**Chủ đề 5. Nền tảng dịch vụ sản phẩm đa phương tiện (ví dụ: Netflix, Spotify)**

**Kịch bản ứng dụng:**

**1. Lỗ hổng:** Xác định các lỗ hổng bảo mật và lỗ hổng trong cơ chế bảo mật hiện có của các nền tảng dịch vụ sản phẩm đa phương tiện như Netflix hay Spotify.

**2. Lập luận đáng tin cậy cho các khoảng trống:** Cung cấp các lập luận dựa trên bằng chứng hỗ trợ sự tồn tại của các lỗ hổng và lỗ hổng bảo mật đã được xác định, có tham khảo các ví dụ và nghiên cứu điển hình trong thế giới thực.

**3. Động cơ:** Nhấn mạnh động lực quan trọng đằng sau việc bảo mật các nền tảng này, xem xét lượng dữ liệu người dùng, thông tin thanh toán và tài sản trí tuệ khổng lồ mà chúng xử lý.

**4. Các tính năng bảo mật và chức năng mong muốn:**

• Bảo vệ và bảo mật dữ liệu mạnh mẽ.

• Bảo mật xác thực và ủy quyền người dùng.

• Đảm bảo tính toàn vẹn và xác thực của dữ liệu.

• Bảo vệ chống lại các mối đe dọa mạng khác nhau như vi phạm bản quyền và truy cập trái phép.

**5. Các bên liên quan:** Xác định các bên liên quan như nhà cung cấp nội dung, người dùng, cơ quan quản lý và quản trị viên của nền tảng.

**Xác định các thuật toán cụ thể:**

**• Mật mã luồng dựa trên hỗn loạn:**

• Được biết đến với tính không thể đoán trước và tính hiệu quả của mã hóa.

• Thích hợp cho việc truyền phát nội dung đa phương tiện an toàn.

• Áp dụng để đảm bảo bí mật dữ liệu trên nền tảng đa phương tiện.

**• AES (Tiêu chuẩn mã hóa nâng cao):**

• Thuật toán mã hóa đối xứng được công nhận rộng rãi.

• Đảm bảo tính bảo mật và an toàn dữ liệu.

• Lý tưởng cho việc mã hóa và giải mã nội dung được lưu trữ.

**Các giải pháp:**

**Giải pháp xây dựng:**

• Triển khai hệ thống mật mã lai sử dụng Mật mã dòng dựa trên Chaotic và AES.

• Các thành phần bao gồm các mô-đun mã hóa/giải mã, quản lý khóa, xác thực người dùng và cơ chế kiểm soát truy cập.

**Chi tiết các tính năng chức năng:**

**• Mã hóa và giải mã:**

• Mật mã luồng dựa trên hỗn loạn để truyền dữ liệu theo thời gian thực.

• AES cho dữ liệu ở trạng thái nghỉ và trong quá trình truyền.

**• Xác thực và ủy quyền người dùng:**

• Bảo mật đăng nhập người dùng và quản lý phiên.

• Kiểm soát truy cập dựa trên vai trò để phân phối nội dung.

**Chi tiết các tính năng bảo mật:**

**• Bảo mật:**

• Cơ chế mã hóa mạnh mẽ để bảo vệ tính bí mật của nội dung đa phương tiện.

**• Xác thực:**

• Bảo mật quy trình xác thực người dùng để xác minh danh tính của người dùng và ngăn chặn truy cập trái phép.

**• Chính trực:**

• Đảm bảo tính toàn vẹn dữ liệu để ngăn chặn giả mạo hoặc sửa đổi nội dung đa phương tiện.

**Triển khai và thử nghiệm:**

**Khuyến nghị về công cụ hoặc thư viện:**

• Sử dụng các ngôn ngữ lập trình như Python, Java hoặc C++ để triển khai.

• Sử dụng các thư viện mật mã như PyCryptodome cho các ứng dụng .

Stream Cipher và các thư viện AES hiện có.

• Tiến hành thử nghiệm bằng cách sử dụng các nền tảng như Jupyter Notebook để phát triển mã.

**Kịch bản thử nghiệm:**

• Mô phỏng truyền tải nội dung đa phương tiện theo thời gian thực.

• Kiểm tra mã hóa AES đối với dữ liệu ở trạng thái lưu trữ.

**Mục tiêu và tiến hành kiểm tra:**

• Mục tiêu: Đảm bảo rằng hệ thống mã hóa kết hợp bảo mật nội dung đa phương tiện một cách hiệu quả và ngăn chặn truy cập trái phép.

• Chỉ đạo:

• Kiểm tra phát trực tuyến theo thời gian thực để đánh giá hiệu suất của Mật mã luồng dựa trên hỗn loạn.

• Kiểm tra tính toàn vẹn dữ liệu đối với nội dung được mã hóa AES ở trạng thái lưu trữ.

**Triển khai:**

• Triển khai hệ thống mã hóa kết hợp trong môi trường được kiểm soát để đánh giá hiệu suất và tính bảo mật trong thế giới thực của nó.

Người giới thiệu:

• Trích dẫn các tài liệu học thuật, sách giáo khoa và các bài báo nghiên cứu về Mật mã dòng dựa trên hỗn loạn,

AES và bảo mật nền tảng đa phương tiện.

**Phiếu tự đánh giá:**

**1. Chất lượng nghiên cứu (15%):** Học sinh đã xác định và biện minh những lỗ hổng trong bảo mật của nền tảng đa phương tiện tốt đến mức nào.

**2. Lựa chọn thuật toán (10%):** Tính phù hợp và căn cứ cho việc lựa chọn Mật mã luồng dựa trên hỗn loạn và AES.

**3. Kiến trúc giải pháp (15%):** Sự rõ ràng và hiệu quả của thiết kế hệ thống mật mã lai.

**4. Tính năng chức năng (20%):** Hiệu quả của các tính năng mã hóa, xác thực và ủy quyền.

**5. Tính năng bảo mật (20%):** Học sinh giải quyết các vấn đề về bảo mật, xác thực và tính toàn vẹn tốt đến mức nào.

**6. Triển khai và thử nghiệm (10%):** Tính hiệu quả của quá trình thử nghiệm và sự phù hợp của nó với giải pháp được đề xuất.

**7. Trình bày và Tài liệu (10%):** Sự rõ ràng, tổ chức và chất lượng của tài liệu trình bày và tài liệu dự án.