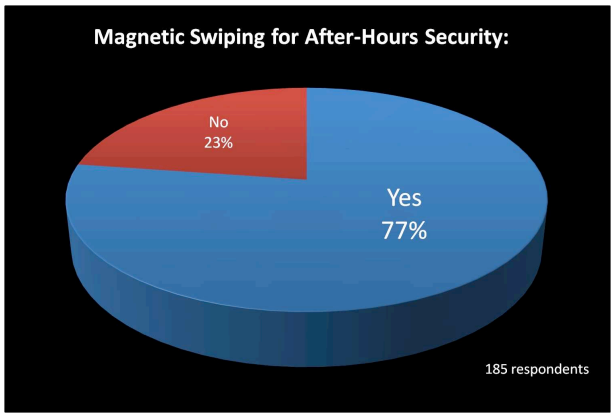

Figure 3. Magnetic Swiping for After-Hours Security

- Only 10 respondents (out of 196) indicated that they had not used their UBCcard as proof of their student status.

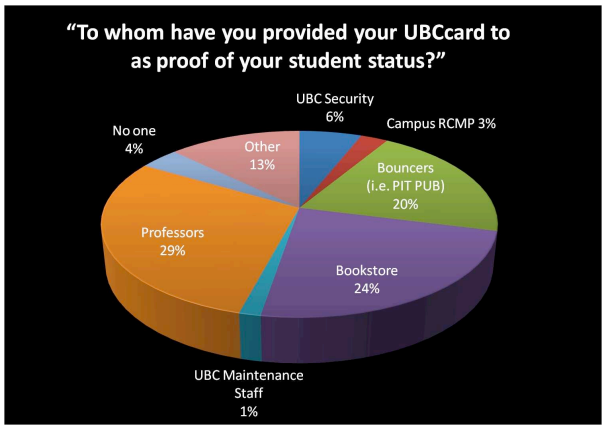

Figure 4. The UBCcard as proof of student status

III. GENERAL UBCCARD ANALYSIS:

Currently the magnetic stripe information on a student card can be used to access UBC Food Services meal plans (Dining a La UBCcard program, Totem Residence meal plan, and Vanier residence meal plan), and Gage Residences with minimal to non-existent security measures taken to ensure that the card swiped is an authentic student card. We have found that there seems to be no specific authentication procedure implemented for UBC Food Services during purchase transactions using meal plan cards. We have also found that there is no authentication procedure in place for access to Gage Residences. No password is used to access Gage tower and only a single password is used to access a unit/quad and a specific room (and as seen in section II, 41 out of 43 students surveyed who used passwords for residence access used default passwords).

IV. CURRENT VULNERABILITIES, AND POSSIBLE EXPLOITS/ATTACKS

UBCcard holders seem unaware that there are many assets that are directly and/or indirectly accessible with that card. These assets are open for an attacker to exploit. Below we will outline what kinds of information may be available on a student card and how it would be obtained, what vulnerabilities exist, and how these vulnerabilities can be exploited (i.e. what possible attacks this may lead to).

A. Vulnerabilities

Currently the information printed on the student card is a photo, student number, first and last name, status (i.e. Undergraduate, Graduate, etc.), issue date, expiration date, and the library barcode of the student (a number that is automatically generated during card fabrication).

There is also information stored on the magnetic stripe of the student card. The UBCcard's website says that the information on the magnetic stripe includes name and student/employee number [E9]. An inquiry to the UBC carding office revealed that the card's expiration date is added to the magnetic stripe. They said that this added measure of security is used so that if your card is lost or stolen then this change will differentiate the old card from your new card in the system, and that your old card will no longer be valid.

To obtain publicly available information (without a student card), one may be surprised to find how easy it can be:

1. To obtain a name and student number (which will indicate a date of arrival at UBC which can be used to guess the expiry date of the card by adding 5 years) combination one need not look any further than the boxes of returned tests and assignments in any university building. To obtain a students full name, status, photo, and many other pieces of personal information (i.e. birthday) one does not have to go farther than a few profiling websites, such as Facebook, Hi5, WAYN, etc.

To obtain a student's UBCcard-specific details (student number, issue date, expiration date, and library barcode), either through visual recording or magnetic stripe recording, one must have some sort of physical access to the student's UBCcard. The physical contact condition can be met

through the following attacks:

2. Inside access (i.e. an employee of UBC food services swiping a student card for payment).
3. Friend/acquaintance access (i.e. a friend/acquaintance looking at your student card)
4. Spoofing access (i.e. a person dressed up as building security official asking to check that you are a student during in a UBC building after-hours)
5. Lost and found access (i.e. victim loses their student card and attacker finds it)
6. Theft access (i.e. an attacker pick-pockets you at the PIT).

B. General methods of information transfer (GMIT)

There are many methods to transfer obtainable information (using vulnerabilities as specified above) into an attacker-utilizable form:

1. Read and then write magnetic stripe information: To read the magnetic stripe information onto a card and then copy that information onto another card, all we need is a magnetic card reader/writer and any card with a magnetic stripe that we can write to.
2. Read and then write barcode information: Barcode information can be obtained from a scan or digital photo of the barcode, or by using the barcode number and some open source software to reproduce the barcode..
3. Obtain and then write visible card information (Best Guess): To obtain information on a card and then write guessed card information all we need to do is obtain any publicly accessible information on a student, a copy of a recent student card to use as a template, and a card printing system.
4. Read and then write visible card information (100% visible Replica):
   To read and then write a 100% visible replica of a valid student card all we need to do is get a digital photo of both sides of a student card and then print these images onto a blank card using a card printing system.

C. Exploits/Attacks

Exploit#1: Replay attack with Magnetic Stripe

This attack can come about when an attacker gets access to a student's magnetic stripe information by exploiting any of vulnerabilities 1-6. Once obtaining magnetic stripe information an attacker may use GMIT 1 (from previous seciont B) to gain access to the victims residence (Gage Towers: tower, unit/quad, and room) or GMIT 1 and 3 to usurp the money on a student's meal plan. Please note that since we began this study UBC food services has made it possible for students to check balance and transaction summaries of all expenditures on their meal plans (this information was obtained on November 21st, 2007).

Exploit#2: Replay attack with Barcode

This attack can come about when an attacker gets access to a student's barcode information and student card photo by exploiting any of vulnerabilities 2-4 and 6 (Note that 5 will only work as long as the student card has not already been reported lost/stolen or replaced, as the barcode will be invalidated after this point). Once obtaining the barcode information an attacker may use GMIT 2 and 3 to steal books and laptops from the library.

Exploit#3: Spoofing attack (to obtain new student card)

This attack can come about when an attacker gets access to your name and student number by exploiting any of the vulnerabilities 1-6. Once they obtain this information, they may obtain a new student card from the UBC carding office. The attacker must use this student card quickly though (or during periods of time when a student is less likely to be at the school), as once a student uses their own card they will find out quickly that it has been invalidated by the creation of the new card.

Exploit#4: Inside-skimming attack (UBC food services)

This attack can come about when an employee of UBC food services has access to swipe your card. Swiping a UBCcard for payment at UBC food services does not require that you sign a receipt or enter a pin-code to verify your purchases, therefore there is no way to prove that you actually bought two as opposed to one of any item. With this lack of paper trail, a disgruntled or merely hungry employee could easily swipe your card for 2 or more coffees as opposed to the 1 you bought (using this extra coffee credit to pocket the money on another similar valued transaction or to eat for free) to exploit their privileges.

Exploit#5: Creation attack (creating 100% replica of the student card)

This attack may come about when an attacker gets access to a student's UBCcard, by exploiting any of vulnerabilities 2-4. Note that vulnerabilities 5 or 6 could be utilized as long as the student does not invalidate their card after it is lost or stolen. Once the attacker obtains card information, they may create a new replica of the student's card using GMIT 1, 2, and 4. With this replica an attacker has access to all assets on the student card and the student may still have full functionality of their card.

Exploit#6: Spoofing attack as a result of exploit 1 and 5 (i.e. obtain new VIN card and keys in residences with student card)

This attack can come as a result of exploit 1 (assuming they may swipe the student card) and 5. Once we have the new

student card, one can obtain VIN cards and keys for every residence as long as the person with the card looks somewhat similar to the person on the card. We may also obtain a UPASS for free, solely by presenting the student card to the UBC carding office and convincing them that we did not receive our UPASS in the mail.

V. Methodology

In our analysis of the UBCcard, we undertook a two-pronged approach.

First, we conducted a risk analysis to justify our continued analysis. Once sufficient evidence had been amassed, we decided to probe the security habits of UBC students (the main users of the UBCcard). To do this, we developed a survey on UBCcard usage (helped by interviewing staff from the UBC Carding Office and campus residences). We then distributed our survey both online (via Surveymonkey) and in person. This provided us with raw data on student security habits with respect to the UBCcard.

The second part of analysis was on the UBCcard itself. Our procedure to analyze the UBCcard was to first acquire a magnetic stripe reader. We found that there are quite a few being used on campus, but because of their confidential and proprietary nature we were unable to procure one directly through the university. We ordered a USB magnetic stripe reader easily through eBay. While waiting for it to arrive we procured a parallel port magnetic stripe reader from a fellow student, and created an audio output magnetic stripe reader from an old cassette player. The parallel port magnetic card reader was in non-functional condition, and we were unable to debug the system. Next we tried building the audio output magnetic card reader. This system showed signs of activity, but could not be made usable for magnetic stripe card reading.

The magnetic stripe reader ordered from eBay was held at customs for an unknown period of time before they contacted and interrogated us. It was then redirected to us and arrived more than a month after we had ordered it. It arrived on the day of our mini-conference presentation, and we were able to scan the UBCcards we had collected. We analyzed the data on the cards to determine the format of the magnetic stripe information, and were able to compare this data to the information printed on the cards.

VI. Magstripe Analysis

A. Magstripe Standards

There are four ISO standards that govern the format of magnetic stripes for identification cards: ISO 7811, ISO 7813, and ISO 4909. ISO 7811 defines the magnetic stripe coercivity and the location of the (up to) three magnetic tracks, ISO 7813 specifies the formatting and content of tracks one and two, while ISO 4909 specifies the formatting and content of track three.

According to the ISO standards, the three tracks are as follows:

Track 1 holds 79 alphanumeric 7-bit characters (6 data bits + 1 parity bit), and is located 5.664mm (0.223") from the top edge of the card

Track 2 holds 40 numeric (BCD) 5-bit characters (4 data bits + 1 parity bit), and is located 8.966mm (0.353") from the top edge of the card

Track 3 holds 107 numeric (BCD) 5-bit characters (4 data bits + 1 parity bit), and is located 12.522mm (0.493") from the top edge of the card

All three tracks have a thickness of 2.794mm .

B. The UBCcard Magstripe

In our analysis of the UBCcard, we discovered that the UBCcard did not adhere exactly to the ISO standards in terms of data encoded on the magnetic stripe (as is the case with many of the proprietary-developed security cards). Nevertheless, the contents of the card were easily observable with our card reader. We found that the digital contents included in a student card consisted of a numeric sequence containing the library barcode (minus the checksum value) and the student number. This was contrary to what the UBC carding office and their website told us. We also checked to see what happened when a student card was replaced and found that only the library barcode value on the magnetic stripe was changed.

VII. Building A Magnetic Stripe Factory

A. Cost of reader/writer

Three-track magstripe reader/writers with Serial and USB adapters are available from a variety of sources. For as little as $207.38 one can be delivered to your door from the USA via eBay, with a 45-day warranty.[E1] Retailers sell similar units for as little as $300 with a one-year warranty included. [E2]

B. Cost of blank cards

Blank plastic cards with magnetic stripes are available by mail-order, 500 cards for $78. [E3] Smaller batches can also be purchased, with 100 cards selling for $40. [E4]

C. Cost of card reproduction with graphics

Magnetic cards can be printed for $1.40 - 2.25 each or less in Vancouver, depending on the size of order. [E5] Considering that an insider accomplice will be needed to create these copies this cost may be higher, in the form of hush-money. Another option is purchasing a personal card printer. Models are available which operate with standard Windows printer drivers, and can produce a dual-sided card in 35 seconds at 300 dpi (print magazine quality). These can be shipped to your door within 2 business days for $2895. [E6]

Custom software will also help to forge the cards. The Advanced ID Creator has a free personal edition, and 30-day trials of its software which feature an easy-to-use Windows interface. The professional version, available for $50 once your trial expires, allows you to add barcodes to your design. [E7] Open source barcode software is available free of charge.

VIII. COUNTERMEASURES

Once data is encoded in a magnetic strip and used as an authentication tool, it is a static target for threat agents. Whether it is a vanilla (i.e. no meal plan and no residence access) student card or one that has access to dining plan funds and residence access, precise reproductions can be cheaply recreated. For most uses of the card, UBC staff display a casual attitude toward identity verification, meaning close photo-to-face scrutiny is rarely encountered.

Yet authentication is critical for services on UBC campus, and the trend toward a single authentication point will continue as the psychological acceptability of such a system is high.

To address the security vulnerabilities we have discovered, we propose the following countermeasures:

1) Change UBCcard security features

This can be done by adding an RFID chip. This is already in practice for UBC faculty who prefer to authenticate themselves for building access using their UBCcard instead of carrying around a keychain fob. The RFID chip is harder to replicate, though it is subject to snooping which can lead to replay attacks, as well as overwriting. The use of reading shields and locking the writable area of the card can prevent these attacks. Holograms can be added to the front of the card to make forgery more difficult.

2) Centralize access and authentication methods

By consolidating library and magnetic stripe information into the RFID chip, economy of mechanism can be implemented through a standard campus-wide security verification process.

3) Require a PIN number

When the UBCcard is used for a debit-card like financial transaction, require a PIN card authentication.

4) Force students in residence to change their default password

This will add to defence in depth, providing a thin but important layer of security against access into residences.

5) Encrypt card information

Adding to defence in depth, cardholder information should be encrypted.

6)Create a campus-wide photo verification policy

By training staff and requiring them to verify photo identification, card user authenticity can be more reliably tested. Providing authentication points with terminals that display a photo from UBC records for verification purposes would help to prevent card fraud. Such a system would place UBC employees in a policing role, and raises the question of how to deal with fraud incidents without compromising personal safety of employees. This system would also be costly to implement and would not address machine-verified building access points (i.e. Gage Residences) where a generic white card with copied magnetic data could be presented.

7) Student security awareness campaign

UBC should implement an information campaign to educate students and faculty in utilizing better security habits in the following ways:

- Informing students about vital information that should be protected and the risks associated with information leaks.
- Requiring that Professors prevent anything that links name and student numbers of student from being publicly available (such as term papers and quizzes in hallway). To fulfill this requirement, professors could either require students to include only name or only student number on assignments and quizzes or they can refrain from leaving tests outside doors or in boxes in publicly accessible places.

IX. Summary

The value of a UBC student card and the assets it can access are undervalued by students. We found that students practice poor security habits surrounding the use of their cards, providing them to unauthorized individuals and neglecting to change their default passwords.

We discovered that the magnetic stripe information on the UBC card is unencrypted and subject to a replay attack. Card replication is easy and cheap. A motivated threat agent can cause extensive financial pain, and in the worst of cases personal danger.

As the card's services expand, students face an increasing threat. A more secure form of card would help to reduce the vulnerabilities we have identified. There should also be more adequate protection and authentication policies associated with the card's use. Improved security may not be costly to achieve, as improved security habits of the cardholders may be sufficient to deter a potential attacker.

X. References

[1] Magnetic card reader/writer available from eBay for $207.38 with 45-day warranty. [Online]. Available: http://cgi.ebay.com/Magnetic-Credit-Card-Reader-Writer-Encoder-Hi-Co-TK 123_W0QQitemZ110194392371QQihZ001QQcategoryZ7147 4QQssPageNameZWDVWQQrdZ1QQcmdZViewItem [Accessed: Nov. 21, 2007]

[2]Magnetic card reader/writer available for $300 with one-year warranty. Tyner.com. Nov. 2007. [Online]. Available: http://www.tyner.com/magnetic/msr_card_writer.htm [Accessed: Nov. 10, 2007]

[3] Blank magnetic cards, 500 for $78, [Online]. Available: http://store.idautomation.com/pvc_loco_cards.asp [Accessed: Nov. 21, 2007.]

[4] Blank magnetic cards, 100 cards for $40. [Online]. Available: http://www.kanecal.net/magnetic-cards.htm [Accessed: Nov. 21, 2007].

[5] Plastic card printing in Vancouver for as little as $1.40 per card.
The Duncan Building
403 - 119 Pender Street West
Vancouver, BC, V6B 1S5
604.872.8943
http://www.printprint.ca/pricelist.html

[6] Dual-sided Colour Card Printer for $2895. [Online]. Available: http://www.idautomation.com/printers/Zebra_p120.html#order [Accessed: Nov. 21, 2007].

[7] "Advanced ID Creator software," [Online]. Available: http://www.advancedidcreator.com/software.asp [Accessed Nov, 21, 2007].

[8] "Barcode reproduction and prevention," [Online]. Available: http://www.adams1.com/pub/russadam/faq.html [Accessed Nov. 23, 2007].

[9] "UBC Card: The University of British Columbia's Official Identification Card," [Online]. Available: http://www.ubccard.ubc.ca/Who_is_eligible/Who_is_eligible.html [Accessed Nov. 13, 2007].

[10] L. P. Visdómine, "Track format of magnetic stripe cards," Dec. 12. 2002. [Online]. Available: http://www.gae.ucm.es/~padilla/extrawork/tracks.html [Accessed Oct. 28, 2007].

[11] "Magnetic Stripe Reading," sephail.net, 2005. [Online]. Available: http://www.sephail.net/articles/magstripe/ [Accessed Nov. 15, 2007].

[12] "ISO Magnetic Stripe Card Standards," cyberd.co.uk. [Online]. Available: http://www.cyberd.co.uk/support/technotes/isocards.htm [Accessed: Oct. 28, 2007].

APPENDIX A

Violated Principles of Secure Software Design

- Complete mediation: food services & library personnel not checking photo ID during every transaction
- Psychological acceptability: student card value is not known by students, leading to poor security habits. A majority of residents (___ %) do not know that it is possible to change their room password.
- Defense in depth: UBC food services infrastructure fails to provide defense in depth (i.e. no passwords for buying food). Only one card needed to gain full access to tower, unit/quad, and individual room in gage Residences. Only one card needed to receive: UPass, Building Access Keys/Fobs. Only student number needed to recieve replacement UBCcard.
- Question assumptions: meal plan & dining a la UBCcard lack effective measures against fraudulent purchases.