From my viewpoints as both a student and a professional, I will discuss wired and wireless security at Coleman University. As a student, I am not privy to such information about the private and public computer networks at Coleman University. As a professional, I have knowledge about computer networks because of my previous education and work experience.

My Perspective on the Wired Network Security at Coleman University

Students usually work on school assignments on the school’s PCs at school. They need Internet connectivity at the school to study research, to access Webclass for the class schedule and schoolwork assignments, and to read their student email. To continue their schoolwork at home, the student typically transfers the data via USB flash-drives. This is a typical scenario for the student. An alternative for the student would be to save their schoolwork data on the cloud, via a user account, i.e. Google Drive, Dropbox, and OneDrive.

When students connect their USB flash-drives into the school’s computers, there is a real chance for computer viruses and worm attacks on the school’s network. The school uses an automated patch update service to keep the desktop PCs updated and upgraded, via the network. This is the first-line of defense against malware intrusion.

Considering the safe environment of the school’s network, I can assume that the school has implemented a security policy to achieve the Quality of Service (QoS) that the school provides. The network administration probably configured the network to include several layers of security, with a DMZ of multiple firewalls, switches, and proxy servers.[[1]](#footnote-1)

If some student thought to unplug the Ethernet cable from school computers and use the wired connection, it would not work. The security policy restricts access to unauthorized computers. The network domain server has a Hosts table setup and uses Address Resolution Protocol (ARP) to deny access to unrecognized computers to join the domain. Though this sounds strange, I have not seen any students try to connect a router device to the wired network but we haven’t been told ‘making a rogue network’ is forbidden, either.

The wired network is provided on school desktop PCs. Access is restricted by security rules that require user authentication from a combination of a student ID number and a password.

Security rules also dictate password strength and limits the count of unsuccessful logins before an account is locked (disabled). The solution requires the student to visit the school’s technical support department to request their assistance to reset the password. Some good guidelines for implementing authentication is the ‘Authentication Cheat Sheet,’ posted among other security cheat sheets, by the Open Web Application Security Project (OWASP)[[2]](#footnote-2)

The school stores computer files on a server that are relevant to the students’ school work, and shared as ‘system services.’ These files are shared, with a student who is logged in as an authenticated user to gain ‘user rights,’ and found by a mapped network ‘R’ drive. The files (data) is logically accessed from a network segment through subnet addressing. The use of ‘group policy’ restricts the data of each program to the students enrolled in that program, i.e. Computer Information Systems, Computer Networking, and Game Programming Design & Development. ‘Account Policies’ separate the curriculum data from the school’s business data, on the same LAN. The school also allocates storage space on the server for each student and is found by a mapped network ‘S’ drive. I believe each student’s ‘S’ drive is limited to 250 Gb. The network shares on the school’s LAN is not accessible outside the wired connection, such as the school’s virtual LAN of the wireless network or from elsewhere via the Internet. I will assume that the school uses a Microsoft® Domain Server to control and manage access to the wired LAN(s). It probably uses role-based access control (RBAC) to make groups of Students, Faculty, Executive Administration, and Support.

My Perspective on the Wireless Network Security at Coleman University

As students evolve, they may use their own personal mobile PCs (laptop/notebook) to store schoolwork, organized and available to them for their prospective professional career. They need Internet connectivity at school to do the research, access Webclass and read student email; and the university provides a wireless network for that access. If there was no wireless network at Coleman University, student would be required to do schoolwork elsewhere. Many students have smartphones and tablets with Internet connectivity via cellular data (does not require a router configuration)[[3]](#footnote-3) but the cell reception inside the school building is weak (sucks). The advantage of cellular data versus Wi-Fi data is connectivity/access in more (or less) places.[[4]](#footnote-4)

I successfully connected to Coleman University’s wireless network for Wi-Fi connectivity to the Internet, with my personal Notebook PC. It runs the Microsoft© Windows 8.1 operating system. It detects wireless networks and I choose the network and it prompts me to enter the network security key (password). I configured the setting to automatically connect when that network is detected. The network detection is called Network Discovery[[5]](#footnote-5) and it requires that the DNS Client, Function Discovery Resource Publication, SSDP Discovery, and UPnP Device Host services are started, that network discovery is allowed to communicate through Windows Firewall, and that other firewalls are not interfering with network discovery.

I successfully connected to Coleman University’s wireless network for Wi-Fi connectivity to the Internet, with my personal Linux Server, Notebook PC. It runs the Ubuntu© 12.04 LTS Server with the Linux Server 3.5 operating system. I typed the Linux command: “sudo vi etc/network/interfaces” to start the Vi editor and edited the interfaces file to add a network connection-string to connect to Coleman University’s wireless network with the network security key (password). The script looks like this: “wpa-ssid ColemanUniversity” and “wpa-ssid DreamsIntoReality” and then I reboot the computer after “sudo shutdown –h now.” The Linux system also has network detection to connect automatically when the network is present. I have a similar connection-string for the Wi-Fi at my home.

As a previous student of the NET210 Wireless Technologies course,[[6]](#footnote-6) I learned about some network security technology such as Wi-Fi Protected Access (WPA), WPA – Pre-shared key (WPA-PSK), Wired Equivalent Privacy (WEP), Advanced Encryption Standard (AES), and Remote Authentication Dial-In User Service (RADIUS) Server, and security policies and implementation. I also learned of some wireless network vulnerabilities and attack methods, such as denial of service (DoS), encryption cracking, authentication cracking, brute-force attacks, and MAC spoofing. Our class walked around Coleman University doing a short, practice site survey of the wireless network layout. We located several access points (APs) and measured their transmitted signal strengths with our smartphones’ mobile app ‘Wifi Analyzer.’[[7]](#footnote-7)

1. SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS, 4th Edition, Mark Ciampa, Ph.D, © 2012 Course Technology, Cengage Learning. Course textbook for SEC200 Intro Network Security, Coleman University, 2015. [↑](#footnote-ref-1)
2. ‘Authentication Cheat Sheet’ is posted by the *Open Web Application Security Project* *(OWASP)* listed on this page: <https://www.owasp.org/index.php/Cheat_Sheets> [↑](#footnote-ref-2)
3. My blog on Google+, downloaded from <https://plus.google.com/100399506962260633705/posts/PtZbQgjc5F2> [↑](#footnote-ref-3)
4. ‘What’s the Difference Between Wi-Fi Data and Cellular Data’ downloaded from <http://www.verizonwireless.com/mobile-living/tech-smarts/wifi-vs-data-plan-verizon-wireless/> [↑](#footnote-ref-4)
5. ‘What is Network Discovery?’ downloaded from <http://windows.microsoft.com/en-us/windows/what-is-network-discovery#1TC=windows-7> [↑](#footnote-ref-5)
6. ‘CWNATM Certified Wireless Network Administrator, Official Study Guide, Third Edition, Exam PWO-100, McGraw Hill, Osborne, 2008. Course textbook for NET210 Wireless Technologies, Coleman University, 2014. [↑](#footnote-ref-6)
7. More information about the mobile app ‘Wifi Analyzer’ at <http://a.farproc.com/wifi-analyzer/> [↑](#footnote-ref-7)