QUY TRÌNH CHỨNG THỰC NGƯỜI DÙNG CHO CÁC HỆ THỐNG DỊCH VỤ TỪ XA SỬ DỤNG ĐA THỨC CHEBYSHEV

***Trương Toàn Thịnh*[1], *Trần Minh Triết*[1], *Dương Anh Đức*[2]**
[1]Khoa Công nghệ Thông tin,
Trường Đại học Khoa học Tự Nhiên, ĐHQG-HCM
[2]Khoa Công nghệ Thông tin,
Trường Đại học Công nghệ Thông tin, ĐHQG-HCM
{ttthinh, tmtriet}@fit.hcmus.edu.vn, ducda@uit.edu.vn

Tóm tắt

Hiện nay, công nghệ truyền thông ngày càng phát triển mạnh mẽ, như 4G hoặc 5G. Có nhiều ứng dụng trực tuyến hữu ích, và một trong số đó là hệ thống chăm sóc y tế từ xa. Nếu dịch vụ này được triển khai rộng rãi thì sẽ giúp người bệnh và bác sĩ có mối liên hệ thường xuyên, và điều này sẽ nâng cao chất lượng cuộc sống. Một trong những thành phần quan trọng để xây dựng hệ thống y tế từ xa một cách an toàn và tiện lợi đó là quy trình chứng thực người dùng. Chúng ta cần ngăn ngừa việc đánh cắp định danh và thông tin liên quan tới người bệnh. Vì thế, quy trình nên cung cấp tính nặc danh người dùng và xem xét tới một số hình thức tấn công phổ biến, như mạo danh hoặc đoán mật khẩu. Giải pháp là sự kết hợp các hướng tiếp cận như hàm băm, các mã khóa công RSA hoặc ECC, nhưng các quy trình hiện nay chưa thực xem việc bảo vệ định danh làm nhiệm vụ chính, rất cần trong môi trường thông tin y tế. Trong bài báo này, chúng tôi sẽ khảo sát một số quy trình hiện nay để có được các phân tích quan trọng, và sau đó là đề xuất quy trình chứng thực phù hợp với hướng tiếp cận đa thức Chebyshev.

Từ khóa: Quy trình chứng thực, đa thức Chebyshev, định danh người dùng, …

USER AUTHENTICATION SCHEME FOR REMOTE SERVICES USING CHEBYSHEV POLYNOMIAL

***Toan-Thinh Truong*[1], *Minh-Triet Tran*[1], *Anh-Duc Duong*[2]**
[1]Faculty of Information Technology, University of Science, VNU-HCM
[2]Faculty of Information Technology, University of Information Technology, VNU-HCM
{ttthinh, tmtriet}@fit.hcmus.edu.vn, ducda@uit.edu.vn

Abstract

Nowadays, communication technologies are more and more strongly advanced, such as 4G or 5G. There are many useful online applications, and one of them is telecare medical information system (TMIS). If this service is widely available, patient and doctor will have more frequently connection. Clearly, this enhances our quality of life. One of the most important module constructing this system securely and conveniently is user authentication scheme. We must prevent user identity and related information from adversary's eavesdropping. Therefore, authentication scheme should provide user anonymity and concern some kinds of attacks, such as impersonation or password-guessing attacks. The solution is the combination of hash function, public-key cryptosystem (RSA or ECC), but current schemes do not consider identity protection as a main task necessary for medical information environment. In this paper, we survey the previous papers to have some important analysis, and then propose a user authentication suitable for TMIS with Chebyshev polynomial.

Key words: Authentication scheme, Chebyshev polynomial, user identity, …