

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**

----------

**BÁO CÁO**

**Bài 15: Lập trình client/server để trao đổi thông tin an toàn**

***Giảng viên hướng dẫn: Vũ Minh Mạnh***

***Sinh viên thực hiện: Nguyễn Quốc Vượng***

***Mã sinh viên: B21DCAT227***

***Lớp: D21CQAT03-B***

**Hà Nội, 2023**

Môn học Thực tập cơ sở

Bài 15: Lập trình client/server để trao đổi thông tin an toàn

# Mục đích

Sinh viên hiểu về cơ chế client/server và có thể tự lập trình client/server dựa trên socket, sau đó thực hiện ca đặt giao thức đơn giản để trao đổi thông tin an toàn.

# Nội dung thực hành

* + 1. *Tìm hiểu lý thuyết*
       - Tìm hiểu về các khái niệm liên quan tới lập trình socket với TCP
       - Tham khảo tài liệu: Chapter 2: Application Layer V8.1 (9/2020) tại địa chỉ <http://gaia.cs.umass.edu/kurose_ross/ppt.php> (chú ý ví dụ từ trang 105). Một số phiên bản cũ hơn có thể lập trình bằng Java thay vì Python.
* **Socket là gì?**
* **Socket** là điểm cuối của một kết nối hai chiều giữa hai chương trình đang chạy trên mạng. Socket cung cấp cơ chế để truyền và nhận dữ liệu qua mạng.
* **TCP là gì?**
* **TCP (Transmission Control Protocol)** là một giao thức hướng kết nối, đảm bảo việc truyền dữ liệu tin cậy, theo thứ tự và không mất mát. TCP sử dụng cơ chế bắt tay ba bước (three-way handshake) để thiết lập kết nối và đảm bảo dữ liệu được truyền thành công.
* **Các loại socket**
* **Stream Socket (SOCK\_STREAM)**: Dùng cho TCP, đảm bảo truyền dữ liệu liên tục và tin cậy.
* **Datagram Socket (SOCK\_DGRAM)**: Dùng cho UDP, không đảm bảo truyền dữ liệu tin cậy hoặc theo thứ tự.
  + 1. *Chuẩn bị môi trường*
       - Môi trường Python hoặc Java để chạy được ứng dụng client/server đã lập trình.
       - Phần mềm Wireshark
    2. *Các bước thực hiện và kết quả cần đạt*
       1. *Lập trình client và server với TCP socket*

1. *Các bước thực hiện*
   * Lập trình client

A computer screen with a screen and a computer screen

Description automatically generated

* + Lập trình server

A computer screen with a screen and a computer screen

Description automatically generated

* + Chạy server sau đó chạy client
  + Client gửi thông điệp cá nhận hóa cho server: “Hello, I am <mã sinh viên> client.”

A computer screen with a screen and a screen with a screen and a screen with a screen and a screen with a screen and a screen with a screen and a screen with a screen and a screen

Description automatically generated

* + Server nhận được hiển thị thông điệp nhận được và gửi lại client thông điệp: server gửi lại “Hello, I am <mã sinh viên> server”

A computer screen with a screen and a computer screen

Description automatically generated

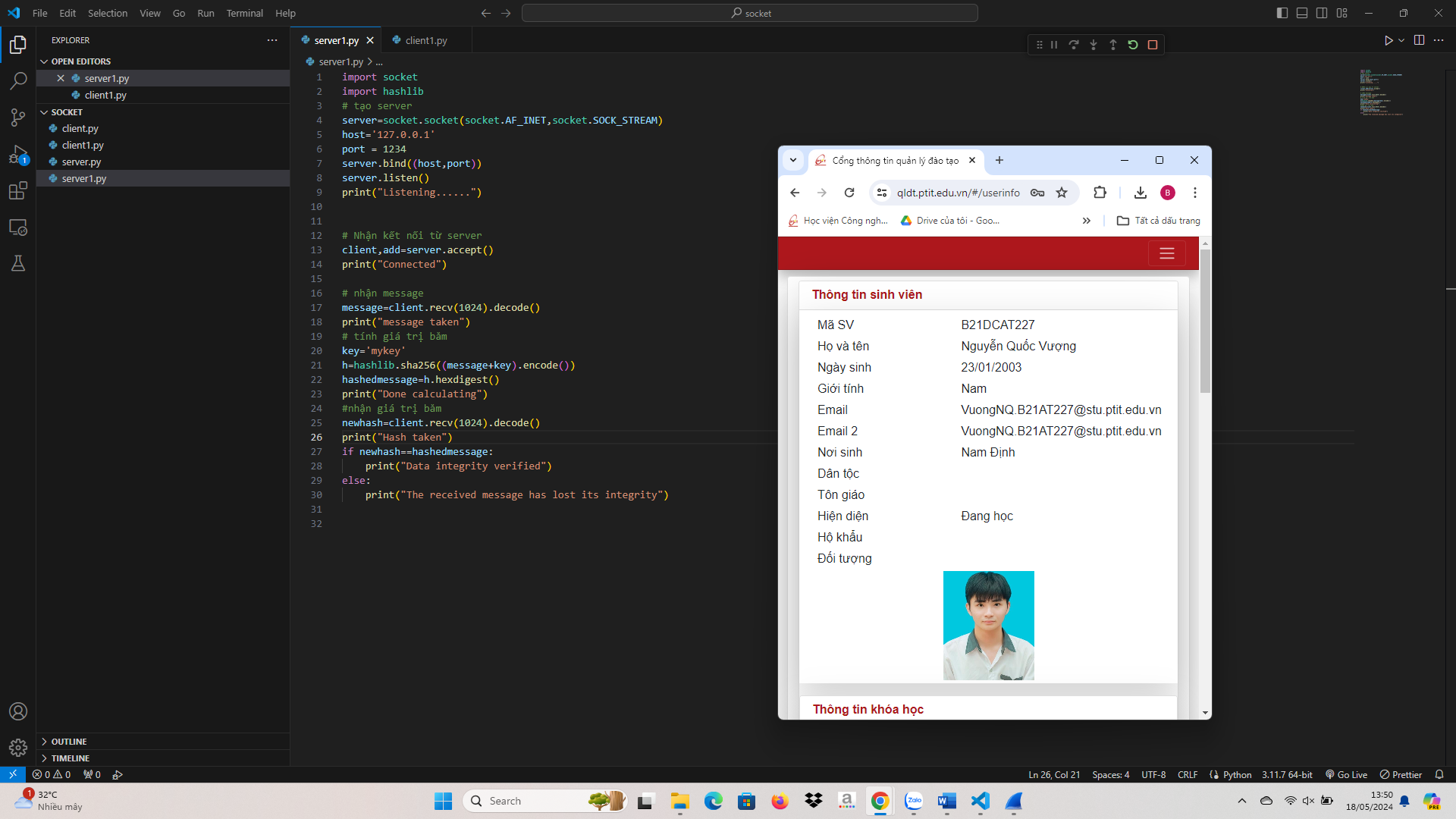
* + Sử dụng Wireshark để bắt các thông tin đã gửi từ client đến server và ngược lại

A screenshot of a computer

Description automatically generated

* + - 1. *Trao đổi thông điệp giữa client và server và đảm bảo tính toàn vẹn của thông điệp khi trao đổi*

1. *Các bước thực hiện*
   * Từ client và server, sửa đổi để sao cho: khi gửi thông điệp sẽ gửi kèm theo giá trị băm của (thông điệp+key) để phía bên kia kiểm tra xác minh tính toàn vẹn. Hai bên có thể thống nhất một giá trị key trước đó.



A computer screen with a screen and a computer screen

Description automatically generated

A computer screen with a screen and a computer screen

Description automatically generated

* + Thay đổi giá trị key tại client và thực hiện gửi lại, nếu không đáp ứng tính toàn vẹn cần thông báo: “The received message has lost its integrity.”

A computer screen with a screen and a screen with a screen and a screen with text

Description automatically generated with medium confidence

* + Bắt được các bản tin trao đổi giữa client và server trong Wireshark

