SECURITY ASSESSMENT REPORT

FOR

UGANDA INSTITUTE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

May 2019

BY

OYEE JAMES
+256773895415
engjames256@gmail.com

Introduction

This report is for the security assessment carried out at Uganda Institute of Information and Communications Technology. The premises is bordered by Makerere University Business School to the East, Nakawa Business Park to the West, Capital Shoppers Supermarket to the North and Nakawa Main Market to the South.

The study looks at the vulnerabilities, security measures in place, weaknesses in the current system used and solutions to the weaknesses observed from the physical and digital assets of the institute. The assets assessed in this report includes the WIFI, website, fence, gates, administration block, classroom block, students hostel, laboratories and library.

Brief background of the Organisation

Uganda Institute of Information and Communications Technology (UICT) was founded in 2000 by Uganda Communications Commission (UCC). Accordingly, the National Council for Higher Education advised the Minister of Education and Sports (MoES) to establish UICT as a public tertiary institution. Consequently, MoES issued Statutory Instrument No. 79 in October 2005 establishing UICT as a public tertiary institution.

In line with this Mandate, the assets of the former Uganda Posts and Telecommunications Corporation (UPTC) Training School, (at Plot 9 –21 Port Bell Road, Nakawa) were invested in UCC, and that is where the Institute is located. UICT is a successor Institute to the UPTC Training School established in 1965 by the then East African Posts and Telecommunications as a regional training center.

The Uganda Communications Act 2013 mandates Uganda Communications Commission to operate and manage the Institute. This has been done to enable the Institute to get policy guidance and funding to upgrade the Institute into a Centre of Excellence to the level of internationally renowned ICT Institutions.

The Uganda Institute of Information and Communications Technology (UICT) is the **only Government institution specializing in skills-based middle-level ICT training**. It offers practical-oriented ICT training at certificate and diploma levels as an alternative to the theoretically-grounded degrees offered by Universities and other Tertiary Institutions in this same professional area. The institute provides education and training in all fields related to the communications sector including telecommunications services, computer engineering, and information technology and business management.

Digital Security Situation

A. WIFI

Vulnerability

- Weak passwords used to secure WIFI access points.
- Guests to the organisation also use the same Access Points.

Security Measures in use

- WIFI secured with passwords.
- Different access points made available for classes, library and staff members.

Weaknesses in the System

- Using weak passwords puts the users at risk of a possible attack as it is easy to crack or guess by the attacker.
- Passwords can also easily be given out by any one who knows it to anyone outside the organisation which grants them access to a possible attack.

Solutions to Weaknesses

- Use strong passwords that has a combination of lower and upper case letters, numbers and special characters.
- Use a passphrase instead of passwords to produce long characters that are hard to guess.
- Use MAC Address Filtering technology which gives only access to admin to connect devices.
- Configure your network to allow only connections for registered students by prompting them to enter their student details on first connection to the network.
- Provide a seperate network access for guest as this will prevent them from affecting the organisations computers as well help in close monitoring of their activities.
- Use firewall to provide defence against attacks coming from outside the network and block suspicious activity.

B. Website (http://www.uict.ac.ug/)

Vulnerability

- Insecure HTTP cookies.
- Directory listing is enabled.
- Communication is not secure.

Security Measures in use

- Free of Malware.
- Secure Renegotiation and TLS_FALL_BACK_SCSVsupported.
- Content is not visible via cross-origin resource sharing (CROS) files and headers.

- Server key and certificate available and transparent - RSA 2048 bits (SHA256withRSA) which is trusted by Mozilla, Apple, Java and Windows among others.

Weaknesses in the System

- Secure Flag missing which allows the browser to send web data over an unencrypted channel (PLAIN HTTP) if a request is made and this allows the attacker to intercept clear text communication between the browser and the server which allows him to steal the cookie of the user.
- HTTPOnly missing which allows the browser to access the cookie from the client side scripts like JavaScript and VBScripts, this can be exploited by an attacker in conjunction with cross site scripting (XSS) attack inorder to steal affected cookie.
- Communication between the web browser and the server is done using HTTP protocol which transmits data over the network which allows the attacker who manages to intercept at network to be able to read and modify any sensitive data transmitted.
- With directory listing the attacker can see the entire structure and sub directories which give them access to sensitive files that may be hidden from the public files in that location.

Solutions to Weaknesses

- Reconfigure the server to use HTTPS which encrypts the communication between the browser.
- Reconfigure the web server in order to set the flags to Secure or HTTPOnly to all sensitive cookies.
- Reconfigure the web server in order to deny directory listing and verify if there are no sensitive files on the public directory.

Physical Security Situation

1. Fence

Vulnerability

- Wire fence can easily be penetrated by a fast speeding car.
- Low height fence.

Security Measures in use

- Fenced with wire.
- Fence about 1.5m high from the ground.

Weaknesses in the System.

- The premise is located near the Portbel highway and the wire fence can easily be penetrated by a fast moving car that leaves the runway and could harm anyone in the compound..
- The fence being around 1.5m high above the ground makes it easy for an attacker to jump in.
- Wire fence also allows an attacker to view the compound from outside which help them to plan an attack.

Solutions to Weaknesses

- Use concrete for fencing as this offers extra resistance that would minimize a possible damage to other structures inside the compound.
- Build the fence that is high from the ground to make it hard for an attacker to jump in. This will also block access to viewing the compound from outside.
- Include sharp objects on the top part of the fence to make it hard for the attacker to pass through safely.

2. Gates

Vulnerability

- Gates has no CCTV Cameras.
- There are three gates to the premises.
- Guards don't have security magnifying glass for checking cars.
- Guards at the main gate dont check students bags on entry and exit.
- Guards don't have metal detectors for checking people accessing the premises.
- The entrance near MUBS and the one opposite Capital shoppers has no guards.
- Guards at the main gate dont check cars accessing the premises on entry and exit.
- Guards at the main gate dont check to verify if people entering the premises are students.

Security Measures in use

- Main gate has guards.
- Bodabodas not allowed in the premises.
- Stop point available for cars before entry.

Weaknesses in the System.

- CCTV camera is needed at the gates because sometimes the Guard may not be around at the gate and so an attacker may get in without his notice.
- Having three gates gives many entry points for the attacker and are hard to monitor at the same time.
- Operating without magnifying glass for cars leaves the victim with an opportunity to hide any harmful material under his car.
- Operating without checking students allows them to escape easily with any school property that they may pick during their time at school.
- Operating without metal detectors allows the attacker to carry some materials that may be of harm.
- Having guards at one gate and leaving two without gives the attacker more potential entry points.
- Failing to check cars on entry gives the attacker a chance to carry any tools they may need for the job and failure to check on exit gives them opportunity to carry out any item of interest to them.
- Failure in verification of who accesses the premises gives the attacker an opportunity to enter as if they belong to the premises.

Solutions to Weaknesses

- CCTV cameras has to be installed at all entry points to closely monitor who comes in and gets out.
- Limit the number of entry points to premises to one where there are guards to avoid illegal entry.
- Guards should also be equipped with security roll magnifying glasses for checking if cars don't have any harmful materials under their car.
- Guards should be advised to always check students bags to see if they haven't carried any school property.
- Guards should also be equipped with metal detectors to help check if a person entering has some metallic material can be on harm.
- Guards should be advised to check cars leaving the premises to check if they have picked any property illegally.
- Guards should be advised to always request identification for people entering to verify if they are students or else verify purpose of visit for non students and advise them accordingly.

3. Parking

Vulnerability

- Parking area has no CCTV Cameras.
- No specific parking lots allocated to staff.

Security Measures in use

- Parking lots marked for each car.

Weaknesses in the System.

- Having no CCTV cameras give an attacker a chance to plan an attack as he only needs to observe the movement patterns of the guards on ground.
- Allowing everyone to park at the same place gives room for an attacker to cause harm to any car pretending to be the owner.

Solutions to Weaknesses

- CCTV cameras should be installed at the parking lot as this makes it easy to track in case of theft by following the video footage.
- Having specific parking lots for staff helps to determine who should access which car as the owners have lots allocated. I also helps to identify a potential attacker in case of mismatch in parking.

3. Compound

Vulnerability

- No assembly point marked on the compound.

Security Measures in use

- Lighting is provided in most areas.
- The grass is well slashed and no bushy areas.

Weaknesses in the System.

- Having no assembly point marked leaves people in panic and stranded in case of any danger like fire outbreak.

Solutions to Weaknesses

- Mark an assembly point in the compound to help guide people when they can come together in case of any danger.

4. Classroom Block

Vulnerability

- No alarms systems such as smoke detectors installed.
- Compound behind the classroom block towards Capital Shoppers has no security light.

Security Measures in use

- Good Air Conditioning.

- CCTV Cameras installed.
- Fire Extinguishers installed.
- Lightning conductor installed.
- Path way provided for the disabled.

Weaknesses in the System.

- Having no security light behind the classroom block allows the attacker to access easily at night.
- Having no alarm systems installed puts the users of the builder at risk as it may not be easy for them to seek help of notify people outside easily when in a problem.

Solutions to Weaknesses

- Put security light to ensure a clear view of the place at night and avoid usage of it as a hiding place by attackers.
- Install alarm systems to help in giving awareness in case of danger in any part of the building.

5. Laboratory (Electronics and Computer)

Vulnerability

- Bags allowed freely in the laboratory.
- Removable devices like flash disks and external hard drive allowed in the computer laboratory.

Security Measures in use

- Good Air Conditioning.
- CCTV Cameras Installed.
- Laboratory attendants available.
- Fingerprint door access for staff.
- Proper shielding of power cables.
- Switches and routes well locked in cabinets.
- Operating system set to update automatically via the internet.
- Antivirus software installed and set to update automatically via the internet.

Weaknesses in the System.

- Allowing bags freely in the laboratory gives an attacker opportunity pick unauthorised property and hide easily.
- Removable device allows the attacker to carry virus they may have in computers they have used the same device on before.

Solutions to Weaknesses

- Removable devices should not be allowed in the computer laboratory, they should use other platforms like email for sharing notes and other study materials.

- The network administrator should block slots for removable devices in the computer laboratory to limited usage of such devices,
- A separate place should be provided in the laboratory where students leave their bags before the class sessions.
- Tags should be provided to each student that corresponds to the porch where the bag is placed for easy identification of bags after a class session and avoid theft of bags.

6. Library

Vulnerability

- Two doors available for students.
- Bags allowed freely in the library.
- Compound behind the library block towards Capital Shoppers has no security light.

Security Measures in use

- CCTV Camera installed.
- Library attendant available.
- Lightning conductor Installed.
- Library card required to access the book section.

Weaknesses in the System.

- Having two doors gives an attacker an opportunity to access the premises easily as ther is only one attendant.
- Allowing bags freely in the library gives an attacker opportunity pick unauthorised property and hide easily.
- Compound behind the library block towards Capital Shoppers has no security light

Solutions to Weaknesses

- Reduce entry points to only one so that it is easy for the liberian to monitor people coming in and leaving easily.
- A separate place should be provided in the library where students leave their bags before the class sessions.
- Tags should be provided to each student that corresponds to the porch where the bag is placed for easy identification of bags after a class session and avoid theft of bags.
- Put security light to ensure a clear view of the place at night and avoid usage of it as a hiding place by attackers.

7. Administration Block

Vulnerability

- No alarms systems such as smoke detectors installed.

Security Measures in use

- CCTV Cameras installed.
- Fire Extinguishers installed.
- Lightning conductor installed.
- Office block partitioned for different departments like bursor, secretary, principal among others.

Weaknesses in the System.

- Having no alarm systems installed puts the users of the builder at risk as it may not be easy for them to seek help of notify people outside easily when in a problem.

Solutions to Weaknesses

- Install alarm systems to help in giving awareness in case of danger in any part of the building.

8. Students Hostel

Vulnerability

- Compound in front of the hostel block towards the dining hall has no security light.

Security Measures in use

- CCTV Camera installed.
- Lightning conductor Installed.

Weaknesses in the System.

- Having no security light in front of the hostel allows the attacker to access easily at night.

Solutions to Weaknesses

- Put security light to ensure a clear view of the place at night and avoid usage of it as a hiding place by attackers.