CS 6400 Wireshark-Captured Networking Data Management

GROUP 21

Jiaxiu Zhao
Zhongyi Luo
Yiling Yin

Wireshark-Captured Networking Data Management

In this project, we've implemented a DBMS which can be used by network administrator to monitor and manage the networking data collected by wireshark and perform access control accordingly. An account system is incorporated to allow potential hotspot users to register to the system; once approved, the administrator will grant the user access to the hotspot. Detailed functions will be listed in next few slides.

Wireshark-Captured Networking Data Management

Achieved Functionalities:

a. Users could register and apply for an account with required information.
b. Administrators can check and manage the account information and approve potential hotspot users' registration request. Once approved, an email will be sent to that user containing the hotspot's name and password.
c. Hotspot users' access entry information can be collected by Wireshark, then parsed and imported into the database by the administrator.
d. Administrator is able to query for specific access histories according to user name and device type.
e. Administrator is able to update and import the restricted website list into the database.

Wireshark-Captured Networking Data Management

Continued...

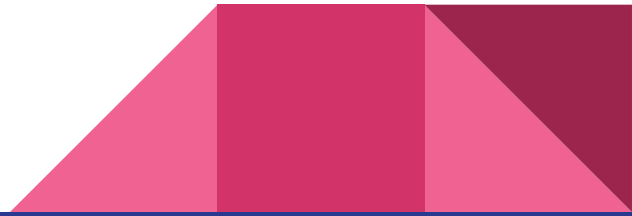
f. Administrator can check for the violation history to see if a specific user violates the rules or not.
g. Administrator is able to send a warning message to the hotspot user by email to warn his/her inappropriate networking behaviors.
h. Administrator is able to manage the hotspot according to the violation histories collected and perform some access control to block the Internet access of those violators.
i. Administrator is able to monitor the network using Wireshark.
j. Hotspot user is able to reset his/her email and password after log in.
k. Hotspot user is able to check his/her own access entries with advanced search.

Wireshark-Captured Networking Data Management

Tools & Libraries Used:

Tools: MySQL 5.6, Eclipse, Wireshark, WiFi HotSpot-Connectifyme.

Library: MySQL-connector-Java.



Wireshark-Captured Networking Data Management

Future Works

Add user behavior pattern

Devide users into different groups to let them be administered by different administrators respectively