Imperial Journal of Interdisciplinary Research (IJIR)
Vol-2, Issue-12, 2016
ISSN: 2454-1362, http://www.onlinejournal.in

Raspberry Pi 2 Platform for Coin-operated WiFi HotSpot Kiosk

Jeffrey Co[1], Geronimo Duran[2] & Charito Sabate[3]
[1,2,3]Computer Engineering Department, Eastern Samar State University
Borongan, Eastern Samar

Abstract: *This project is a Coin-operated WiFi HotSpot Kiosk using raspberry pi 2 that can be deployed outside the library or any places where internet access is necessary, ideally to support research needs of students, faculty and staff. The default behaviour here is to deny access on internet. Users will have to insert five (5) peso coin into the kiosk and a username and password will be printed. The username and password generated by the system will be used as a log in credentials to access the internet. An authenticator redirects any request for connection to a log-in page and verifies the log-in credentials. Once the authenticator checks the log-in credentials from the database, it will return the IP address of the URL being requested and the users can then access the internet. The system also includes generation of billing report. It is a billing statement that shows the clients internet usage.*

1. Introduction

Raspberry Pi is a series of credit card-sized single-board computers developed in the United Kingdom. It has memory capacity and several peripheral device support such as RAM, I/O, processor, Ethernet and USB port. By utilizing this chip and integrating it with an open-source captive portal like a chilli spot, a system was developed that provides a controlled public-access network. In this paper, a WiFi Hotspot is designed where the user are obliged to view or interact with before access to internet.

Unlike with the WiFi hotspots for internet users that are typically used in coffee shops, business centers, airport, hotel lobbies, and other venues that offers WiFi hotspots, the system uses a raspberry pi 2 board that significantly cuts down the cost of providing paid internet access. Also in this project, a username and password is printed and is used as log-in credentials.

The project is a Wi-Fi HotSpot kiosk that can be located in public places where people can access internet by inserting 5 peso coin to the coin-slot. The notable innovation on this project is random generation of printed username and password to be used as internet log-in credentials to access the internet. The default behaviour here is to deny access on internet. When the users key-in the username and password generated, the authenticator redirects any request for connection to a log-in page and verifies the log-in credentials. Once the authenticator checks the log-in credentials from the database, it will return the IP address of the URL being requested and the users can then access the internet. Accounting utility is also used in this project to redirects the request to a web log-in portal if time for internet use expires.

Several prior arts are similar to this study like the PESONet of PLDT. In the PESONet, the user inserts 1peso coin for every 15minutes of internet access but this kind of system runs only in a wired network typically in internet café where computers are connected thru cables and computers are in fixed location. Due to increasing use of wireless mobile gadgets in schools or in any establishment, it would be more convenient for students to have internet access to aide their studies. More often, it is very expensive to deploy wireless access point with RADIUS server and an authenticator. In this project, the concept of PESONet was used in a wireless network where log-in authentication is required but uses a very cheap replacement of a RADIUS server and an authenticator by using a raspberry pi platform.

2. Review of Related Literature and Studies

This section includes the review of related literature and studies which the researcher has perused to shed light on the development of the project.

Piso Net also known as "*hulog-piso*" is a mini-type internet or gaming machine. It is basically a merge of PC rental and arcade rental services wherein customers can pay the services by inserting coins to the machine. The rate is typically 4mins/peso which also amounts to the typical Internet Cafe rate of Php15/hr. This rate can be tweaked higher or lower either to be more competitive and entice customers or gain more income by decreasing the minutes/peso. According to Lim [12], they were able to offer data services in "sachet" with the advent of pisonet. This allows their customers to pay only for the internet services that they need. PisoNet became popular because it offers benefits like easy maintenance, no need for additional man power, can utilize space, and the customer can access sites and other apps cheaply.

Reference [4] shows that in Maxcom Taiwan, "*Tap Coin Wi-Fi Hotspot Pay Terminal*" is very popular. The technology is a coin operated WiFi hotspot pay terminal which is a fee-based or free-registration WiFi solution designed to help all indoor venue owners (e.g. coffee shops, retail stores, chain shops). It provides the visitors an immediate WiFi hotspot service, by connecting with xDSL/cable modem or 3G/4G network (optional backup connection, only for model WIFI-B202) wherein the customers tap their smartphone on the kiosk screen. A coin is also inserted to access the internet depending on how long the customer wishes to surf the internet.

The project is based on the idea of the pisonet and the tap coin WiFi Hotspot of Maxcom. However in this project, a raspberry pi 2 platform and an open source captive portal are used which significantly cuts down the cost of the technology.

3. Methodology

The following discussion describes the materials and processes used in the development of the project.

3.1 Hardware Components Interconnection

Figure 1 outlines the interconnection of the hardware components of the project. As seen in figure 1, it is composed of a raspberry pi which serves as the system platform and a dongle to allow access to wireless broadband. Contained in the raspberry pi are LINUX operating system, PUTTY (programming language for raspberry pi), a Python program for random password generation and printing, and a MySQL database for access authentication.

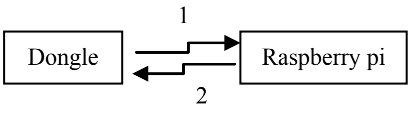


Figure 1. Hardware Components Interconnection for Wi-fi Kiosk

Particularly, the researcher developed the wi-fi kiosk that generates and prints random password, authenticates internet credentials, redirection page if the time of usage expires, and filters restricted site.

3.2 Log-in Authentication

An opensource RADIUS software was used in this project to authenticates internet access credentials. A RADIUS software enables the remote access to a network, it receives request and authenticates the request as shown in Figure 2. The user or a machine sends a request to raspberry pi in the form of password and username. The RADIUS software checks that the information is correct using authentication schemes. The user's proof of identification is verified along with other information stored in the database in the MySQL. Once the identification was verified, the RADIUS software will send back the ip address of the site that the user is requesting.

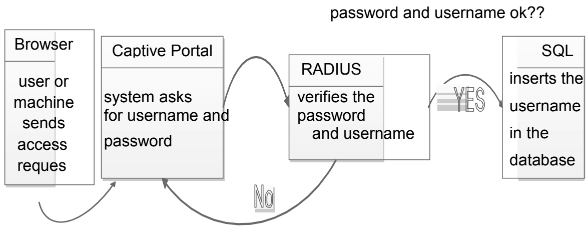

password and username ok??
Browser
user or machine sends access reques
Captive Portal
system asks for username and password
RADIUS
verifies the password and username
YES
SQL
inserts the username in the database
No

Figure 3. Authentication Process of the Internet Access Credentials

3.3 Web Log-in Redirection Page

CoovaChilli is an open-source software access controller, based on the popular, but now obsolete, ChiliSpot project. This software provides a captive portal/walled garden environment and uses RADIUS for access provisioning. CoovaChilli software was used in this project as captive portal or web log-in redirection page. Figure 3 shows the block diagram of the how the web log-in redirection page works.

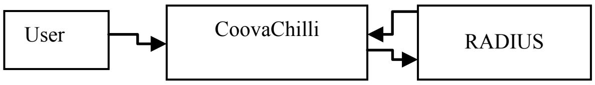


Figure 4. Web Log-in Redirection Page using ChoovaChili Access Controller

4. Results and Discussions

Most WiFi wireless access points / routers claim to support up to 255 devices. Users can be connected to this system via wireless network. While it is theoretically possible to connect up to 255 users to the kiosk, it is not recommended because performance of the system will be very poor. For better internet connections, the system can only handle 30 concurrent users, it is recommended to install multiple access or adding more access points to the network to effectively handle a larger number of users that can be supported. Figure 5 shows the developed Coin-operated HotSpot Kiosk.

The system consists of a thermal printer that prints the randomized unique username and password that will be used as log-in credentials in order to access the internet. Python program was used to randomly generate password and username

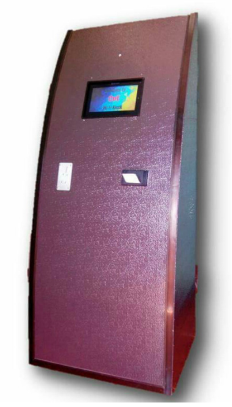


Figure 5. Coin-operated Wi-Fi HotSpot Kiosk

When a five (5) peso coin is inserted in a coin slot, high signal is detected in a serial port of the raspberry pi. The serial port triggers the "makeusername" and "makepassword" block to be executed. When the raspberry finished executing these block of line of code, it will print the generated password and username. In the "INSERTINTO", the structured query language will insert into the database the generated password and username. Figure 6 shows the interconnection of the project's electronic components.

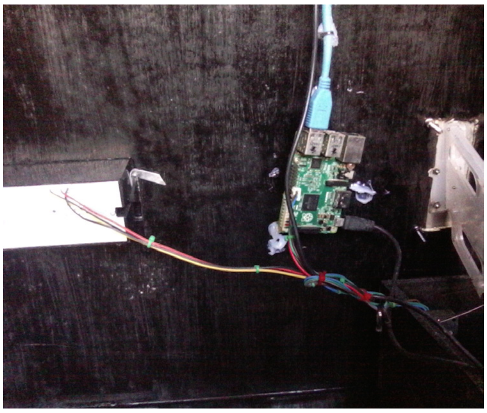
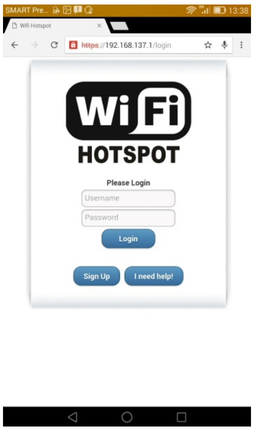


Figure 6. Electronic Components of the Coin-operated WiFi HotSpot Kiosk Showing the Interconnection

When user requests access to internet, the user first logs on to a network with a captive portal, a Web page is encountered that requires certain actions before Internet access is granted. A simple captive portal used in this project is shown in figure 7 which forces the user to log-in by entering their username and password. Captive portals used in this project require the entry of the username and password generated by the system before accessing the Internet.

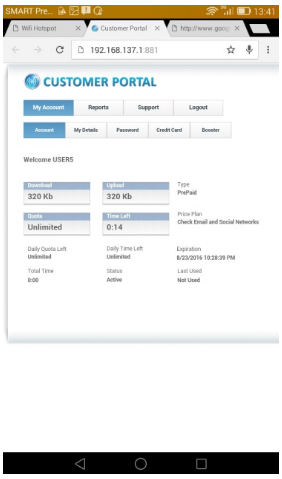
Even when a simple captive portal is used in a free public-access network, certain people may repeatedly connect, using the network on an almost continuous basis to download music, videos, or other large files. This activity, called bandwidth hogging, can be minimized by additional programming in the captive portal. Such programming can control the speed at which large files are downloaded, limit the size (in kilobytes or megabytes) of files that can be downloaded, restrict the number of downloads that can occur in a single session, or block connection to Web sites commonly used for downloading large files. This is called bandwidth throttling or traffic shaping which can also be found in this project.



https://192.168.137.1/login

Figure 7. Web Log-in Redirection Page

After successful log-in to the captive portal, the network user will be redirected to the second web redirection page (figure 8). The access time, upload and download speed can be seen in this portal .



192.168.137.1:881

Welcome USER5

Download 320 Kb

Upload 320 Kb

Type PrePaid

Quota Unlimited

Time Left 0:14

Price Plan Check Email and Social Networks

Daily Quota Left Unlimited

Daily Time Left Unlimited

Expiration 8/23/2016 10:28:39 PM

Total Time 0:00

Status Active

Last Used Not Used

Figure 8. Customer Portal Showing the Remaining Access Time and Upload/Download Speed

5. Summary

This project is a kiosk that can be deployed outside the library or any places where internet access is necessary, ideally to support research needs of students, faculty and staff. The architecture presented in this paper does not require any client software installations. It uses a raspberry pi as a platform that prints randomized unique username and password that is used as log-in credentials. The captive portal technology used in the project is an open source CoovaChilli to show login page in customer browser. Upon connecting to the network, the network user will be prompted to enter valid username and password to get Internet access. After successful login, the internet can see the remaining time and bandwidth quota, expiration date and other relevant info. HotSpot keeps track of customer account and shows warning message when the account is due to expire, helping the users to request for additional time of internet access to continue using the service without interruption.

6. Acknowledgements

The researchers would like to express the deepest appreciation to the Research and Development Services Office, Eastern Samar State University under the direction of Dr. Grace O. Manlapas and the ESSU President Dr. Edmundo Campoto for funding this study.

To the Vice President for Research and Extension, Dr. Eva P. Palada for continuously and convincingly conveyed support in writing this paper. She had showed enthusiasm and excitement with regards to conducting research.

The researchers would like to thank the College Dean, Dr. Leovigildo Cardenas and to the Technical Writing Group member Engr. Arnaldo Villalon for their constructive suggestions and comments to improve the content of this paper.

7. References

[1] Lack, Rex (August 2009). Managing the Testing Process: Practical Tools and Techniques for Managing Hardware and Software Testing. Hoboken, NJ: Wiley. ISBN 0-470-40415-9

[2] *ISO. 2013. Retrieved 2014-10-14.S. Zh*ang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 1999.

[3] ISO/IEC/IEEE DIS 29119-4 Software and Systems Engineering - Software Testing - Part 4- Test Techniques. ISO. 2013. Retrieved 2014-10-14.

[4] MaxCom. (2012) MaxCom homepage on Phil. [Online]. Available: http://www.ri.maxcom.com/en

[5] Cimperman, Rob (2006). UAT Defined: A Guide to Practical User Acceptance Testing. Pearson Education. pp. Chapter 2. ISBN9780132702621

[6] Goethem, Brian Hambling, Pauline van (2013). User acceptance testing : a step-by-step guide. BCS Learning & Development Limited. ISBN 9781780171678.

[7] Pusuluri, Nageshwar Rao (2006). Software Testing Concepts And Tools. Dreamtech Press. p. 62. ISBN 9788177227123.

[8] "Factory Acceptance Test (FAT)". Tuv.com. Retrieved September 18, 2012.

[9] "Factory Acceptance Test". Inspection-for-industry.com. Retrieved September 18, 2012.

[10] "Introduction to Acceptance/Customer Tests as Requirements Artifacts". agilemodeling.com. Agile Modeling. Retrieved 9 December 2013.

[11] Don Wells. "Acceptance Tests". Extremeprogramming.org. Retrieved September 20, 2011.

[12] C. Lim, "A Smart Communication Launches PisoNet," *Smart Communications*, vol. 7, pp. 2-3, October 2010.