Risk Analysis of MacLeod and Kaiser Buildings

I. Fakinlede, A. Gagné, R. (Kin Wai) Lo, G. Tu, *Students, EECE 412*

***Abstract* - The objective of this project is to carry out a thorough analysis of the EECE department's buildings: MacLeod and Fred Kaiser. Our goal is to investigate the vulnerabilities of the current security system installed and provide suggestions. We have achieved this by first doing a risk analysis of the building then we evaluated the effectiveness of the security measures employed in the department based on the combined findings from the risk analysis and low-level attacks.**

***Index Terms* – Security, Risk analysis, Performance Evaluation, Radio Frequency Identification System**

I. Introduction

The MacLeod and Kaiser buildings are the home of the Electrical and Computer Engineering department. The MacLeod building comprises of 4 floors while the Kaiser building is made up of 5 floors. The floors in both buildings contain labs and classrooms full of equipment for teaching and research as well as offices which contain student records, administrative records, personal information and assets belonging to the teaching staff.

This project has afforded us the means to practice the skills and concepts learned in EECE 412: Computer Security. Our analysis involves a high and low level analysis of the security of the two buildings. The high-level analysis includes an investigation of the assets and possible threats to the security system already employed to protect the assets. The low-level analysis has been carried out by actual attempts to breach the current security system and gain unauthorized access into the building, labs, classrooms, or even computer accounts.

This report is divided into the following sections:

Risk Analysis: This includes the high level investigation of the assets in the building, the potential threats and the risk of their occurring.

Security Mechanisms: This includes a brief technical analysis of the currently installed security system and the possible types of attacks associated with each different mechanism.

Evaluation and Attack Scenarios: Includes a description of the human issues involved in the current implementation of the security system.

Conclusion and Suggestions: Finally we provide suggestions for tightening up the current security system as well as further work that can be done in security analysis of the buildings.

II. Risk Analysis

Risk Analysis is not an easy task to carry out; most systems are complex and the entities to consider are diverse. It is also hard to analyze the value of assets taking everything into consideration. This difficulty was further compounded by the department staff's reticence in giving out information of any sort once the term "security" was used. We were more successful when we disguised our questions, first by removing any reference to security and by affecting nonchalance.

TABLE I
VALUATION OF ASSETS

ASSET	EXAMPLE	ESTIMATED PRESENT VALUE	ASSOCIATED SECURITY SERVICES/ POLICIES Confidentiality Integrity Availability
Lab Equipment (Electrical and Mechanical)	Measuring devices, cutting tools	$1000 per equipment	Availability
Computers	Software	$100 per software	Confidentiality: UBC policy #104 and # 85 Users are prohibited from accessing other users' computer IDs or accounts and communications, without specific prior authorization from the appropriate administrative head of unit.
	ECE website		
	Z drives		
	Hardware	$1200 per computer	Integrity and Availability
Classroom Hardware	Chairs and desks	$400 per set	Availability
	Teaching equipment	$1200 per equipment set	
	Fixings e.g. clock	$100	

Services	E.g. Washrooms facilities	$300	Availability
Student/ Administration Information	Student records	$0.01	Confidentiality and Availability: UBC policy #106 Ensure the confidentiality, availability and integrity of Administrative Systems and Administrative Data and to reduce the risk of loss whether by accidental or intentional modification or destruction
Staff Personal Effects	Staff's document, computer	$2000 per room	Confidentiality
Student Personal Property	Textbooks and laptop	$400 per person	Confidentiality
Safety (students and staff)			Availability: UBC policy #7 The University aims to provide a safe, healthy and secure environment in which to carry on the University's affairs.

TABLE II
IDENTIFICATION OF THREATS

ASSETS	THREATS	THREAT AGENTS	THREAT TYPES	VIOLATED POLICY
Lab Equipment, Hardware and Supplies	Theft	Malicious person with access	Usurpation	Availability
	Loss	Careless user	Disruption	Availability
	Damage by user	Incompetent user or staff	Disruption	Availability
		Careless user	Disruption	Availability
		Malicious user	Disruption	Availability
	Damage by non-human means	Unstable power apply	Disruption	Availability
		Aging	Disruption	Availability
Software and Computer Data	Corruption	Malware	Disruption	Availability
	Theft of information	Spies	Disclosure	Confidentiality
	Unauthorized coping of data or software	Spies	Disclosure	Confidentiality
	Theft of files	Spies	Usurpation	Confidentiality
	Loss of files	Software engineer (faulty design)	Disclosure	Availability
		System overload	Disclosure	Availability
		Deficiencies in operating system (i.e. Microsoft Windows)	Disclosure	Availability
Staff Offices	Access by unauthorized person	Student or other staff	Usurpation	Availability
	Theft of personal properties	Malicious person	Usurpation	Availability
Student Lockers	Theft of personal properties	Malicious person	Usurpation	Availability
Services	Theft	Malicious person	Disruption	Availability
Intellectual Property	Theft	IP thief	Usurpation	Confidentiality
	Destruction of research	IP thief	Disruption	Availability
	Destruction of research hardware	IP thief	Disruption	Availability
Student Items	Theft of items during exams	Student thief	Usurpation	Availability

III. Security Mechanisms

This section includes a brief technical analysis of the currently installed security system and the possible types of attacks associated with each different mechanism.

A. Radio Frequency Identification System

The Radio Frequency Identification (RFID) Security system used in EECE buildings is the iClass 13.56 MHz Contactless Smart Key fobs base Model Number 2051 designed and marketed by HID Corp. [7]. The locks employed on the EECE buildings are the three-sided abloy keys. These keys come in units of 5000 keys each key in the unit costing $500 [3]. Therefore if a master key gets lost it will cost the department about half a million to replace. Rather than giving students these keys, the department uses keypads for access control. At the beginning of every term, key combination are generated and assigned to the students registered in

EECE course. However these key codes need to be reprogrammed on the each keypad and the codes can easily be compromised through shoulder surfing. The RFID has proven to be a more effective solution both for security and cost. Like the standard RFID system, the iClass front end is comprised of a tag and a reader. The RFID stations are installed most of the doors leading into both buildings, on all doors leading to each floor and the store on the first floor of MacLeod, and administrative offices, postgraduate and research labs in Kaiser building. The system grants authorization based on Role Based Access Control (RBAC) System.

1) Threat Analysis: The front-end attacks that first come to mind when talking about a radio frequency based technologies are sniffing, replay, spoofing and denial of service attacks. In the iClass, HID has designed an RFID system that reduces the risk of such attacks through an encrypted mutual authentication process and collision detection [7]. However the effectiveness of such features depends on how the system is administered. The following vulnerabilities still exist.

--Social Engineering: Without human surveillance insiders compromise the system through complacency and negligence. We found methods for gaining entry such as tailing and tagging to be effective in the MacLeod Building.

--Usability: It costs about $3000 per RFID station [3]. In order to save money the department has installed only one station per room for most rooms. Since several rooms in the Kaiser building have two doors, one of the doors (usually the back door) is accessed with an abloy key. As it happens these back doors are more convenient for accessing washrooms and other offices. Therefore, they are often left propped open to provide easy access.

--Design Vulnerability: Mutual authentication between reader and tag is based on the *ISO 9798-2* standard, in which both participants in the communication check the other party's knowledge of a secret encrypted key [2]. Each tag is secured with its own unique key based on its Serial number using an encryption algorithm and a standard master key K_M. Every reader has this master key and the encryption algorithm. Therefore during an authentication process the reader calls for the tag's serial number and uses it to derive the secret key, which is used for further communication. The same K_M exists on all HID readers. HID appears to place more emphasis on keeping the encryption algorithm secret while the key is more easily accessible. With access to this key the following attacks can be performed:

--Cryptanalysis to discover the algorithm: With unlimited access to a reader and a tag, signal analysis can be performed on mutual authentication process to discover the encryption algorithm. This will involve the use of a skimmer/spectrum analyser and signal processing tools such as matlab [6].

--Man-in-the-middle attacks: An interesting attack we found was to build two devices that would communicate with one another over a low latency link and with a key fob and reader. Using these devices one could effectively extend the range of the RFID system from the standard 3cm to upwards of 50m [9].

2) Countermeasures: --Fob protection: To prevent man-in-middle attacks, key fobs should be rendered unreadable while not in use using blocker tags and faraday casing.

--More secure keys: HID now provides the ability for administrators of the iClass system to create their own keys rather than rely on the standard K_M. Adopting this security feature will greatly enhance the security provided by the RFID system [7].

--Double access control: This method controls access both into and out of the building. Therefore the backend system of the RFID keeps track of everyone in the building. This prevents man-in-the-middle attacks, because it prevents attackers from reusing the tags of somebody inside the building. If the attacker is able to use the tag of somebody not in the building then when owner tries to gain access the computer will also deny the owner access. However the owner will be able to lodge a complaint. That tag can be disabled and the attacker will not be able to leave the building without turning him/herself in to security. This will also hinder insiders from easily letting unauthorized persons in. To let someone in a person would have to let themselves out and then re-access the building. This method can also be used in investigating crime because the computer will know who was where, when and for how long.

B. Keypad

Keypads are currently used to protect the student labs and computer labs in the MacLeod and Kaiser buildings. The keypad lock can be unlocked by entering the corresponding 4-digit key code. If a malicious outsider can obtain the key code, he/she then will be able to get a hold onto the valuable lab and computer equipment of the EECE department.

1) Threat Analysis: The simplest way to enter a space protected by a keypad door lock is to enter the correct key code. The key code can be somehow easily obtained through social engineering and shoulder surfing. Furthermore, with certain knowledge, it has been found that each keypad unit can be individually reprogrammed since there is no central system managing them. Lastly, the doors are susceptible to physical sabotage by authorized users leaving the doors propped open.

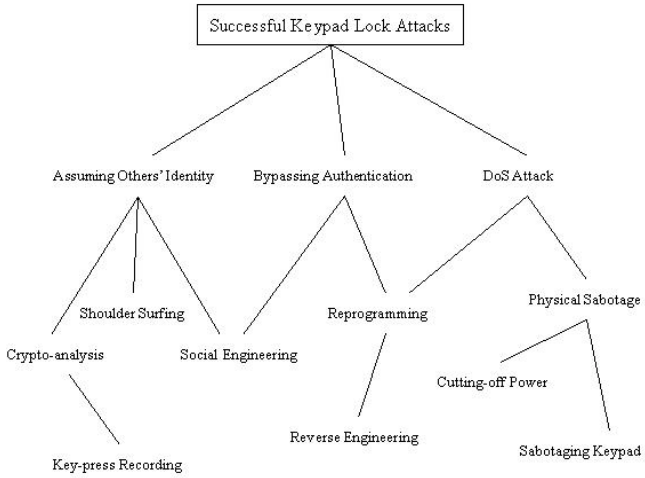

Fig. 1 – Keypad Attack Threat Tree

2) Countermeasure: The EECE department can post signs on the doors installed with keypad system reminding authorized people to protect their confidential key code from leaking out or not to open the door for unknown outsiders to get into the room. More importantly is to change all keypad mechanisms to the more secure RFID fob system.

C. Lock and key

Abloy Lock and keys are used for all doors rooms in the MacLeod and Kaiser building. These cylindrical keys are difficult to break and expensive to copy (about $200 per key) [3].

D. Computer Accounts Password

Each EECE staff or student has one EECE account, which contains his or her important data or work. Therefore, the protection of the EECE account is very important. The only accessing protection of the account is the user ID and password. Attacking the password can reveal all the secrets in each EECE account.

1) Threat Analysis: The easiest way to steal a user's password is to do shoulder surfing. To accomplish this, an attacker would simply memorize the password as they watched a user inputting it. Another way is to use keylogging to record what passwords users type. Keyloggers can be physical devices that are plugged in between the keyboard and the computer that would appear invisible to the user. Student accounts are also vulnerable to other students. Every authenticated user has access to other user's accounts.

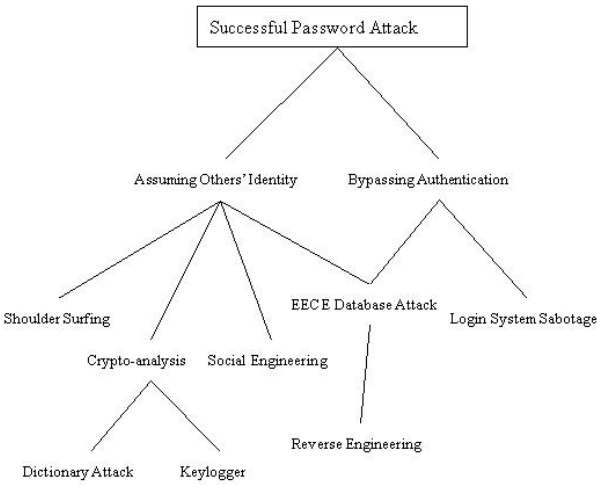

Fig. 2 – Password Attack Threat Tree

2) Countermeasures:

--The EECE department can replace the current computer cages with cages that completely cover the computer, which will prevent the installation of keyloggers.

--In addition, the EECE department should set all students' initial passwords to some random passwords.

--Informing users on the risks cannot be underestimated. If students were aware of the fact that people can access their accounts by default and were also informed of the facilities available to protect themselves.

--Set the default permissions on accounts to deny access rather than allow it. This would, of course, limit the amount of access regular operators have to student accounts. Restricting operators from accessing student data is a functional separation of duties.

--Allow users to change their passwords. This would allow students to increase the security to their account on their own discretion.

IV. Evaluation and Attack Scenarios

This section includes a description on the human issues involved in the implementation of a security system, a review of how well the current security measures mitigate the security threats, and some simple attack scenarios we have conducted.

A. Department Administration's Perspective on Security

UBC has three policies that the department is obligated to consider when making security decisions. These are:
Policy #7 – Availability of Safety
Policy #85 – Intellectual Integrity
Policy #104 – Confidentiality of computer accounts
Policy #106 – Confidentiality, Integrity and Availability of Administrative Records for students and staff [13].
In addition there exists a Risk and Management Section in UBC Treasury whose mandate is to minimize the economic impact on the University from loss or damage to its physical assets and from third party allegations of liability through the assistance of employees and risk financing.

While department has been keen on up holding policy #106 with tight firewalls, they have less careful in protecting physical assets and student computer accounts. The main reason behind their negligence on security we later discovered is because the UBC has spent a large sum of money on insurance. The department administrators probably felt the only loss was in time to replace given that they have insurance covering everything in the department buildings. Insurance, though proven to be a sound investment area in some cases, does not solve all problems. The lack of interest and knowledge in the importance of security along with the over-reliance on the insurance coverage has potentially devastating consequences of which we will discuss in scenario 2.

B. Student's Perspective on Security

Like the department administration's loose attitude toward security, according to the observation, most students of the EECE department are not concerned with security either. The lack of security awareness greatly undermines the effectiveness of installed security mechanisms. For example, the inconvenience caused by the key fob system installed at the building entrances has fostered a sense of community in the students such that they will help one another bypass this system by opening, or keeping open the door, for one another. It has been widely known and often observed that for one hoping to enter the buildings, all he/she has to do is simply knock. In this case, the existence of the entrance key fob system becomes more or less pointless.

C. Attack Scenarios

In this section, two attack scenarios are formulated to demonstrate the inadequacy of the current security mechanisms and measures employed with the EECE department.

Scenario 1: The Thief

This scenario will outline how an attacker without any prior access to the building can get in and steal an item of value from one of the classrooms.

The classrooms are located on many of the upper floors of the MacLeod buildings. Often times they are open late, 6-7pm, on the weekdays. What an attacker could do is first gain access to Kaiser. From there they would have access to the first floor of Kaiser. They can then either get to the second floor of Kaiser or the first floor of MacLeod.

The second floor is easily reached by going up the main stairs; from there they can attempt to access the second floor of MacLeod or the higher floors of Kaiser. The higher floors would be difficult as the stairwell becomes locked at roughly 6pm. They may be able to bypass that on the kindness of insiders as well, although they would hopefully have to be more skilled at it than simply wait around at the door for someone. The higher floors of Kaiser are dedicated entirely to research so one would hope that people would be more reluctant to let someone into one of the floors; but people can easily rationalize (explain) why someone would be doing that. From the higher levels of Kaiser the doors then open *into* MacLeod allowing one to easily get in without an alarm going off. From there they would be in MacLeod.

Once in MacLeod the route to the classroom would depend on which floor the attacker was coming in from. If they were not on the floor of the classroom they could take the northwest stairwell. The doors in this stairwell do not close entirely by themselves. The doors do sound an alarm if opened but rarely will students react to it, again the ability of people to rationalize is at work. From there the attacker needs only gain access to the classrooms. At 6-7pm the classrooms are all open and people may or may not be in them. To leave the building just about every way leads to an exit and there is nothing preventing people from leaving the building. The trickiest part about all of this is the cleaning staff. The cleaning staff will take notice if someone is removing items from the room where they are cleaning.

If this attack were successful then it would result in a Denial of Service attack. The insurance that is taken out on the items in the classrooms would pay for the item itself but if it were important (a projector or a screen) then the classroom itself would be rendered partially unusable for the time it would take to replace the item. This would affect the quality of teaching.

Scenario 2: The Malicious Student

This scenario will outline how a student can bypass the security features of the department to simulate an act of plagiarism between two other students/groups.

First off the attacker would need the usernames of the targets. There are several ways that the attack could gain this. If the attacker were in a class with their

targets they would have access to their names. As the EECE undergrad accounts are usually the first letter of your first name combined with your last name it wouldn't be that difficult to guess at someone's account.

The attacker would then need the password to one of the target's accounts. The undergrad account passwords are usually a student's student number. Students are often required to write their student numbers on their quizzes or written assignments. It wouldn't take much for an attacker to record the student number of one of their attackers. They could also gain access to the password by installing a keylogger on the machines in the undergraduate student lab.

Once the attacker has both the username and the password it's a simple process of waiting for the perfect opportunity. Such an opportunity would be the day before an assignment is due. The attacker would log into the system as one of their targets, navigate to the home folder of their other target, copy the assignment files, and then place code/text from the copied assignment into the assignment of the first target. If the code is functionally equivalent then a simple run through test wouldn't reveal anything. The key point is that this attack would have to happen close enough to the due date that the first target would not notice and yet not so close that they would've already turned it in. The modified assignment has to be the version that the professor sees. With this accomplished the attacker has just forged academic misconduct as defined in the UBC Student Calendar [11].

The possible repercussions of academic misconduct range from a 0 on the assignment to being expelled from UBC [12]; this includes both those who copied and those who supplied the material. The amazing thing about this attack is that it's so incredibly easy given the current setup of the EECE system. Students and academic professionals do not take the necessary steps to protect what are considered special resources such as student numbers and the access control on the undergraduate machines are open by default. Students are not trained on how to use Unix and students cannot change their passwords via the command line.

V. Conclusion and Suggestions

After the survey and analysis, one conclusion can be drawn which is that based on the security policies the University has set up as guidelines, the amount of security provided to the MacLeod and Kaiser buildings is lax. The reason for this is that there aren't enough recorded cases of reaches of security and also the physical assets have been insured. However the lack of records isn't due to the lack of cases but the lack of an official way of reporting and recording such cases.

The RFID system that is currently used for access control is quite secure for the amount of security required for the buildings. However its ineffectiveness is due to the way it is administrated and the complacency and negligence of insiders. The RFID itself could do with more improvements however the kind of security breaches that can be carried out by exploiting its vulnerabilities is quite expensive and not very viable as there are easier way of gaining unauthorized access. However for higher security application the countermeasures we mentioned such as the Fob Protection and Double access control system will be very effective. However these countermeasures have the disadvantage of reducing the usability of the system therefore more work needs to be done to make these countermeasures more usable.

For student accounts, at the present there is nothing to protect one student's account from other students. According to the University policy #104 the department is obligated to do more to make them more secure.

VI. References

[1] M. Bhuptani, S. Moradpour, *RFID field guide* (Book Style) Upper Saddle River, NJ: Sun Microsystems/Prentice Hall PTR, 2005

[2] K. Finkenzeller, *RFID Handbook* (Book Style) Chichester, England ; Hoboken, N.J: Wiley, 2003

[3] L. Filipozzi, D. Dawson, D. Chuchung D, E. Russell, A. Vlassov, Personal Interview. February/March 2007.

[4] I. Kirschenbaum, A. Wool. (2006, May 8) *How to Build a Low-Cost, Extended-Range RFID Skimmer*. [Online]. Available: http://www.eng.tau.ac.il/~yash

[5] S. Shepard, *Radio Frequency identification* (Book Style) New York : McGraw-Hill, 2005

[6] I. Kirschenbaum, A. Wool. (2006, May 8) How to Build a Low-Cost, Extended-Range RFID Skimmer. [Online]. Available: http://www.eng.tau.ac.il/~yash/

[7] *iCLASS™ Serial Protocol Interface,* HID Corp., [Online]. Available: http://www.hidcorp.com

[8] *ISO 14443-B*, AMTEL Corportation [Online]. Available: http://www.atmel.com/dyn/resources/prod_documents/doc2056.pdf

[9] G. Hancke, *A Practical Relay Attack on ISO 14443 Proximity cards.* http://www.cl.cam.ac.uk/~gh275/relay.pdf

[10] HID, *Application Note (Preliminary)* http://www.hidcorp.com/pdfs/appnote_28.pdf

[11] University of British Columbia, *Academic Misconduct*. Academic Calendar, Section V.3. http://www.students.ubc.ca/calendar/index.cfm?tree=3,54,111,959

[12] University of British Columbia, *Disciplinary Measures*. Academic Calendar, Section V.3. http://www.students.ubc.ca/calendar/index.cfm?tree=3,54,111,960

[13] Board of Governors Policies, Procedures & Guidelines, UBC. [Online]. Available: http://www.universitycounsel.ubc.ca