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

Tạ Việt Hoàng - 220202018

Tóm tắt

Tạ Việt Hoàng - MSSV: 220202018

https://github.com/tvhoang2012/CS2205/

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

Giới thiệu

- Kết nối thông qua internet để sử dụng các dịch vụ trực tuyến có rủi ro về bảo mật thông tin.
- Xác thực đa yếu tố và bảo vệ khóa phiên được coi là giải pháp tốt nhất để xây dựng kênh truyền tải dữ liệu an toàn nhưng các mô hình xác thực bảo vệ khóa phiên hiện tại vẫn còn lỗ hổng bảo mật.
- Nghiên cứu này tìm hiểu và triển khai các cách xác thực đa yếu tố nhằm tăng tính bảo mật và hiệu quả của xác thực đa yếu tố, và đánh giá tính hiệu quả của chúng thông qua thực nghiệm theo kịch bản thực tế.

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

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.

Nội dung

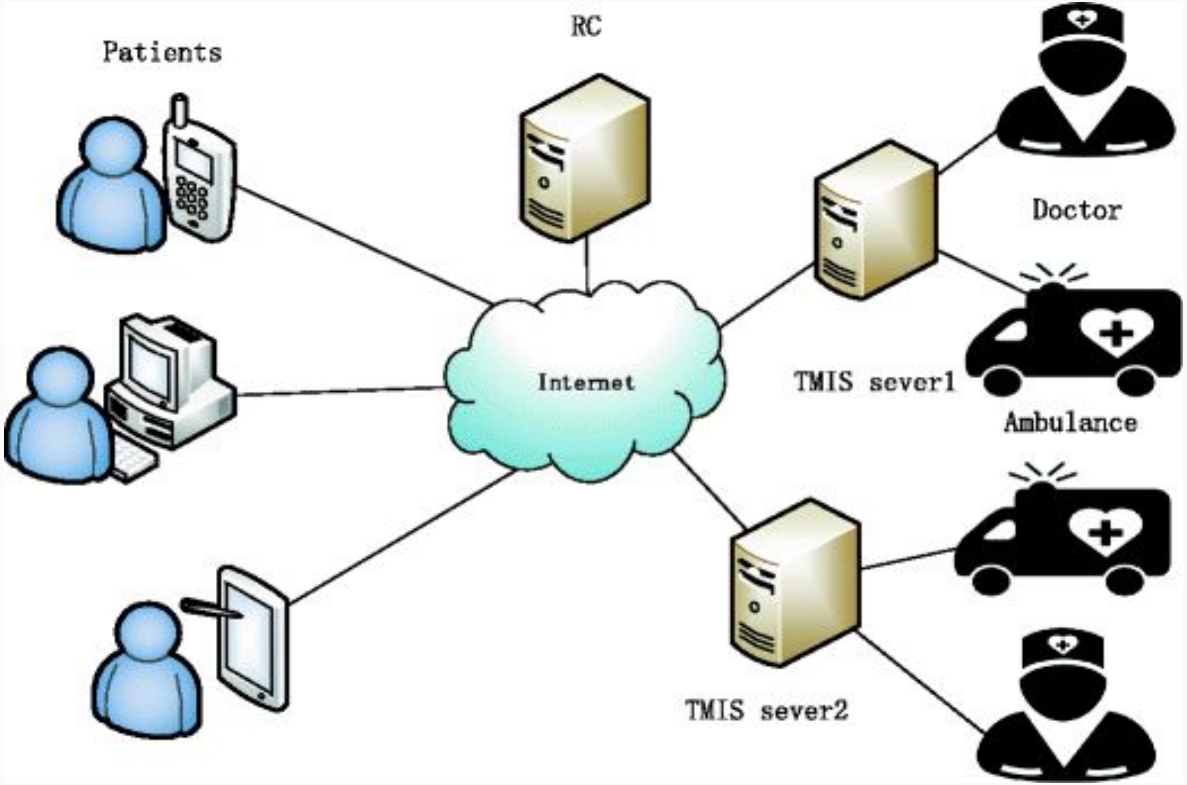
Nghiên cứu các đề án xác thực và tạo khóa phiên cho môi trường ứng dụng đa máy chủ:

- Nghiên cứu và phát triển phương pháp xác thực đa yếu tố trong môi trường đa máy chủ và 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.

Phương pháp

- 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, 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.

Phương pháp


Patients
RC
Doctor
Internet
TMIS sever1
Ambulance
TMIS sever2

Kết quả dự kiến

- 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.
- 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.
- Đáp ứng yêu cầu Telecare Medical Information System: Triển khai xác thực đa yếu tố trong sẽ giúp đáp ứng yêu cầu cao về bảo mật và độ tin cậy trong hệ thống.

Tài liệu tham khảo

[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.