3. An toàn khi truyền dữ liệu

THỰC HÀNH BẢO MẬT INTERNET OF THINGS – v3.2024

PHỤC VỤ MỤC ĐÍCH GIÁO DỤC
FOR EDUCATIONAL PURPOSE ONLY

A. GIỚI THIỆU TỔNG QUAN

1. Mục tiêu

Trong bài thực hành này, sinh viên sẽ tìm hiểu về các phương pháp để bảo mật dữ liệu khi truyền giữa các thiết bị IoT.

2. Môi trường và thiết bị thực hành

- 02 WeMos D1 (esp8266).
- 02 nút bấm, 06 đèn LED, điện trở, break board, dây dẫn.
- 01 máy ảo sử dụng hệ điều hành Ubuntu/CentOS triển khai các dịch vụ Mosquitto. Sử dụng card mạng Bridge để thiết bị Arduino có thể kết nối đến.

B. NỘI DUNG THỰC HÀNH

Triển khai 02 node, mỗi node bao gồm 1 WeMos D1, 01 nút bấm, 03 đèn led (đỏ, vàng, xanh). Nút bấm được sử dụng để thay đổi thứ tự đèn sáng (tại mỗi thời điểm chỉ có 01 đèn sáng, khi bấm nút sẽ chuyển sang sáng đèn tiếp theo).

luanvt@uit.edu.vn

1. Chứng thực khi tham gia vào MQTT

Giao thức MQTT cung cấp cơ chế xác thực sử dụng USERNAME và PASSWORD. Các MQTT client cần cung cấp thông tin chứng thực khi thiết lập các kết nối đến MQTT broker.

Tên đăng nhập được thể hiện bằng chuỗi ký được được biểu diễn dưới dạng UTF-8. Mật khẩu là một đoạn dữ liệu nhị phân tối đa 65535 byte.

Sinh viên thực hiện các yêu cầu sau:

1. Triển khai MQTT Broker sử dụng dịch vụ Mosquitto có hỗ trợ chứng thực bằng tài khoản đăng nhập và mật khẩu. Thông tin các tài khoản sẽ được lưu trữ trong cơ sở dữ liệu.
2. Sử dụng WeMos D1 kết nối vào MQTT Broker đã triển khai để gửi / nhận dữ liệu bất kỳ.
3. Cho phép điều khiển bật/tắt đèn LED trên tất cả các node *(điều khiển thông qua nút bấm trên mỗi node hoặc gửi thông tin điều khiển vào 1 topic).*
4. Sử dụng phần mềm hoặc công cụ có chức năng bắt gói tin (TCPDUMP, WireShark,…) để quan sát các gói tin được trao đổi trong quá trình thiết lập kết nối và gửi dữ liệu. Từ đó, mô tả ngắn gọn quá trình hoạt động dựa trên những gì quan sát được.

2. Mã hoá kênh truyền TLS/SSL cho MQTT

Transport Layer Security (TLS) và Secure Sockets Layer (SSL) là giao thức mã hoá cung cấp kênh truyền an toàn giữa thiết bị đầu cuối và máy chủ.

Sinh viên thực hiện các yêu cầu sau:

1. Cấu hình MQTT Broker để hỗ trợ mã hoá kênh truyền với TLS / SSL.
2. Sử dụng WeMos D1 kết nối vào MQTT Broker để gửi nhận dữ liệu đảm bảo TLS/SSL đã hoạt động.
3. Cho phép điều khiển bật/tắt đèn LED trên tất cả các node. *(điều khiển thông qua nút bấm trên mỗi node hoặc gửi thông tin điều khiển vào 1 topic).*

4. Sử dụng phần mềm hoặc công cụ có chức năng bắt gói tin (TCPDUMP, WireShark,…) để kiểm chứng dữ liệu không thể bị nghe lén trong quá trình truyền.

3. Mã hoá dữ liệu khi truyền cho MQTT

Mã hoá dữ liệu (payload encryption) được sử dụng như một lớp bảo vệ để đảm bảo an toàn cho dữ liệu khi truyền. Đặc biệt, trong trường hợp không thể triển khai TLS, phương pháp này sẽ hữu dụng để đảm bảo được sự an toàn cho dữ liệu trao đổi với kênh truyền không an toàn. Tuy nhiên, khi áp dụng các phương pháp mã hoá sẽ ảnh hưởng đến khả năng tính toán và năng lượng tiêu hao của các thiết bị IoTs.

Mã hoá giữa thiết bị đầu cuối (End-to-end encryption): Với phương thức này, các thông tin metadata của gói tin sẽ không được mã hoá để sử dụng cho việc định tuyến và xử lý QoS, chỉ phần dữ liệu ứng dụng (payload) sẽ được mã hoá. Lúc này, ngay cả MQTT Broker vẫn không thể giải mã được dữ liệu payload. Chỉ có các client hợp lệ sử dụng đúng khoá mới có thể đọc được dữ liệu được mã hoá.

Mã hoá giữa Client và Broker (Client-to-broker encryption): Phần dữ liệu (payload) sẽ được mã hoá khi truyền thông giữa client và broker. Lúc này, broker sẽ giải mã nội dung trước khi phân phối và tất cả subscriber sẽ nhận dữ liệu không mã hoá.

Lựa chọn phương thức và thuật toán mã hoá phù hợp để mã hoá dữ liệu trước khi truyền. Sinh viên xây dựng một kịch bản sử dụng WeMos D1 và các cảm biến, linh kiện phù hợp để minh hoạ.

4. Giải pháp nâng cao bảo mật

Từ quá trình thực hiện các yêu cầu trên, bạn hãy cho biết các điểm yếu và hạn chế có thể dẫn đến nguy cơ bị kẻ xấu khai thác và tấn công. Giải pháp để nâng cao tính an toàn và phòng tránh tấn công cho hệ thống IoT này.

C. YÊU CẦU NỘP BÀI

Sinh viên hoàn thành tất cả các yêu cầu tại phần B (nội dung thực hành). Thực hiện thêm các yêu cầu mở rộng, nâng cao sẽ có thêm điểm cộng. Khuyến khích sinh viên thực hiện bài thực hành theo nhóm 04 thành viên.

Khi nộp bài, sinh viên cần tuân thủ các quy định sau:

- Báo cáo chi tiết về quá trình thực hiện bằng định dạng docx (Word Document), sử dụng mẫu báo cáo được cung cấp tại Website môn học.
- Báo cáo có thể viết bằng ngôn ngữ tiếng Việt hoặc tiếng Anh. Tuy nhiên không trộn lẫn nhiều ngôn ngữ (ngoại trừ các cụm từ, từ khóa không thể dịch được).
- Đối với các **yêu cầu lập trình** (viết ứng dụng hoặc script), cần đính kèm tất cả mã nguồn và file thực thi (nếu có) khi nộp bài. Trong báo cáo cần giải thích chức năng của các khối mã nguồn quan trọng và ảnh chụp demo quá trình hoạt động.

Không sao chép báo cáo. Nếu phát hiện tình trạng sao chép của nhau (hoặc sử dụng báo cáo của sinh viên từ các khóa trước) để nộp bài sẽ không được chấp nhận.

> **Lưu ý:** Nén file báo cáo và các file liên quan với định dạng **ZIP (.zip)**, đặt tên theo quy tắt sau:
>
> *LabX-NhomX-MSSV1-MSS2-MSSV3.zip*

luanvt@uit.edu.vn