THÔNG TIN LUẬN ÁN

Tên luận án: **BẢO MẬT TRONG XÁC THỰC TỪ XA SỬ DỤNG ĐẶC TRƯNG SINH TRẮC**

Chuyên ngành: **KHOA HỌC MÁY TÍNH**

Mã số chuyên ngành: **62.48.01.01**

Họ và tên NCS: **NGUYỄN THỊ ÁI THẢO**

Người hướng dẫn khoa học: **PGS. TS. ĐẶNG TRẦN KHÁNH**

Cơ sở đào tạo: **Trường Đại học Bách khoa – Đại học Quốc Gia TP. Hồ Chí Minh**

Tóm tắt nội dung luận án

Ngày nay hệ thống xác thực bằng đặc trưng sinh trắc cung cấp ngày càng nhiều lợi ích cho người dùng so với các hệ thống xác thực truyền thống. Tuy vậy, lợi ích luôn đi kèm với nhiều thách thức. Đặc trưng sinh trắc về bản chất rất nhạy cảm - chứa đựng nhiều nguy cơ bị tấn công, đặc biệt là các nguy cơ xuất phát từ đường truyền mạng và nguy cơ ngay tại các mẫu sinh trắc được lưu trữ trong máy chủ của hệ thống. Trong luận án này, tôi đề xuất một giao thức mới an toàn cho hệ thống xác thực từ xa bằng đặc trưng sinh trắc có khả năng chống lại các loại tấn công phổ biến trên đường truyền mạng cũng như các tấn công ở nội tại máy chủ không đáng tin cậy. Đóng góp nổi bật của công trình này là trình bày một lược đồ bảo vệ mẫu sinh trắc trong hệ thống xác thực dùng đặc trưng sinh trắc. Đây là một dạng lược đồ lai, kết hợp kĩ thuật Phép chiếu trực giao ngẫu nhiên và Cam kết mờ, trong đó các yếu tố bảo mật và độ hiệu quả nhận dạng của hệ thống được phân tích nhằm thiết kế một lược đồ vừa tận dụng được các ưu điểm, đồng thời khắc phục những nhược điểm vốn có của các kĩ thuật này. Lược đồ này nhúng vào trong hệ thống xác thực theo kiến trúc từ xa có khả năng chống lại các tấn công từ bên trong hệ thống nhờ vào một bộ đồng xử lý bảo mật. Người quản lý hệ thống vẫn có quyền để điều khiển hệ thống nhưng sẽ không có khả năng lợi dụng các dữ liệu được lưu trữ trên máy chủ để giả mạo người dùng đánh lừa

toàn hệ thống vì các tính toán liên quan tới dữ liệu nhạy cảm đều được thực hiện trên bộ đồng xử lý bảo mật tích hợp trong bộ xử lý của máy chủ.

Các đóng góp chính của luận án

- Áp dụng hướng tiếp cận lai để bảo vệ mẫu sinh trắc vừa đảm bảo được những ưu điểm của các kĩ thuật đơn vừa khắc phục được những khuyết điểm nội tại của nó. Trong đó, kĩ thuật cam kết mờ được kết hợp với phép chiếu trực giao ngẫu nhiên tạo nên lược đồ bảo vệ mẫu sinh trắc trước khi đưa nó vào quá trình xác thực.
- Đưa ra giải pháp sử dụng bộ đồng xử lý bảo mật để tính toán trên máy chủ nhằm đảm bảo các tính toán trên dữ liệu nhạy cảm của người dùng được an toàn. Giao thức đề xuất cách giao tiếp giữa bộ xử lý chính và bộ đồng xử lý bảo mật để đảm bảo tối thiểu tính toán trên bộ xử lý bảo mật, bên cạnh đó cũng tối thiểu hóa các tiếp xúc với dữ liệu nhạy cảm ở bộ xử lý chính.
- Giao thức xác thực đề xuất có thể áp dụng cho các đặc trưng sinh trắc khác nhau có dạng vector. Độ chính xác của quá trình xác thực tương đương với hệ thống không áp dụng quy trình bảo mật nào. Hệ thống cũng đảm bảo được sự xác thực lẫn nhau giữa người dùng và máy chủ, đảm bảo chống lại các tấn công trên đường truyền mạng.

Cán bộ hướng dẫn khoa học	**Nghiên cứu sinh**
PGS. TS. Đặng Trần Khánh	**Nguyễn Thị Ái Thảo**