Sri Lanka Institute of Information Technology

IE2052 - Advanced Networking Technologies

Year 2, Semester 2

(Assignment 01 – Individual)-2023

Student Register Number	Student Name
IT21167096	DE ZOYSA A.S.

ABASTRACT

The goal of this study is to uncover the university's logical and physical security problems. The major goal of this study is to clarify the physical and logical basis of these hazards as well as feasible strategies for their avoidance or mitigation. Moreover, it offers recommendations for how to make these conditions and their impact on the university better. To create this research, the researchers also took a look at a wide range of potential security issues.

Physical Vulnerabilities

1. Increased probability of unauthorized persons entering the SLIIT premises

The students of SLIIT Institute have been given an ID card to confirm their identity while registering for their future higher education activities in that institution. But it can be seen that it is misused today. As a result, their girlfriends, boyfriends, and other outsiders who are studying in other universities that are not SLIIT regularly enter without permission using the ID cards of students currently studying at SLIIT. That the security guards within the entry gates are ignoring this is disappointing.

Solution: -

I can see how this may be resolved; even if only the ID card's essential information is included, when it is admitted via the main gate, the name, National ID number, registration status, and photo provided at registration are simply noted in the register number. A pupil cannot genuinely be uniquely identified. Consequently, they may prove their identification accurately without taking much time while visiting Slit University at any time by adding fingerprint scanners, eye scanners, etc. to the data system in addition to the details of the students who are presently enrolled in the institution.

2. **Students are harassed by animals at canteens and other facilities, and animals mess up the canteens.**

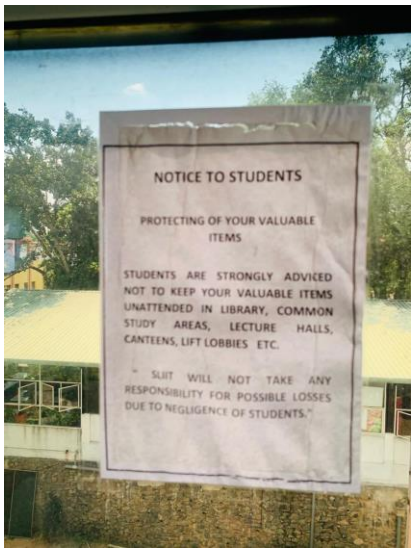
Students are used to feeding animals (dogs) while eating in the study area downstairs in the main building and in the canteen of the same building and in the new building's dining hall. Therefore, due to reasons such as food being overturned and students snatching the food while eating, because dogs frequent there, there is a chance of their insects breeding. Therefore, such places have become dirty places.

Solution: -

One remedy is to point out that the entrance doors are designed to prevent dogs from accessing such shared spaces.

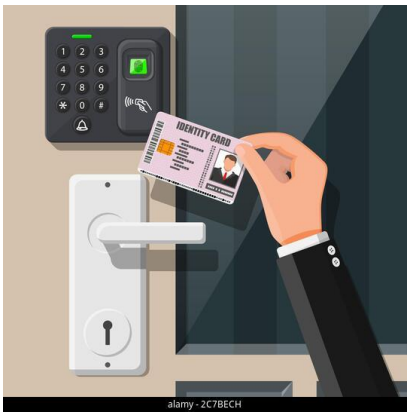
3. **Study area the constant thefts, that is, there is no security for students' equipment in the study area.**

For students' private study, a separate study space has been built in the main building. Yet I've heard in recent months that laptops and chargers are vanishing. As a result, it was discovered that there is virtually little security there. We saw that there are just one or two CCTV cameras in operation. Children frequently collaborate in the study area since it is a location where they may learn without restriction.



Solution:-

Placing a verification machine next to the station that opens and closes the door to the study area to check the student ID will allow for the conclusion to be drawn as to whether they stayed for a specific period of time by recording the times when entering and departing the area. There should be additional CCTV equipment as well.



4. **The safety of the Rack for students' equipment and bags at the front of the library is very low.**

Despite the presence of a number of facilities for bag storage at the entrances to the study area and the library, items like bags, packages, chargers, and laptops are more likely to be taken by a third party.

Solution: -

I propose adding lockers to it that can be opened and closed in order to maintain the security of the items kept within, as well as a pin number that can be used to lock the chambers.

5. **There is no proper management of the entrance and exit of the library so there is room for thieves to enter the library.**

Just one CR book may be carried into the library while accessing it as a restricted area; laptop coverings are allowed. You can work on your laptop in the library area while keeping it there. A spinning door is what you'll notice as soon as you walk inside the lobby. There is a slight wait to access the library even though there is no security present. There is no requirement for people entering the library to have their identity card verified, and the security offered by the rotating door is insufficient. This is true even though a device has been installed close to the rotating door that can verify a student ID for the identity confirmation of coming to the library. Because they have the ability to leave with unauthorized books even if the personnel there has departed for whatever reason. It might not be possible to authenticate the identification, even if there is CCTV.

Solution: -

I propose using automated ticket gates in place of spinning doors as a remedy for this. Entry is not permitted without completing a required card.It might be thought of as a precautionary action to take when visiting this place. Hence, even if a student enters the library, it might be deemed a need to check the ID card before leaving.

6. The security in the back area of the university is very weak.

When entering the back gate, it is seen that the security officers are neglecting to check the students' student ID cards. Most of the time we do not have our student IDs checked when traveling in that vicinity. And it is often only accompanied by a security guard. Last year, we were able to see that students' valuable laptops were stolen through the university's WhatsApp group. In reaction to that, SLIIT University was alerted that a stranger had entered through this rear gate and taken the computers. There was no security present in the parking area that was available for those pupils. The site mirror, for example, had been either taken or broken, despite the fact that the motorcycle was parked. This was mostly visible because security employees were careless, CCTV systems were malfunctioning, and parts of the lights from Curtin University to the rear gate were not turned on at night.

Solution:-

I propose employing a number of security guards as a solution for this.increasing the safety of CCTV, establishing a special parking area just for student automobiles, constructing motorcycle queue chains as obstacles, putting in place a sufficient system to validate the card so that the university may stamp the pass card it provides to students for their vehicles with information about their arrival and departure times.

Logical Vulnerability

1. **The PCs at the computer labs are all very slow and do not have any antivirus software installed.**

In computer laboratories, about 95% of the machines are operating extremely slowly. Hence, regular computer lab users like university employees and students could have trouble getting work done. Students also have a lot of trouble with this. For certain systems, not using anti-virus software is also a dangerous practice. Without this defense, computers are susceptible to viruses, malware, and other security threats that may compromise personal data and lead to other issues.

Solution: -

The computer lab's hardware and software can be inspected to identify outdated parts or applications that can be contributing to performance issues. Budgets should be set aside for new computers or other upgrades in order to boost performance. A thorough security strategy that mandates the installation of antivirus and anti-spyware software on computers should be developed to address this issue.

2. The ID card number on our SLIIT course web and email is a weak password.

default password for the course web and SLIIT e-mail Students are given our ID number, which is a very weak password, by SLIIT Control Unit. It is quite simple for someone else to uncover it and very simple for someone else to take our personal information.

Solution:-

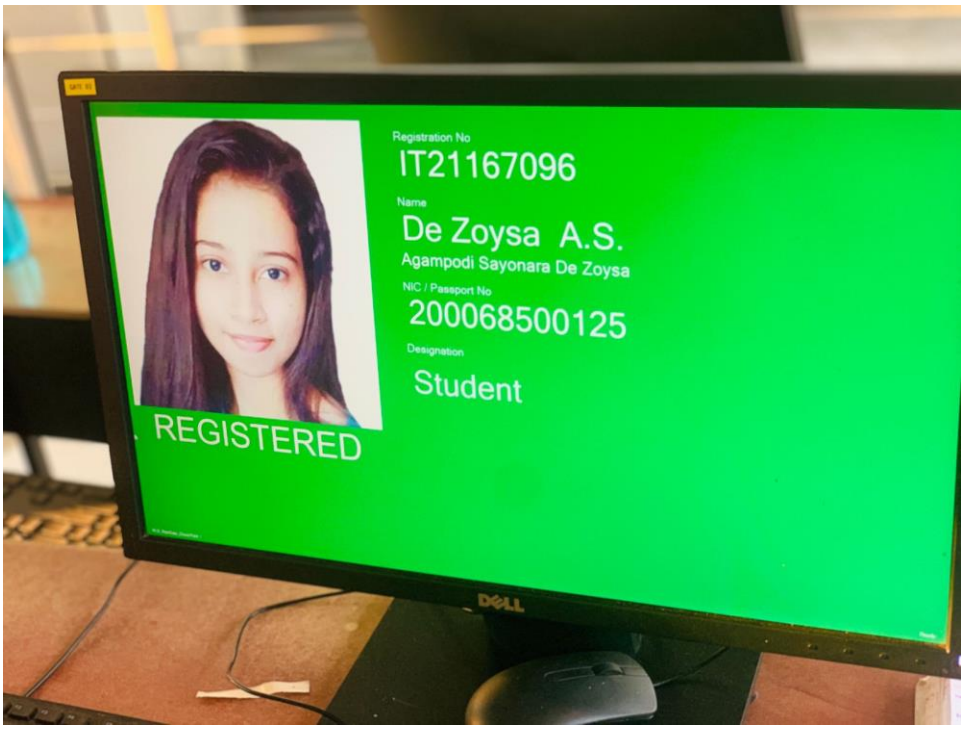
After receiving their first password from SLIIT when they enroll, students should be forced to enter a password that is exceptionally secure. The first password needs to be unique.

3. **Student information can be viewed while confirming identify with a university ID card.**

Displaying all the information about the students on the computer screen, allowing visitors to the institution to view their university ID cards to verify their identification, might be considered as a logical vulnerability. This is due to the fact that websites like course web, eduscope, and net exam can be accessed by using someone else's information (NIC number, IT number).

Solution:-

One solution is to lessen the amount of data displayed on the computer screen. Instead of the student's NIC number and IT number, their name and picture may appear on the computer screen.



4. **Some software in the computers in the computer labs have not been updated.**

This out-of-date software is used by employees and students to waste time and be less productive. Also, because obsolete software that has not been updated gets downloaded into computers, which makes them vulnerable, the likelihood of a hacker assault is great.

Solution:-

A software update strategy that mandates regular upgrades for all software in computer laboratories should be implemented to address this issue. A procedure should be put in place to make sure that updates are applied promptly and thoroughly tested in order to prevent any interruptions.

5. Periodic failure or downtime of servers like eduscope, courseweb, etc.

There are numerous primary web servers at the institution. The two most important ones are the Course web and Eduscope servers. Data and information concerning all SLIIT internal operations, such as lecture materials, schedules, announcements, and more, are available on the Course web server. Also, there is a strong demand for the Eduscope server's server. Teachers and professors frequently post lecture recordings for every module from every faculty. Sometimes, logging onto these two websites is not an option. The servers are offline. Information may be greatly at danger from this.

Solution:-

This danger may be reduced or perhaps eliminated by strengthening the web server network. This refers to the placement of servers throughout a number of data centers, all of which need to be physically close to one another and linked to different networks. This will result in a single web server receiving all network traffic.

7. When an external device is connected to a PC machine in a lab, there is a possibility of malicious applications getting installed by that device if it is infected with a virus. It will be difficult to get rid of it if the machine has not been initiated with a virus guard.

   Solution :-
   Installing of malware detection systems to all severs in the campus premises.

8. There are different users who can login to the PC machines in a lab. The students can login only to the students' account. However, if they got to know the credentials to PC through staff's account, they will get the access and can view the information which should be only viewed by the staff.

   Solution:-
   Using of two-factor authentication when logging in to a system so as to ensure data being secured.

9. In SLIIT, the students who are following the Cyber Security degree have an idea on how to guess passwords. If a student was able to crack the password of a system in the administration maybe using brute force method, he can get access to sensitive information. And there is sensitive information such as details of students and lecturers and the results of the students in the servers in the campus. These data may get altered or damaged by an unauthorized person where the administration will not be able to take use of that information again.

   Solution:-
   Using of intrusion detection or prevention systems helps to protect the servers from attacks like DOS.

10. Students during lab sessions may login to various websites and this may download unauthorized programs to the server and also they may click on various links.

    Solution:-
    Restricting the students by not to visit any websites and verifying the links before clicking on them

REFERENCES

- https://www.studocu.com/in/document/banaras-hindu-university/statistical-mechanics/logical-security-controls-and-measures/5621752#:~:text=What%20is%20a%20logical%20threat,without%20actually%20damaging%20your%20hardware.
- https://portswigger.net/web-security/logic-flaws
- https://blog.usecure.io/physical-security-risks