TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

──────── \* ───────

Báo cáo bài tập lớn

**CÁC HỆ PHÂN TÁN**

**ĐỀ TÀI 01: XÂY DỰNG ỨNG DỤNG MYSSH**

Giáo viên hướng dẫn: TS. **Nguyễn Bình Minh**

Sinh viên thực hiện :

**Nguyễn Hiển Tường 20122776**

**Trần Văn Hiếu 20151369**

**Hà Đình Khoẻ**

HÀ NỘI 5-2018

**MỤC LỤC**

[I. Yêu cầu đề tài 2](#_Toc481990125)

[II. Phân công công việc 2](#_Toc481990126)

[III. Công nghệ sử dụng 4](#_Toc481990127)

[IV. Phân tích thiết kế hệ thống 4](#_Toc481990128)

[4.1. Mô hình hệ thống 4](#_Toc481990129)

[4](#_Toc481990130)

[4.2. Tác nhân tương tác 4](#_Toc481990131)

[4.3. Phân tích chức năng, nghiệp vụ của hệ thống 5](#_Toc481990132)

[a. Với chức năng trên Server 5](#_Toc481990133)

[b. Chức năng trên Client 6](#_Toc481990135)

[V. Cài đặt, minh họa chương trình 6](#_Toc481990138)

[5.1. Cài đặt 6](#_Toc481990139)

[5.2. Minh họa chương trình 6](#_Toc481990144)

[VI. Danh mục tham khảo 11](#_Toc481990145)

1. Yêu cầu đề tài

Viết ứng dụng myssh mô phỏng chương trình “ssh” để Client kết nối từ xa đến Server thực hiện các lệnh hệ thống trên Server dùng socket, giao thức TCP.

Kịch bản hoạt động yêu cầu như sau:

* Giao diện dòng lệnh
* Multiclients: cho phép nhiều clients kết nối đồng thời (giới hạn N clients, vượt quá N thì không cho phép kết nối)
* Khi client kết nối tới phải đăng nhập (username / pass). CSDL người dùng là của chương trình, không phải của hệ thống, cơ chế lưu tùy ý (CSDL, text, v.v)
  + Server thông báo kết nối thành công hay không
* Khi kết nối thành công thì client có thể thực hiện các lệnh trên hệ thống của server
  + Các lệnh có thể có tham số hoặc không
  + Một số lệnh cơ bản: hiển thị thư mực hiện thời, in danh sách các tệp, thư mục trong thư mục hiện thời, xóa, di chuyển tệp, thư mục, hiển thị ngày giờ hệ thống, v.v...
* Server phân tích lệnh nhận được từ phía client, thực hiện và trả kết quả cho client
  + Nếu các lệnh thực hiện không được phép chạy thì phải thông báo lỗi.
  + Lệnh chạy trên server phụ thuộc vào hệ điều hành mà server được cài đặt lên (Windows, Linux)
* Kết thúc phiên làm việc client gửi lệnh ngắt kết nối tới server và chấm dứt kết nối.

1. Phân công công việc

Công việc được phân công theo bảng phân công sau:

|  |  |  |
| --- | --- | --- |
| **Trần Văn Hiếu** | **Hà Đình Khỏe** | **Nguyễn Hiển Tường** |
| Nghiên cứu tài liệu  Thực hiện code:  - server + client  - xử lý request | Nghiên cứu tài liệu  Kiểm thử  Mã hóa dữ liệu | Nghiên cứu tài liệu  Kiểm thử  Kết nối csdl  Báo cáo |

1. Công nghệ sử dụng

Các mô hình và công nghệ sử dụng:

* Ngôn ngữ : JAVA
* Kết nối trên nền tảng kỹ thuật Socket – TCP
* Thực thi câu lệnh thông qua runtime và process

1. TỔNG QUAN HỆ THỐNG
2. Một số kiến thức chung

SSH là gì?  
  
SSH ( Secure Shell) là một giao thức mạng dùng để thiết lập kết nối mạng một cách bảo mật. SSH hoạt động ở lớp trên trong mô hình phân lớp TCP/IP. Các công cụ SSH sẵn có như: OpenSSH,… cung cấp cho người dùng cách thức để thiết lập kết nối mạng được mã hoá để tạo một kênh kết nối riêng tư.

1. Mô hình hoạt động

Ứng dụng được thiết kế với mô hình multi service – Một Server có thể phục vụ nhiều máy client tham gia điều khiển (Trong chương trình nhóm em cho phép tối đa 5 client kết nối đồng th)

Phương pháp giải quyết : Kỹ thuật Multi-thread, Mỗi client khi kết nối với server thì tiến trình sẽ sinh ra một thread tương ứng để phục vụ.

Hình 1: Mô hình hệ thống

1. Các đối tượng tham gia hoạt động

Chỉ có 2 đối tượng chính : CLIENT tác động tới SERVER

Hình 2: Tác nhân tương tác hệ thống

1. Khái quát chức năng của hệ thống
2. Với chức năng trên Server

Hình 3: Chức năng trên server

1. Chức năng trên Client

Hình 4: Chức năng trên client

1. Cài đặt, minh họa chương trình
   1. Cài đặt
   2. Mã hóa dữ liệu trên đường truyền
      1. Giao thức thống nhất khóa Diffie-Hellam

Để thiết lập khóa bí mật chung giữa client và server, nhóm sử dụng giao thức Diffie-Hellam, đây là giao thức phổ biến cho phép client và server thiết lập khóa chung mà không cần bên thứ ba tin cậy.

Phương pháp thực hiện:

* Client và server thống nhất chọn ra 1 số nguyên tố p, một căn nguyên thủy α tức là:
  + {} = {1, 2, 3, …, p-1}
* Client chọn 1 số ngẫu nhiên . Server chọn 1 số ngẫu nhiên .
  + Client giữ bí mật của server giữ bí mật
* Client tính và Server tính
* Client Server:
* Server Client:
* Client tính:
* Server tính:

Như vậy hai bên client và server trao đổi hai giá trị tích lũy thừa của α (với bậc và ) từ đó hai bên cùng tính ra cùng 1 số K. Vì được dữ bí mật và không truyền đi nên K cũng bí mật, tức là hai bên thống nhất chọn K là khóa bí mật chung.

* + 1. Cơ chế mã hóa DES

Sau khi trao chuyển khóa thành công, hai bên thống nhất chọn K là khóa bí mật chung, nhóm sử dụng cơ chế mã hóa DES để mã hóa thông tin trên đường truyển giữa client và server.

Phương pháp thực hiện: Sử dụng bộ thư viện javax.crypto của java.

* 1. Demo chương trình

**Chức năng khởi tạo của server**

**Chức năng kết nối và xác thực trên client**

**Chức năng kết nối khi có quá nhiều client**

**Chức năng nhập lệnh trên client và kết quả trả về**

**Chức năng thoát ( ngắt kết nối giữa client và server )**

Danh mục tham khảo

Retrieved from <http://donbadao.blogspot.com/2014/11/khai-niem-socket-la-gi-va-lap-trinh.html>

Retrieved from <https://vi.wikipedia.org/wiki/Client-server>

Retrieved from <https://vi.wikipedia.org/wiki/SSH>

Retrieved from <https://vi.wikipedia.org/wiki/TC>

Runtime and process in java: <https://www.geeksforgeeks.org/java-lang-runtime-class-in-java/>

socket java example: <https://www.javaworld.com/article/2077322/core-java/core-java-sockets-programming-in-java-a-tutorial.html>

Code DES tham khảo: <https://stackjava.com/demo/code-java-vi-du-ma-hoa-giai-ma-voi-des.html>

Giáo trình cơ sở an toàn thông tin – TS. Nguyễn Khanh Văn.