


THÔNG TIN CHUNG CỦA BÁO CÁO

- Link YouTube video của báo cáo (tối đa 5 phút): <https://youtu.be/ht5F-yxt3MI>
- Link slides (dạng .pdf đặt trên Github):
<https://github.com/lvnguyenit/CS2205.APR2023/blob/main/Nguy%C3%AAn%20L%C3%A2m%20V%C4%A9nh%20-%20xCS2205.DeCuong.FinalReport.Template.Slide.pdf>
- *Mỗi thành viên của nhóm điền thông tin vào một dòng theo mẫu bên dưới*
- *Sau đó điền vào Đề cương nghiên cứu (tối đa 5 trang), rồi chọn Turn in*

<ul style="list-style-type: none">● Họ và Tên: Lâm Vĩnh Nguyên● MSHV: 230202029 	<ul style="list-style-type: none">● Lớp: CS2205.APR2023● Tự đánh giá (điểm tổng kết môn): 8.5/10● Số buổi vắng: 1● Số câu hỏi QT cá nhân: 0● Link Github: https://github.com/lvnguyenit/CS2205.APR2023
--	---

ĐỀ CƯƠNG NGHIÊN CỨU

TÊN ĐỀ TÀI (IN HOA)

NGHIÊN CỨU VÀ PHÁT TRIỂN ỨNG DỤNG XÁC THỰC KHÔNG MẬT KHẨU CHO QUẢN LÝ MẬT KHẨU TẬP TRUNG

TÊN ĐỀ TÀI TIẾNG ANH (IN HOA)

RESEARCH AND DEVELOPMENT OF PASSWORDLESS AUTHENTICATION APPLICATION FOR CENTRALIZED PASSWORD MANAGEMENT

TÓM TẮT

Trong thời đại kỹ thuật số hiện nay, mỗi người sử dụng Internet đều phải quản lý nhiều tài khoản đăng nhập khác nhau. Tuy nhiên, việc tạo và ghi nhớ nhiều mật khẩu không phải là điều dễ dàng đối với đa số người dùng, đặc biệt là khi phải nhớ nhiều mật khẩu dài và phức tạp cho từng trang web hoặc ứng dụng khác nhau.

Đề tài này tập trung vào việc **nghiên cứu và phát triển một ứng dụng xác thực không mật khẩu cho quản lý mật khẩu tập trung**. Giải pháp này nhằm mục đích giải quyết các vấn đề liên quan đến việc sử dụng mật khẩu yếu hoặc sử dụng 01 mật khẩu cho nhiều ứng dụng. Bằng cách **tạo ra một phần mềm quản lý mật khẩu**, cho phép người dùng tạo mật khẩu ngẫu nhiên với độ phức tạp cao, lưu trữ mật khẩu hiện có của họ một cách an toàn và tiện lợi. Thay vì nhớ mật khẩu cho từng trang web, **người dùng chỉ cần xác thực bằng các phương thức không mật khẩu** như xác thực vân tay, nhận dạng khuôn mặt.

Qua việc áp dụng giải pháp này, người dùng sẽ trải nghiệm tiện lợi hơn trong việc quản lý mật khẩu, đồng thời tăng cường tính bảo mật cho các tài khoản trực tuyến. Ngoài ra, việc sử dụng các phương thức xác thực không mật khẩu cũng giảm thiểu rủi ro tấn công từ các kỹ thuật tấn công dựa trên mật khẩu, hoặc phishing. Điều này mang lại lợi ích to lớn cho người dùng trong việc giảm thiểu rủi ro bị xâm nhập tài khoản.

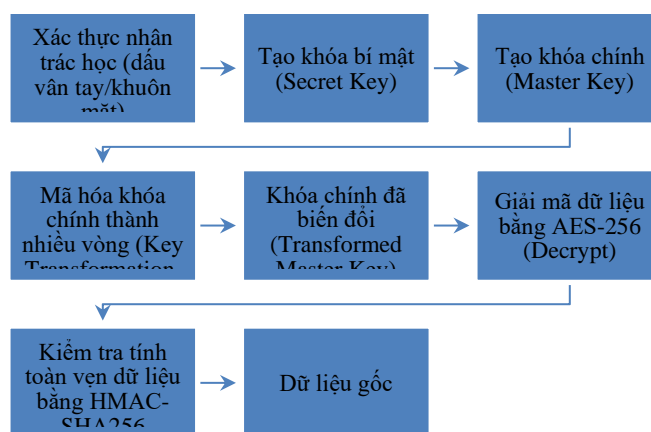
GIỚI THIỆU

Trong thời đại kỹ thuật số ngày nay, một trong những thách thức lớn mà người dùng

Internet phải đối mặt là việc quản lý mật khẩu. Với sự gia tăng nhanh chóng của các ứng dụng và dịch vụ trực tuyến, mỗi cá nhân thường phải sở hữu nhiều tài khoản và mật khẩu riêng biệt cho mục đích sử dụng hàng ngày.

Tuy nhiên, việc quản lý nhiều mật khẩu không chỉ là một công việc phiền toái mà còn tạo ra nhiều rủi ro về bảo mật. Sử dụng mật khẩu yếu hoặc dễ đoán có thể dễ dàng bị tấn công bởi hacker. Trong khi đó, sử dụng mật khẩu mạnh và phức tạp lại gây ra vấn đề về khả năng ghi nhớ và quản lý cho người dùng.

Để giải quyết vấn đề này, nghiên cứu và phát triển một ứng dụng xác thực không mật khẩu cho quản lý mật khẩu tập trung trở thành một lựa chọn hợp lý. Đây là một hướng tiếp cận tiên tiến, đi theo xu hướng xác thực mới là chuyển từ "thông tin người dùng nắm giữ" như mật khẩu sang "thông tin chỉ người dùng sở hữu", như sinh trắc học vân tay, khuôn mặt. Mục tiêu của đề tài là tạo ra một ứng dụng an toàn và thuận tiện cho việc quản lý mật khẩu. Thay vì nhớ hàng tá mật khẩu, người dùng chỉ cần sử dụng các phương thức xác thực “người dùng sở hữu” - không mật khẩu như nhận dạng vân tay, nhận dạng khuôn mặt, để truy cập các tài khoản và dịch vụ trực tuyến. Quy trình mã hóa và giải mã được mô tả bên dưới:



Trong phạm vi của đề tài này, chúng tôi tập trung vào việc nghiên cứu và phát triển một ứng dụng xác thực không mật khẩu, nhằm tối ưu hóa tính bảo mật và tính tiện lợi cho người dùng. Chúng tôi tin rằng giải pháp này không chỉ giúp người dùng bảo vệ thông tin cá nhân một cách hiệu quả hơn mà còn mang lại trải nghiệm trực tuyến an toàn và thuận tiện hơn, đồng thời đóng góp tích cực vào việc xây dựng một môi trường Internet an toàn và bảo mật hơn cho mọi người.

MỤC TIÊU

Sau khi hoàn thành, đề tài sẽ đáp ứng được các yêu cầu sau:

1. **Tối ưu hóa tính bảo mật:** Nghiên cứu các thuật toán/cơ chế mã hóa phù hợp đối với mật khẩu, để đảm bảo rằng thông tin người dùng được bảo vệ an toàn và không thể khôi phục nếu không xác thực được bằng nhân trắc học. Sự tập trung vào tính bảo mật sẽ giúp xây dựng niềm tin từ phía người dùng và giảm thiểu nguy cơ mất dữ liệu.
2. **Phát triển ứng dụng xác thực không mật khẩu:** Xây dựng một ứng dụng hoạt động hiệu quả, cho phép người dùng quản lý mật khẩu một cách an toàn và tiện lợi thông qua phương thức xác thực không mật khẩu, như vân tay, nhận dạng khuôn mặt.
3. **Giao diện thân thiện và an toàn:** Phát triển một ứng dụng có giao diện trực quan, dễ hiểu và dễ sử dụng, giúp người dùng dễ dàng thực hiện các thao tác quản lý mật khẩu mà không gặp phải khó khăn. Đảm bảo rằng ứng dụng hoạt động một cách mượt mà và nhanh chóng, không gây ra sự chậm trễ khi truy cập và quản lý mật khẩu. Đồng thời ứng dụng cũng có thể tự động phát hiện URL đã được đăng ký trước đó, tự động điền mật khẩu. Điều này sẽ giảm thiểu nguy cơ người dùng bị phishing khi truy cập vào website giả mạo, có giao diện giống với website thật. Sự tập trung vào trải nghiệm người dùng sẽ giúp tăng cường sự chấp nhận và sử dụng rộng rãi của ứng dụng.

NỘI DUNG VÀ PHƯƠNG PHÁP

Nội dung:

Để giải quyết các mục tiêu của đề tài nêu ra, chúng tôi sử dụng kết hợp 02 giải pháp là Keeweb và FIDO2.

Keeweb là một ứng dụng quản lý mật khẩu mã nguồn mở, hỗ trợ định dạng tệp KeePass (KDBX). Nó cho phép người dùng lưu trữ và quản lý mật khẩu của họ một cách an toàn thông qua một tệp mã hóa, truy cập được từ nhiều thiết bị và nền tảng khác nhau. Keeweb cung cấp nhiều tính năng bảo mật như mã hóa AES-256, kiểm tra tính

mạnh của mật khẩu và tích hợp với các dịch vụ đám mây như Dropbox, Google Drive, OneDrive.

FIDO2 là một tập hợp các tiêu chuẩn do FIDO Alliance phát triển nhằm cải thiện bảo mật xác thực trực tuyến bằng cách giảm sự phụ thuộc vào mật khẩu. FIDO2 bao gồm hai thành phần chính: WebAuthn và CTAP. FIDO2 sử dụng các phương pháp xác thực mạnh mẽ như khóa bảo mật phần cứng và sinh trắc học mà không cần mật khẩu.

Điểm mới của đề tài là **tích hợp FIDO2 vào Keeweb để tận dụng ưu điểm trong xác thực không mật khẩu của FIDO2 vào quản lý mật khẩu tập trung của Keeweb.**

Việc sử dụng Keeweb có thể giải quyết yêu cầu về tối ưu hóa tính bảo mật, và giao diện người dùng. Các mật khẩu và thông tin nhạy cảm được lưu trữ trong các tệp tin .kdbx, đảm bảo rằng chỉ người dùng có khóa giải mã mới có thể truy cập - khóa này sẽ được xác thực bằng FIDO2 thông qua dấu vân tay. Bên cạnh đó, Keeweb cung cấp một giao diện người dùng trực quan, dễ sử dụng, hỗ trợ kéo và thả, tìm kiếm nhanh, và các tính năng quản lý nhóm mật khẩu.

Phương pháp:

- **Thiết lập môi trường thử nghiệm:** Cài đặt Keeweb trên các hệ điều hành, cụ thể là Windows. Sử dụng các thiết bị FIDO2 từ nhiều nhà cung cấp khác nhau, trong đề tài này chúng tôi chọn thiết bị từ Yubico và VinCSS.
- **Các bước thực hiện:** Chuẩn bị tập tin mẫu .kdbx với nhiều mật khẩu đa dạng để thử nghiệm. Đăng ký dấu vân tay với thiết bị FIDO2, sau đó tích hợp với Keeweb để xem dấu vân tay như là “Master Password”.
- **So sánh khả năng bảo mật của Keeweb giữa xác thực Master Password qua FIDO2 với xác thực theo cách truyền thống:** So sánh dựa trên khả năng Master Password bị tấn công brute-force, khả năng bảo vệ giữa các cuộc tấn công phishing, khả năng phòng chống tấn công man-in-the-middle.
- **Đánh giá thời gian xác thực, độ tin cậy và trải nghiệm người dùng:** Đo lường thời gian cần thiết để đăng nhập vào Keeweb giữa việc thông qua FIDO2 và nhập mật khẩu theo cách truyền thống. Đánh giá độ tin cậy của quá trình xác thực thông qua nhiều lần thử nghiệm khác nhau. Ghi nhận về trải nghiệm người dùng về sự tiện

lợi của FIDO2 so với việc xác thực Master Password bằng mật khẩu.

KẾT QUẢ MONG ĐỢI

Trong phạm vi nghiên cứu và phát triển của đề tài, chúng tôi mong đợi ứng dụng sau khi hoàn thành sẽ được các kết quả sau:

1. **Tính bảo mật cao:** Chúng tôi kỳ vọng rằng sau khi triển khai, ứng dụng sẽ đạt được một mức độ bảo mật cao, đảm bảo rằng thông tin cá nhân và mật khẩu của người dùng được bảo vệ an toàn khỏi các mối đe dọa mạng và tấn công.
2. **Trải nghiệm người dùng tốt:** Chúng tôi mong đợi rằng giao diện người dùng sẽ được thiết kế một cách thân thiện và dễ sử dụng, giúp người dùng quản lý mật khẩu một cách hiệu quả và tiện lợi. Phản hồi tích cực từ người dùng về trải nghiệm sử dụng sẽ là một chỉ số quan trọng cho sự thành công của dự án.
3. **Đóng góp vào sự phát triển công nghệ:** Cuối cùng, chúng tôi mong đợi rằng đề tài sẽ đóng góp vào sự phát triển của công nghệ bảo mật và quản lý mật khẩu, đồng thời mang lại giá trị và lợi ích cho cộng đồng người dùng trực tuyến.

TÀI LIỆU THAM KHẢO

- [1]. Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, Sven Bugiel: Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. 2020 IEEE Symposium on Security and Privacy (SP). 2020: 1-5
- [2]. Mohammed Aziz Al Kabir, Wael Elmedany: An Overview of the Present and Future of User Authentication. 2022 4th IEEE Middle East and North Africa COMMunications Conference (MENACOMM). 2022
- [3]. Sumedh Ashish Dixit, Arnav Gupta, Ratnesh Jain, Rahul Joshi, Sudhanshu Gonge & Ketan Kotecha. FIDO2 Passwordless Authentication for Remote Devices.
- [4]. Wagner, P., Heid, K., Heider, J.: Remote WebAuthn: FIDO2 authentication for less accessible devices (2021). Networks and Systems in Cybernetics (CSOC 2023). 2023:349–362