


THÔNG TIN CHUNG CỦA BÁO CÁO

- Link YouTube video của báo cáo (tối đa 5 phút):

<https://www.youtube.com/watch?v=mm3k2VA3pLM>

- Link slides (dạng .pdf đặt trên Github):

<https://github.com/tvhoang2012/CS2205/blob/main/T%E1%BA%A1%20Vi%E1%BB%87t%20Ho%C3%A0ng%20%20-%20xCS2205.DeCuong.FinalReport.Slide.pdf>

<ul style="list-style-type: none">• Họ và Tên: Tạ Việt Hoàng• MSSV: 220202018 	<ul style="list-style-type: none">• Lớp: CS2205.APR2023• Tự đánh giá (điểm tổng kết môn): 9.75/10• Số buổi vắng: 0• Số câu hỏi QT cá nhân:• Số câu hỏi QT của cả nhóm: 10• Link Github: https://github.com/tvhoang2012/CS2205/
---	--

ĐỀ CƯƠNG NGHIÊN CỨU

TÊN ĐỀ TÀI (IN HOA)

XÁC THỰC ĐA YẾU TỐ VÀ THỎA THUẬN KHÓA PHIÊN TRONG MÔ HÌNH MẠNG ĐA MÁY CHỦ

TÊN ĐỀ TÀI TIẾNG ANH (IN HOA)

MULTI-FACTOR AUTHENTICATION AND KEY AGREEMENT PROTOCOL FOR MULTI-SERVER ENVIRONMENTS

TÓM TẮT (Tối đa 400 từ)

Đề tài nghiên cứu tập trung vào việc triển khai và đánh giá hiệu quả của các phương pháp xác thực đa yếu tố nhằm tăng cường tính bảo mật và hiệu quả trong quá trình xác thực. Các yếu tố xác thực được sử dụng bao gồm mật khẩu sử dụng một lần (TOTP), sinh trắc học (như vân tay), sinh trắc thiết bị dựa trên hệ điều hành và phần cứng, cùng với việc sử dụng module phần cứng hỗ trợ như TPM.

Nghiên cứu cũng tập trung vào xác thực đa yếu tố trong môi trường multi-server, đảm bảo tính ẩn danh cho người dùng. Điều này giúp người dùng truy cập vào các máy chủ khác nhau mà không tiết lộ danh tính của họ.

Đề tài được triển khai thực nghiệm trong Telecare Medical Information System, hệ thống thông tin y tế trực tuyến. Bằng cách áp dụng các phương pháp xác thực đa yếu tố trong hệ thống này, mong đợi đạt được tăng cường tính bảo mật, đáp ứng yêu cầu cao về bảo mật và độ tin cậy của dữ liệu y tế. Cuối cùng, đánh giá hiệu quả và bảo mật của các phương pháp xác thực đa yếu tố được tiến hành để xác định khả năng đáp ứng và đảm bảo tính toàn vẹn của hệ thống. Kết quả dự kiến từ nghiên cứu này là tăng cường tính bảo mật, tính hiệu quả và bảo vệ thông tin và quyền riêng tư của người dùng trong quá trình xác thực.

GIỚI THIỆU (Tối đa 1 trang A4)

Trong thời đại hiện nay, bất kỳ ai ở bất kỳ nơi nào trên thế giới cũng có thể sử dụng các dịch vụ như làm việc từ xa, giám sát từ xa, mua hàng trực tuyến và các tính năng

khác thông qua các tiện ích thông minh có kết nối internet. Nhưng việc kết nối thông qua internet được coi là không an toàn do vì tồn tại các rủi ro về bảo mật thông tin. Để tránh những rủi ro như vậy thì xác thực bảo vệ khóa phiên được coi là một trong những giải pháp tốt nhất để xây dựng các kênh truyền tải dữ liệu an toàn. Nhiều mô hình xác thực bảo vệ khóa phiên đã được đề xuất nhưng vẫn tồn tại các lỗ hổng như là: privileged insider attack [1], impersonation attack [1], Để giải quyết các lỗ hổng này nhiều mô hình mới với việc tăng cường factor xác thực đã được đề xuất [1]. Xác thực là một biện pháp bảo vệ cơ bản chống lại việc truy cập bất hợp pháp vào thiết bị hoặc các ứng dụng nhạy cảm khác cho dù là ngoại tuyến hoặc trực tuyến. Cơ chế xác thực hiện tại phổ biến nhất là Single-Factor Authentication (SFA) chỉ dựa vào duy nhất là mật khẩu, nhưng rõ ràng đây là mức xác thực yếu nhất rất dễ bị kẻ tấn công khai thác để thực hiện các kỹ thuật tấn công xã hội, tấn công từ điển, ...

Do đó, việc triển khai xác thực nhiều yếu tố (Multi-factor Authentication hay MFA) là rất quan trọng. MFA sẽ sử dụng thêm hai lớp bảo mật bổ sung để đảm bảo những người đang cố gắng truy cập vào tài khoản trực tuyến là chính họ. Đầu tiên, người dùng vẫn sẽ cần mật khẩu để truy cập. Sau đó, thay vì ngay lập tức có được quyền truy cập, họ được yêu cầu cung cấp thêm một thông tin khác. Yếu tố thứ hai này có thể là:

- Knowledge factor (1): có thể là mã PIN, một câu hỏi bí mật
- Ownership factor (2): có thể là thẻ thông minh, điện thoại thông minh, phần cứng nhỏ.
- Biometric factor (3): gồm các mẫu sinh trắc học như vân tay, móng mắt, võng mạc.

Mật khẩu dùng một lần, bao gồm TOTP, là yếu tố "Ownership factor" giúp tăng tính bảo mật cho tài khoản người dùng. Đối với biometric factor để bảo vệ mẫu sinh trắc học và xác thực cụ thể là vân tay thì có 2 phương pháp phổ biến là biohashing [2] và fuzzy extractor [3]. Ngoài ra, cũng có thể sử dụng sinh trắc thiết bị (device fingerprint) dựa trên hệ điều hành, phần cứng máy tính: cpu, gpu,... nhằm tăng cường tính bảo mật trong việc xác thực [4]. Xác thực đa yếu tố cũng được sử dụng trong việc xác thực lẫn nhau, trao đổi khóa và đảm bảo quyền riêng tư của người dùng [5].

Trong nghiên cứu này ,tác giả nghiên cứu một số cách xác thực đa yếu tố nhằm tăng cường tính bảo mật và tính hiệu quả của xác thực đa yếu tố. Qua đó, tác giả triển khai thực nghiệm theo kịch bản thực tế và đánh giá tính hiệu quả của các cách xác thực đa yếu tố.

MỤC TIÊU

- Tìm hiểu về xác thực đa yếu tố dựa trên mật khẩu, TOTP, xác thực và bảo vệ các mẫu sinh trắc học.
- Tìm hiểu về cách xác thực sử dụng sinh trắc của thiết bị (Device Fingerprints) và cách sử dụng module phần cứng (Hardware Assisted) để bảo vệ các thông tin dùng trong xác thực.
- Triển khai thực nghiệm và đánh giá tính hiệu quả trong việc xác thực trong Telecare Medical Information System

NỘI DUNG VÀ PHƯƠNG PHÁP

1. Nội dung chi tiết

1.1 Nghiên cứu các yếu tố sử dụng trong xác thực:

- Mật khẩu sử dụng một lần: Sử dụng mật khẩu dựa trên thời gian (TOTP) để đảm bảo tính duy nhất và tăng cường bảo mật trong quá trình xác thực.
- Sinh trắc học (vân tay): Sử dụng kỹ thuật Biohashing và Fuzzy-extractor để bảo vệ và xác thực các mẫu sinh trắc học như vân tay.
- Sinh trắc thiết bị dựa trên hệ điều hành và phần cứng: Sử dụng thông tin từ hệ điều hành và phần cứng máy tính (GPU, CPU) để xác thực người dùng và tăng cường tính bảo mật.
- Module phần cứng hỗ trợ: Sử dụng TPM (Trusted Platform Module) để đảm bảo tính toàn vẹn và bảo mật thông tin trong quá trình xác thực.

1.2 Nghiên cứu các đề án xác thực và tạo khóa phiên cho môi trường ứng dụng đa máy chủ:

- Nghiên cứu và phát triển phương pháp xác thực đa yếu tố trong môi trường multi-server, đảm bảo tính ẩn danh cho người dùng. Điều này đảm bảo rằng các người dùng có thể truy cập vào các máy chủ khác nhau mà không cần tiết lộ danh tính của họ.

2. Triển khai ứng dụng và đánh giá:

- Lựa chọn kịch bản ứng dụng: Triển khai xác thực đa yếu tố trong môi trường multi-server, cụ thể là Telecare Medical Information System. Đây là một hệ thống thông tin y tế trực tuyến, nơi xác thực đa yếu tố có thể đảm bảo tính bảo mật và an toàn cho dữ liệu y tế.
- Đánh giá tính hiệu quả và bảo mật và khả năng đáp ứng các yêu cầu của hệ thống trong việc xác thực người dùng: Tiến hành đánh giá hiệu quả của các phương pháp xác thực đa yếu tố đã triển khai trong Telecare Medical Information System.

KẾT QUẢ MONG ĐỢI

Kết quả dự kiến từ đề tài nghiên cứu này là tăng cường tính bảo mật và hiệu quả trong quá trình xác thực đa yếu tố. Bằng cách triển khai các phương pháp xác thực như mật khẩu một lần (TOTP), sinh trắc học và sử dụng module phần cứng hỗ trợ, mong đợi đạt được những kết quả sau:

- Tăng cường tính bảo mật: Sử dụng xác thực đa yếu tố giúp bảo vệ người dùng khỏi các cuộc tấn công mật khẩu đơn giản và tăng cường khả năng chống lại các cuộc tấn công xác thực. Các yếu tố bảo mật như mật khẩu một lần, sinh trắc học và module phần cứng hỗ trợ đảm bảo rằng chỉ người dùng chính mới có thể truy cập vào tài khoản và thông tin nhạy cảm.
- Bảo vệ thông tin và quyền riêng tư: Xác thực đa yếu tố giúp đảm bảo tính toàn vẹn và bảo mật của dữ liệu và quyền riêng tư của người dùng. Sử dụng các yếu tố bảo mật như sinh trắc học và module phần cứng hỗ trợ đảm bảo rằng thông tin cá nhân không bị lộ ra ngoài và chỉ có người dùng chính mới có thể truy cập vào nó.

- Đáp ứng yêu cầu Telecare Medical Information System: Triển khai xác thực đa yếu tố trong Telecare Medical Information System sẽ giúp đáp ứng yêu cầu cao về bảo mật và độ tin cậy trong hệ thống thông tin y tế trực tuyến. Điều này đảm bảo an toàn và riêng tư cho dữ liệu y tế, đồng thời chỉ cho phép những người dùng có quyền truy cập vào thông tin nhạy cảm, ngoài ra còn đảm bảo tính ẩn danh cho người dùng.

TÀI LIỆU THAM KHẢO (*Định dạng DBLP*)

- [1] Inam ul Haq, et al. “A Survey of Authenticated Key Agreement Protocols for Multi-Server Architecture.” J. Inf. Secur. Appl., vol. 55, 2020, p. 102639, doi.org/10.1016/j.jisa.2020.102639, <https://doi.org/10.1016/j.jisa.2020.102639>.
- [2] Jin, Zhe, et al. “Ranking-Based Locality Sensitive Hashing-Enabled Cancelable Biometrics: Index-of-Max Hashing.” IEEE Trans. Inf. Forensics Secur., vol. 13, 2018, pp. 393–407, doi.org/10.1109/TIFS.2017.2753172, <https://doi.org/10.1109/TIFS.2017.2753172>.
- [3] Canetti, Ran, et al. “Reusable Fuzzy Extractors for Low-Entropy Distributions.” J. Cryptol., vol. 34, 2021, p. 2, doi.org/10.1007/s00145-020-09367-8, <https://doi.org/10.1007/s00145-020-09367-8>.
- [4] Tomer Laor, et al. DRAWN APART: A Device Identification Technique Based on Remote GPU Fingerprinting. The Internet Society, 2022, www.ndss-symposium.org/ndss-paper/auto-draft-242/.
- [5] Secure ECC-Based Three-Factor Mutual Authentication Protocol for Telecare Medical Information System.” IEEE Access, vol. 10, 2022, pp. 11511–11526, doi.org/10.1109/ACCESS.2022.3145959, <https://doi.org/10.1109/ACCESS.2022.3145959>.