HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA CÔNG NGHỆ THÔNG TIN

BÀI TẬP MÔN HỌC CƠ SỞ AN TOÀN BẢO MẬT THÔNG TIN

VIẾT CHƯƠNG TRÌNH QUẢN LÝ DỮ LIỆU AN TOÀN DƯỚI DẠNG MẶT NẠ DỮ LIỆU TRÊN SQLITE SỬ DỤNG NGÔN NGỮ RUST

Ngành: Công nghệ thông tin
Chuyên ngành: Kỹ thuật phần mềm nhúng và di động

Người hướng dẫn
TS.Nguyễn Đào Trường
Khoa Công nghệ thông tin - Học viện Kỹ thuật mật mã

Nhóm sinh viên thực hiện:
Phạm Thị Phương Anh CT040401
Phạm Văn Dũng CT040308
Lớp L01

Hà Nội - 2022

LỜI NÓI ĐẦU

Ngày nay với sự phát triển mạnh mẽ của công nghệ thông tin, đặt biệt là sự phát triển của mạng Internet, ngày càng có nhiều dữ liệu lớn được sản sinh và lưu trữ, bảo vệ quyền riêng tư và đảm bảo an toàn thông tin ngày càng trở nên cấp thiết hơn bao giờ hết. Trong thực tế nhiều dữ liệ quan trọng và nhạy cảm được lưu trữ trong các hệ thống máy tính, cơ sở dữ liệu, ứng dụng web và ứng dụng di động, tạo ra mối đe dọa đến quyền riêng tư của người dùng.

Để giải quyết vấn đề này, mặt nạ dữ liệu (Data Masking) đã trở thành một trong những kỹ thuật phổ biến để bảo vệ dữ liệu nhạy cảm và đảm bảo an toàn thông tin. Kỹ thuật này cho phép ẩn danh hoặc che giấu dữ liệu trong một tập dữ liệu, giúp đảm bảo những thông tin này không bị tiết lộ và được bảo vệ.

Với mong muốn tìm hiểu về Data Masking, nhóm thực hiện báo cáo với đề tài: "**Viết chưng trình quản lý dữ liệu an toàn dưới dạng mặt nạ dữ liệu trên SQLITE sử dụng ngôn ngữ Rust**". Với mục tiêu trên, báo cáo bao gồm các chương và bố cục sau:

Chương 1: Tổng quan về an toàn và bảo mật thông tin
Chương 2: Xây dựng chương trình
Chương 3: Kết luận và đánh giá

Hà Nội, ngày 04 tháng 11 năm 2022

Nhóm sinh viên thực hiện

MỤC LỤC

LỜI NÓI ĐẦU i

MỤC LỤC ii

DANH SÁCH HÌNH VẼ iv

DANH SÁCH BẢNG v

DANH SÁCH KÝ HIỆU VÀ CHỮ VIẾT TẮT vi

1 GIỚI THIỆU TỔNG QUAN 1

1.1 Tổng quan về an toàn và bảo mật thông tin . . . 1

1.1.1 Khái niệm mở đầu . . . 1

1.1.2 Các mối đe dọa và thiệt hại . . . 1

1.1.3 Giải pháp điều khiển và kiểm soát . . . 2

1.1.4 Mục tiêu và nguyên tắc chung . . . 2

1.1.5 Ba mục tiêu . . . 2

1.1.6 Hai nguyên tắc . . . 2

1.1.7 Giải pháp . . . 2

1.2 Mặt nạ dữ liệu . . . 2

1.3 Mã hóa dữ liệu . . . 2

1.4 Trao đổi khóa Diffie-Hellman và Elliptic-curve Diffie-Hellman . . . 2

1.4.1 Trao đổi khóa Diffie-Hellman . . . 2

1.4.2 Mật mã đường cong Elliptic . . . 3

1.4.3 Trao đổi khóa Diffie-Hellman trên đường cong elliptic . . . 3

1.5 Hệ mã dòng có xác thực ChaCha20-Poly1305 . . . 3

1.5.1 Hệ mã dòng ChaCha20 . . . 3

1.5.2 Mã xác thực Poly1305 . . . 3

1.6 Hàm băm BLAKE2s . . . 3

2 THIẾT KẾ HỆ THỐNG 4

2.1 asdf . . . 4

3 THỬ NGHIỆM - ĐÁNH GIÁ **5**
3.1 Sản phẩm thực tế 5
3.2 Thử nghiệm chức năng 5
3.3 Thử nghiệm hiệu năng, tốc độ 5
3.4 Đánh giá hệ thống 5

DANH SÁCH HÌNH VẼ

DANH SÁCH BẢNG

DANH SÁCH KÝ HIỆU VÀ CHỮ VIẾT TẮT

DH Diffie-Hellman 2

Chương 1: GIỚI THIỆU TỔNG QUAN

1.1 Tổng quan về an toàn và bảo mật thông tin

1.1.1 Khái niệm mở đầu

Ngày nay với sự phát triển bùng nổ của công nghệ thông tin, hầu hết các thông tin của doanh nghiệp như chiến lược kinh doanh, các thông tin về khách hàng, nhà cung cấp, tài chính, mức lương nhân viên,…đều được lưu trữ trên hệ thống máy tính. Cùng với sự phát triển của doanh nghiệp là những đòi hỏi ngày càng cao của môi trường kinh doanh yêu cầu doanh nghiệp cần phải chia sẻ thông tin của mình cho nhiều đối tượng khác nhau qua Internet hay Intranet. Việc mất mát, rò rỉ thông tin có thể ảnh hưởng nghiêm trọng đến tài chính, danh tiếng của công ty và quan hệ với khách hàng.

Hệ thống thông tin là một hệ thống bao gồm các yếu tố có quan hệ với nhau cùng làm nhiệm vụ thu thập, xử lý, lưu trữ và phân phối thông tin và dữ liệu và cung cấp một cơ chế phản hồi để đạt được một mục tiêu định trước. Các thành phần của hệ thống bao gồm phần cứng, phần mềm, mạng truyền dữ liệu, dữ liệu và con người trong hệ thống thông tin.

Các phương thức tấn công thông qua mạng ngày càng tinh vi, phức tạp có thể dẫn đến mất mát thông tin, thậm chí có thể làm sụp đổ hoàn toàn hệ thống thông tin của doanh nghiệp. Vì vậy an toàn và bảo mật thông tin là nhiệm vụ rất nặng nề và khó đoán trước được, nhưng tựu trung lại gồm ba hướng chính:

- Bảo đảm an toàn thông tin tại máy chủ
- Bảo đảm an toàn cho phía máy trạm
- Bảo mật thông tin trên đường truyền

1.1.2 Các mối đe dọa và thiệt hại

Ba mối đe dọa chủ yếu đối với hệ thống:

- Phá hoại: kẻ thù phá hỏng thiết bị phần cứng hoặc phần mềm hoạt động trên hệ.
- Sửa đổi: tài sản của hệ thống bị sửa đổi trái phép. Điều này thường làm cho hệ thống không hoạt động đúng chức năng của nó. Ví dụ như thay đổi mật khẩu, quyền người dùng làm họ không thể truy cập vào hệ thống để làm việc.

- Can thiệp: Tài sản bị truy cập bởi những người không có thẩm quyền, các truyền thông thực hiện trên hệ thống bị ngăn chặn, sửa đổi. thống

1.1.3 Giải pháp điều khiển và kiểm soát

1.1.4 Mục tiêu và nguyên tắc chung

1.1.5 Ba mục tiêu

1.1.6 Hai nguyên tắc

Tấn công mạng là một trong những vấn đề quan trọng về an toàn và bảo mật thông tin. Đó là những nỗ lực của kẻ tấn công để truy cập vào các hệ thống mạng của một tổ chức hoặc cá nhân mà không có sự cho phép. Những tấn công mạng này có thể gây ra những thiệt hại nghiêm trọng cho các tổ chức hoặc cá nhân, bao gồm mất dữ liệu, mất tiền và thiệt hại đến danh tính.

Phần mềm độc hại: Phần mềm độc hại là một loại phần mềm được thiết kế để gây hại cho hệ thống máy tính hoặc để truy cập vào thông tin cá nhân. Các loại phần mềm độc hại bao gồm virus, phần mềm giám điệp, phần mềm mã độc và phần mềm ransonware.

Xâm nhập: Xâm nhập là quá trình xâm nhập vào hệ thống hoặc mạng của một tổ chức hoặc cá nhân mà không có sự cho phép. Các tấn công xâm nhập này có thể gây ra những thiệt hại nghiêm trọng cho các tổ chức hoặc cá nhân, bao gồm mất dữ liệu và thiệt hại đến danh tiếng.

Lừa đảo trực tuyến: Lừa đảo trực tuyến là một hoạt động gian lận trực tuyến được thực hiện bằng cách sử dụng các kỹ thuật gian lận để lừa đảo người dùng đưa ra thông tin cá nhân hoặc tiền bạc.

Rò rỉ dữ liệu: Rò rỉ dữ liệu là quá trình tiết lộ thông tin cá nhân hoặc thông tin nhạy cảm của một cá nhân hoặc tổ chức cho người không có quyền truy cập vào thông tin đó. Rò rỉ dữ liệu có thể gây ra những thiệt hại nghiêm trọng cho các tổ chức hoặc cá nhân.

1.1.7 Giải pháp

1.2 Mặt nạ dữ liệu

1.3 Mã hóa dữ liệu

1.4 Trao đổi khóa Diffie-Hellman và Elliptic-curve Diffie-Hellman

1.4.1 Trao đổi khóa Diffie-Hellman

Diffie-Hellman (DH) là abc abc

1.4.2 Mật mã đường cong Elliptic

1.4.3 Trao đổi khóa Diffie-Hellman trên đường cong elliptic

1.5 Hệ mã dòng có xác thực ChaCha20-Poly1305

1.5.1 Hệ mã dòng ChaCha20

1.5.2 Mã xác thực Poly1305

1.6 Hàm băm BLAKE2s

Chương 2: THIẾT KẾ HỆ THỐNG

2.1 asdf

Chương 3: THỬ NGHIỆM - ĐÁNH GIÁ

3.1 Sản phẩm thực tế

3.2 Thử nghiệm chức năng

3.3 Thử nghiệm hiệu năng, tốc độ

3.4 Đánh giá hệ thống