Analysis and Design of a Smart Card Transit Security System

Timothy D. Kinisky, Michael D.G. Hewitt, Derek Kwei, Colleen Qin

ABSTRACT—TransLink currently has several liabilities in its security policy making it vulnerable to attacks in the form of fraud and fare evasion. Exploitation of the newly celebrated U-pass program may be approached from several levels. The economic implications of these losses significantly impact TransLink's business model. Hence, to drive revenue opportunities while upgrading quality of service, a smart card TransLink system is proposed. Smart cards are by evolution more functionally secure and scalable than magnetic stripe technologies currently utilized by TransLink. They also address other transit challenges such as rate of passenger processing and validation of fare. An implementation of a secure smart card system will both transform a legacy security system and enhance Translink's value proposition to customers.

***Index Terms*— Magnetic stripe, smart card, transit security, U-pass**

I. Introduction

The current transit system in the Greater Vancouver Regional District ("GVRD"), TransLink, operates on magnetic stripe technology. In 2003, the U-Pass system was deployed for students attending the University of British Columbia and Simon Fraser University as a cost-effective method of transportation [1]. However, with this new program, the transit system may be faced with the new threat of previously unforeseen fare evasion as a result of fraudulent U-passes.

II. Current TransLink Vulnerabilities

Historically, the TransLink system has been prone to fare evasion as a consequence of its proof-of-purchase, honour-based system [2]. The introduction of the U-Pass, however, has altered a security landscape. Over the last few years, the U-Pass program, has gained popularity amongst its mandatory enrollees. The magnetic stripe technology used by the program is slow to read, and passenger processing at popular boarding locations such as Broadway/Commercial and UBC terminus is excruciatingly slow. Hence, authenticating the data stored on the magnetic stripe is often ignored, and passengers are able to board busses simply by flashing their U-Pass cards. The bus driver is delegated responsibility of determining whether the small portrait on the U-Pass matches the facial features of the passenger exhibiting it. For the fall academic term of 2005, visual validation has become the only method of authentication as the U-Passes issued by TransLink experienced errors when being read by the magnetic stripe reader. This had assurance implications for both TransLink and Cubic Corp., the U-Pass manufacturer.

A. *U-Pass Visual Inspection Vulnerabilities*

The method of visual transit fare validation is problematic, as it permits passengers many methods of exploiting the system by presenting counterfeit U-Passes. Even individuals who are not technical adept may reproduce U-Passes with minimal effort.

There are two simple approaches an individual may take to replicate the external properties of a U-Pass to circumvent the visual inspection procedure.

1) Novice method of duplicating a fraudulent U-Pass

In the simplest form, to duplicate a fraudulent U-Pass, a practitioner can simply go to a website www.upass.ubc.ca and copy the available U-Pass template. Then, this individual can photograph his/her face against a white wall and paste the picture in the portrait section of the U-Pass template. As a final step, the person adds text to the name field of the U-Pass and prints it on a glossy photo paper.

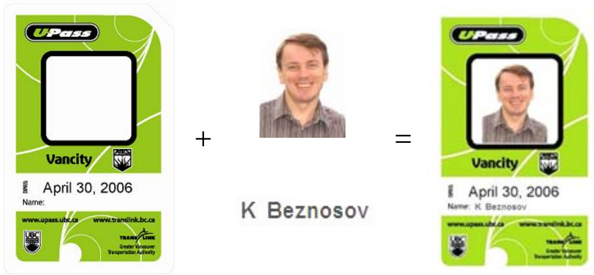


Figure 1: Example of a how to duplicate a fraudulent U-Pass

This method is inherently simple. Upon a casual visual inspection, a fraudulent copy arguably has the capability of being accepted. However, a pass manufactured by the above method is still different from a genuine U-Pass. The most noticeable and distinguishing factor is the text resolution. Because the template on the website is 12.9 KB in size, the resolution associated with the picture is low. Hence, the text printed by the U-Pass is detectable as being slightly blurry. In addition, because the template is from the website, there is no back side to the U-Pass, and this is easily detectable by an inspecting transit official if the back of a fraudulent U-Pass is exposed.

2) Artistic method of duplicating a fraudulent U-Pass

If the individual wishing to produce a fake U-Pass is slightly more technically adept and can engage a graphics program, a more convincing U-Pass can be produced.

As a first step, a real U-Pass must be obtained to scan both the front as well as the back of the card to produce images of higher resolution. The practitioner adjusts the coloring of the U-Pass to match the exact palette scheme and tonal ranges of a genuine U-Pass. Such a process is often accomplished through trial and error. Following this, a picture of the individual coupled with a name inscribed in *Arial 12 pt.* font is added to the U-Pass, similar to the previous method. The newly adjusted front and back images are printed on a semi-plastic piece of material, allowing for reflectivity.

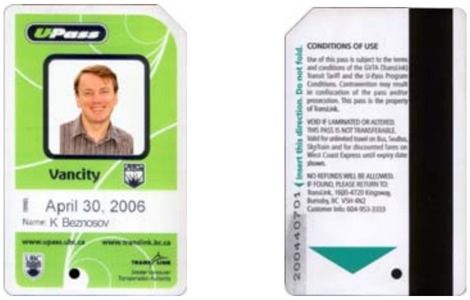

UPass
Vancity
April 30, 2006
Name: K Beznosov
www.upass.ubc.ca
www.translink.bc.ca
TRANSLINK
Greater Vancouver Transportation Authority
CONDITIONS OF USE
Use of this pass is subject to the terms and conditions of the GVTA (TransLink) Transit Tariff and the U-Pass Program Conditions. Contravention may result in confiscation of the pass and/or prosecution. This pass is the property of TransLink.
VOID IF LAMINATED OR ALTERED. THIS PASS IS NOT TRANSFERABLE. Valid for unlimited travel on Bus, SeaBus, SkyTrain and for discounted fares on West Coast Express until expiry date shown.
NO REFUNDS WILL BE ALLOWED. IF FOUND, PLEASE RETURN TO: TransLink, 1600-4720 Kingsway, Burnaby, BC V5H 4N2 Customer Info: 604-953-3333
Insert this direction. Do not fold.
200440701

Figure 2: Duplicating both the front and back side of an U-Pass

This form of producing a fraudulent U-Pass is much more effective at deception. If the exact proportions of the U-Pass are used and the work is printed on plausible material, the visual properties of the U-Pass are enhanced to the effect of the real U-Pass. Yet, the only method of detecting such exploitation would be to feed the card into the reader. If the system only allows valid U-Passes (Cubic Corp. and TransLink will be issuing new U-Passes for 2006 [3]), then this U-Pass is detected as a faulty card.

In addition to these visual vulnerabilities, there are also technological exploitations that can occur for the current U-Pass program.

B. Exploiting the U-Pass Magnetic Stripe Technology

When newly minted U-Passes are to be read by magnetic stripe readers slated for January, 2006 [1], frauds may no longer visually by-pass TransLink fare inspection, especially where there exists a security mechanism to read a stripe. However, because the magnetic stripe technology offers no security mechanism to protecting information (confidentiality) [4], the data on the U-Pass can simply be copied onto a fraudulent U-Pass without being detected. This method can completely bypass all validation steps that TransLink currently has in its security policy. Any magnetic stripe reader will falsely authenticate counterfeit U-Passes.

The magnetic stripe card was first developed and produced by IBM in the 1960's [5]. Little has evolved in the basic mode of operation but as the card's use became widespread, standard bodies have been formed to regulate their use. The main standards are ISO 3554 and ANSIx4 16-1976 [5]. These standards outline the basic dimensions and specifications of the cards. These include number of tracks, density, and encoding format. The standard credit card has three tracks each with differing track density and parsing. Track 1 contains the most data which is encoded in 7-bit ASCII [6]. It often contains a card holder's name, card number, expiry date, PIN, and the name of the banking institution that issued the card. Track 2 is a lower density track which provides support for older card readers and redundancy for newer ones. The track is encoded in 4-bit BCD in an effort to conserve bits thereby limiting the track to digits and control symbols [7]. The relevant information from track 1 is repeated on track 2. This usually is the card number, expiry date, PIN, and the bank's name. Track 3 is the same density as track 1 and is permissibly open to data. Often this 3rd track is used to write transactional information to the card [6].

However the U-Pass, which was designed and manufactured by Cubic Transportation Systems, does not follow any of the aforementioned standards. The magnetic stripe on the card contains only 1 track which is wider than the total width of the three tracks found on a standard card. The magnetic stripe even adheres to a thinner plastic body.

By using a magnetic stripe reader, see figure 3, the contents of track 2 on the U-Pass magnetic stripe can be read.

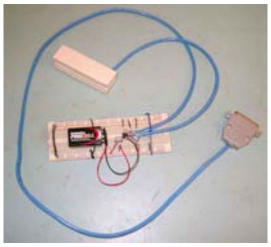
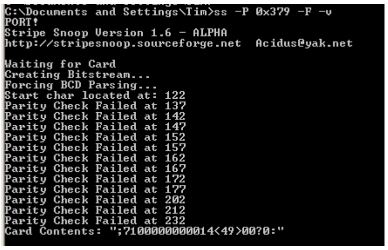


Figure 3: Magnetic Stripe Reader

As seen in figure 4, these contents reveal many parity bit errors, and this is possibly the reason why the stripe reader on the bus cannot read the card.

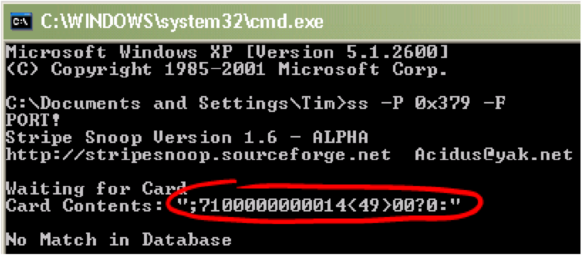


```
C:\Documents and Settings\Tim>ss -P 0x379 -F -v
PORT!
Stripe Snoop Version 1.6 - ALPHA
http://stripesnoop.sourceforge.net  Acidus@yak.net

Waiting for Card
Creating Bitstream...
Forcing BCD Parsing...
Start char located at: 122
Parity Check Failed at 137
Parity Check Failed at 142
Parity Check Failed at 147
Parity Check Failed at 152
Parity Check Failed at 157
Parity Check Failed at 162
Parity Check Failed at 167
Parity Check Failed at 172
Parity Check Failed at 177
Parity Check Failed at 202
Parity Check Failed at 212
Parity Check Failed at 232
Card Contents: ";710000000000014<49>00?0:"
```

Figure 4: Parity Errors found in Track 2 contents of the U-Pass

These errors make it very difficult to analysis the data structure. Yet, even with these errors, it is still simple to determine that every U-Pass is encoded with identical data, including parity errors. Figure 5 displays the binary encoded data that can be read from any U-Pass.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Tim>ss -P 0x379 -F
PORT!
Stripe Snoop Version 1.6 - ALPHA
http://stripesnoop.sourceforge.net  Acidus@yak.net

Waiting for Card
Card Contents: ";710000000000014<49>00?0:"

No Match in Database
```

Figure 5: The data that can be read from every U-Pass

This binary decimal encoded data can be decoded into the following sequence of bits:

```
00000011010111001000000001000010000100001000010000100
00100001000010000100001100000010000111001001001101110
0000100001000010101111111010000000000000
```

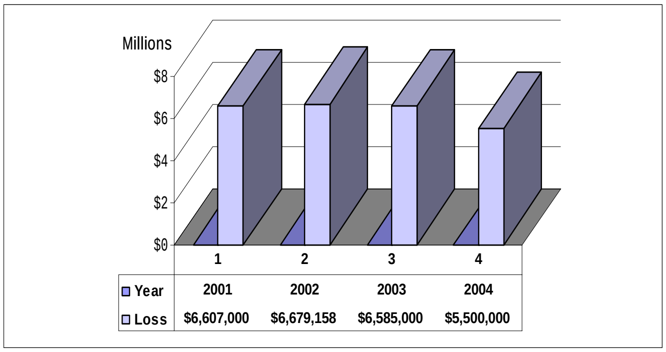
Having the same data on every single U-Pass is a very large security concern. Not only is it now impossible to collect statistical ridership numbers. It is also impossible to monitor for abnormalities that could give information on possible fraudulent copied cards being used. Without any identification marks, even if a known counterfeit was confiscated and subsequently analyzed there would not be discerning features to allow any further investigation. And it would not be possible to monitor or block known forged U-Passes or to track fraudulent cards back to their source.

C. *Economical Implications of Fare Evasion*

Both visual and technological exploitations of the U-Pass system present challenges to the TransLink system to gain the deserved revenue. The economical cost of U-Pass exploitation can be increasingly significant if the methods for producing fraudulent U-Passes become more wide spread as there is no current method of distinguishing magnetic stripe U-Passes that have been copied during the access control decision.

To provide a conservative estimate of how much revenue TransLink is losing, a number of realistic assumptions are made in reference to statistical data. An assumption is made that 1 in 4 persons take Transit and 1 in 1000 persons commit fare evasion. This is a very conservative as the criminal rate of the Greater Vancouver region is much higher than this. There is a strong public perception that fare evasion is linked with criminal activity. The 2002 consensus indicates that there are 545,761 persons in the Greater Vancouver Regional District [8]. With these figures, it can be calculated that there are 136 fraudulent U-Passes produced every year. Seeing that the 1-zone monthly bus pass price (minimum amount that a fare evader would otherwise pay) is $63, the conservative estimate is that TransLink is losing $103,131 annually. However, more realistically, it is often the case that frauds desire to earn money by marketing counterfeit U-Passes to select base. Hence, if only 10 frauds each sell 50 passes a month. At the average rate of $80 per 2-zone pass, TransLink is experiencing another incremental cost of $480,000, resulting in a total annual revenue loss of around $580,000.

Translink operates one of the few transit systems in the world which rely on a proof-of-purchase honour system. On an annual basis, estimated losses due to fair evasion stand roughly to be 3-6% of net revenue [9]. On average TransLink is expected to lose roughly $6 million each year due to absence of fare or freeloading if all potential losses are considered realizable. A slight dip in fare evasion can be seen in 2004, due largely to increases in fare violation penalties and security personnel. Given that only 20% of persons issued violations actually pay [10], TransLink cannot rely on fines as a profitable business model to recoup losses.



▪ Year	2001	2002	2003	2004
□ Loss	$6,607,000	$6,679,158	$6,585,000	$5,500,000

Figure 6: Estimated lost potential revenue due to fare evasion [9] [10]

With increase in the use of U-Passes, no doubt will fare evasion increase. However, with the use of magnetic stripe technology, fare evasion through the copy of magnetic stripe data will be extremely difficult to detect. Hence, it is necessary to find a new solution to address the current vulnerabilities of the TransLink system.

III. Implementing a Smart Card System for TransLink

Smart cards are becoming an increasing popular application, and they are capable of addressing the current vulnerabilities experienced by the current TransLink system. With their ease of use, security features, and customizable functionality, smart cards can enable the TransLink system to be fast in processing passengers as well as reduce fare evasion that is caused by fraudulent U-Passes.

A. *Smart Card Technology*

A smart card is essentially memory and a CPU. The major difference between magnetic stripe systems and smart card systems is the CPU. This CPU is what determines access control to different memory locations. In addition, the CPU can be a cryptographic processor ensuring data confidentiality is kept.

B. *The Smart Card Solution*

A smart card system has many benefits over the magnetic stripe system; faster to read, extremely hard to replicate, allows for more security mechanisms to be employed, more memory, additional types of memory, and even ability to control access to different parts of memory.

In addition, the memory capabilities on the smart card allows for storing temporary transit data for TransLink to use and analyze as well as for the busses and transit authorities to manage the zone changeovers.

For the TransLink user, the main benefit is ease of use and reliability. What TransLink gains are user statistics, faster throughput on busses, reduced incidences of fair evasion and an advanced system ready to be integrated into other industries.

C. *Smart Card Security Principles*

There are 10 fundamental security principles and the smart card solution makes use of them all.

1. Least Privilege

The fact that a smart card has the ability to build in access controls allows one to control the flow of information. For example, using an RBAC system, the definition of the card owner could be a read only definition, whereas the definition of reader could be read/write to certain parts of the card, read only to other parts and no access to other parts.

2. Fail-Safe Defaults

Mechanisms such as detect and destroy circuitry ensure that if the card is compromised, all access is prevented.

Originally pay TV smart cards worked in reverse; everyone had access to every channel, and channels were blocked accordingly. By placing something between the reader and the card, one can circumvent the system. [2] Fortunately this was easily fixed by applying this principle.

3. Economy of Mechanism

Using past proven standards to implement security means less bugs and issues and provides resources to analyze problems that do occur. Making the process modular will allow each block to be tested individually and make testing simpler. Since the information is stored mainly on the card very little system data synchronization or checking is needed.

4. Complete Mediation

This principle is based on how the system is implemented. For obvious reasons, is better if for any access of the card and its materials, that a pin or some other security mechanism is checked for validity. Many are based on the protocols used.

5. Open Design

The fact that the smart card can be physically obtained by anyone makes the design open. Protocols are desirably standard and encryption algorithms are well known. There is some secrecy in that if one uncovers the layout of the chip, it becomes easier to attack. Thus convoluting the layout by adding abstraction defeats this design principle.

6. Separation of Privilege

In the proposed smart card system, both the smart card reader and the bus driver must be utilized for the user to be granted access to the bus. The passenger requires the driver's permission and a valid smart card. The reader could even give some basic information such as gender and age class to help the driver identify and authenticate the passenger.

Since the card memory can be broken up in any way the designer desires, if this solutions is scaled to involve other uses, such as merchandise sales, possibly separate access rights, privileges and security mechanisms would have to be in place to ensure the system remains secure. For example, if the government has a certain hash used to unlock the ability to write to a certain part of memory, the same hash cannot unlock another part of memory it should not possess access to.

7. Least Common Mechanism

Similarly, this is addressed through controlling access to different areas of memory.

The transmission of data must travel through air as a medium, therefore the channel cannot be completely covert but the pattern of information can be varied and encrypted to confuse a potential attacker. The bus itself does not store any specific user data. Instead the smart card will store everything associated with the physical person. The most vulnerable transfer mechanism is likely one online between the card and the user's host.

One other transfer vulnerability is in the card reader. The card must be sandboxed so that it cannot pass any malware to the reader to produce ill effects, which may corrupt future reads.

8. Psychological Acceptability

Smart cards are designed to deliver ease of use to a complex, time consuming process. This is especially the case when considering the current system which is a labour intensive activity.

Building public trust in smart cards could be tricky. An average user may be skeptical of new technologies which try to converge too much confidential information into one location. This is analogous to a central database. The difference being that substantial information is not likely to be stored on this device; rather it represents a major inconvenience and recovery issue if this central card happens to get lost.

9. Defense in Depth

Many techniques such as encryption, hidden protocols, authentication, salting and key management are employed to provide layers of defense to software attacks while detect and destroy circuitry, randomization and other physical circuitry provide layers of physical defense.

10. Question Assumptions

A scheduled maintenance analysis should be run to continue development and reassess the security issues to improve the system. If the card is scaled up for usage as, say a debit card in addition to transit card. All assumptions about the transit card will have to be revisited to ensure that they are still valid and if not, changed.

There is a conflict with Open Design and Defense in Depth and Least Common Mechanism. The idea is to use a secret ordering of data transmission or protocol as a layered or additional defense means that this secret cannot be openly known. Although if this information is leaked the system remains secure but looses this extra protection layer.

There can be a conflict between Psychological Acceptability and Separation of Privilege. The reason for this is mainly in the user name and password phase. For security a randomly generated key or pin may be used over a user defined password but this makes it cumbersome to remember. In addition, if biometrics are used as a security measure (or layer), people may object to having their bio-information such as fingerprints or DNA on file.

Synergy occurs between the Economy of Mechanism and Psychological Acceptability because Economy of Mechanism is based on simple and systems and simple systems are more usable and thus more Psychologically Acceptable.

The principles of least privilege and complete mediation are synergistic in that each time authentication must be given to access something. This means that each time the smart card is used, you start out with no privileges and you apply to gain privilege, and thus need to be re authenticated.

The principle of psychological acceptability has synergy with defense of depth because as the public sees that there are many layers of security their trust grows.

D. Attacks

Attacks on smart cards can occur in two broad categories; invasive and non-invasive., the latter being more practical for the average attacker.

In brief, invasive attacks involve physically dismantling the processor to view and access logic. Accessing this logic allows an attacker to by-pass security measures and obtain data from the chip.

At cheapest, invasive attacks cost tens of thousands of dollars [11]. This implies methods for the average attacker are economically infeasible if one seeks only to gain a few dollars worth of transit fare.

Smart cards are particularly vulnerable to these because the attacker has complete control of the power and clock supply lines and, unlike invasive attacks, can be done at reasonable costs.

Essentially there are three types of non-invasive attacks: software, eavesdropping and fault generation.

Software attacks are attacks on the cryptography and transfer protocols used on the chip and between the reader/writer and the card. Generally the crytoprocessor and ciphers are DES/tripleDES or AES. The more secure the data required the more secure the algorithm must be to protect this data. As a point of interest, it should be noted that DES is easily cracked, however 3DES has never been cracked and neither has AES, while AES is starting to replace 3DES in most applications.

Eavesdropping attacks are based on having physical access to the read/write infrastructure. If smart cards become ubiquitous and appear in web applications and other distributed systems, this type of attack will become more eminent. However, this is not a concern for transit as the card is only in contact with a bus reader or a filling station; both places would be very difficult to eavesdrop upon.

Fault generation attacks rely on changing voltage and clock signals to the processor. As an example, the data stored in EEPROM can be erased via modified voltage signal. Also, by increasing the clock frequency for a brief time can cause flip flops to trigger and read data before the new state is supposed to occur [11]. Essentially the system is driven from a secure state to an insecure state.

Fault generation attacks such as differential power analysis can also extract an encryption key from a smart card by statistically analyzing the difference in power delivery to areas of the processor. In addition, different power levels are used for 1s and 0s meaning that it is possible to detect when a 1 or 0 is used.

Indeed, invasive and fault-generation attacks are the Achilles heel of smart cards. However, there are solutions:

1. Technological advancement

As technology advances, smart cards become harder to attack. Smaller chips require the attacker to use more advanced and expensive machinery for invasive attacks. Power fluctuations are harder to produce due to sensitive detection circuits. Differential power analysis attacks are made increasingly difficult as normal supply fluctuations are difficult to distinguish from real signals within the processor.

Obviously, as chip fabrication technology becomes better, so does chip attack technology, however this is not a significant problem as the cost for such equipment is rather high and extremely traceable.

2. Detection and Destruction Circuitry

This type of circuitry, such as a sensor mesh, can detect an attacker tampering with the physical layout of the circuit. If an attack is sensed, a fuse will blow, disabling access to certain areas of the chip. As an example, sensor meshes are active while there is power to the chip. If a short or other fault is detected when the chip is powered, the destruction fuses are blown and access is disabled [11].

Not surprisingly, attackers do have a countermeasure for this. They can stitch the fuses with microprobes.

3. Clock-Randomization

Making a process non-deterministic plays a key role in the physical security of a smart card. Randomization of clock frequency prevents triggering flip-flops into non-secure states.

E. Implementation Cost to TransLink

TransLink being the largest coin handling agency in British Columbia should view Smart cards as an enhancement to customer convenience as well as to their own security mechanisms.

It is public perception that links fare evasion with criminal activity. If Smart cards help negate forms of fare evasion and fraud then it is TransLink's mandate to improve quality of service, which in turn generates ridership.

Comparison between turnstiles vs. increasing staff to negate fare evasion

NPV-all figures relative to Base Case

	Full Gates	*Full POP*
Cost-Labour	$58.4	$187.6
Cost-Capital	$46.7	$0.1
Costs-Total	$105.1	$187.7
Revenue Gain-Security	$13.2	$13.2
Revenue Gain-Fare Compliance	$40.8	$40.8
Revenue Gain-Total	$54.0	$54.0
Net Revenue Gain	-$51.1	-$133.7

Turnstiles have already been considered by TransLink but have been ruled out after several economic and cost-benefit analyses. In table above, two security mechanisms are compared: the first is the installation of 37 gated turnstiles at all 26 sky train stations [12] ("Full Gates"), the second involves increasing personnel configuration at each station until the same level of fare compliance is reached ("POP" or Proof-of-Purchase). The Base Case represents the status quo. Revenue Gain-Security is a result of increased ridership from a generated sense of safety. All figures are extrapolated to a net present value using a cost of capital of 5% over a twenty year period [13]

Naturally, security projects of higher capital cost often result in higher operational & maintenance expenditures as well. Turnstiles as a consequence are not feasible given a capital cost of $47 million and operating costs exceeding $1.2 million. These costs do not deliver a reasonable return-on-investment (ROI) if even all potential revenues lost by fare evasion are realized. In addition due to the narrow funneling caused by turnstiles, the dangers of queuing subjects and placing them in harm's way prior to an access control decision remains an architectural and even legal problem.

According to Kennan Kitosaka, a UBC civil engineering graduate and manager of TransLink ITS, reducing *dwell time* or the amount of time a transit coach spends at a stop grants substantial cost savings. Smart cards, given their relatively quick validation, offer a means of expediting boarding. Furthermore contactless smart cards can be debited if only within several feet of a reader, offering perpetual effusion through points of entry rather than a stop-and-go reference monitor. For the 99 B-line, a celebrated coach which bears many students to campus each fall, reducing dwell time by 45 minutes allows cost reduction of $650,000 per year while upholding level of service. [12] Linear arithmetic indicates removing four buses per day results in a savings of $2.5 million. Such operational research is seen to offset potential revenue losses attributable to fare evasion.

However, fare evasion may need to be redefined. The present may foretell a sea change in fraudulent attacks against TransLink. Already TransLink's current security policy can be breached by electronically cloning proof-of-payment receipts or by *burning*, the act of reusing one fare by multiple persons. This redefinition constitutes a larger scope of fare evasion than estimated in previous years.

Kitosaka estimates for a Smart card program to be successfully implemented and assured could cost between $30 to $40 million [14]. Intuitively, a Smart card program is cheaper to maintain than installed physical gating. It also assures against future threats stemming from more creative and advanced forms of fare evasion. From a marketing perspective, the value-add of paperless authentication forms a basis for customer loyalty programs. By using accountability best practices, including monitoring and auditing traffic, statistics can be leveraged to provide discounts to encourage boarding at desired Skytrain stations and bus stops.

At present, TransLink is undertaking a Smart card initiative which is at an “internal benefits analysis” stage investigating how easily it can be integrated across functional units within the organization in terms of business process and usability. The next step pending is to build a business case and open a request for proposal aimed at Smart card vendors.

IV. Conclusion

Using smart cards as a solution for the problems that TransLink is currently experiencing with the magnetic stripe U-Passes and fare tickets is a viable solution that would not only enhance security but also prove to be useable and scalable in future applications.

References

[1] www.upass.ubc.ca

[2] Options to Improve SkyTrain Passenger Safety & Security and Reduce Fare Evasion by Edwin Blewett & Associates Inc.

[3] www.translink.bc.ca

[4] http://www.mtc.ca.gov/services/TransLink/

[5] http://stripesnoop.sourceforge.net/

[6] http://history.sandiego.edu/gen/recording/magnetic4.html

[7] http://www.bookrags.com/sciences/computerscience/magnetic-stripe-cards-csci-03.html

[8] http://www.city.vancouver.bc.ca/commsvcs/cityplans/CityFactsv2.PDF

[9] TransLink 2003 Annual Report

[10] Options to Improve SkyTrain Passenger Safety & Security and Reduce Fare Evasion by Edwin Blewett & Associates Inc.

[11] Interview with Kennan Kitosaka, Manager, TransLink ITS

[12] Brenda Jones, Media Relations Manager, TransLink

[13] KPMG Forensic Report

[14] O. Kommerling and M. G. Kuhn, Design principles for tamper-resistant smartcard processors, Proceedings of USENIX Workshop on Smartcard Technology, 1999

[15] R. Anderson. Security Engineering: A Guide to Building Dependable Systems pg. 290-99, Wiley 2001