Xây dựng giải pháp bảo mật bioPKI và ứng dụng để bảo mật hệ thống nhận dạng vân tay

Nguyễn Thị Hương Thủy [1], Nguyễn Văn Toàn [2], Nguyễn Ngọc Kỷ [1], Nguyễn Thị Hoàng Lan [2]
[1] Phòng Thí nghiệm MP&THHT, Tổng cục IV, Bộ Công an
[2] Viện CNTT, Trường Đại học Bách khoa Hà Nội

Tóm tắt: Sử dụng vân tay để xác thực chủ thể truy cập hệ thống có nhiều ưu thế so với việc dùng mật khẩu truyền thống. Vân tay có nhiều ưu điểm so với các đặc trưng sinh trắc khác, tuy nhiên, vân tay cũng có thể bị làm giả và bản thân hệ thống nhận dạng vân tay cũng là một mục tiêu tấn công tiềm tàng nên việc bảo mật hệ nhận dạng vân tay là hết sức cần thiết. Báo cáo này tập trung trình bày kết quả cài đặt tính năng bảo mật cho hệ nhận dạng vân tay C@FRIS ứng dụng công nghệ bioPKI, bao gồm các công đoạn: kiểm soát xác thực chủ thể đăng nhập hệ thống, truy cập cơ sở dữ liệu, dùng chữ ký số và xác thực chữ ký để đảm bảo vệ xuất xứ dữ liệu mức bản ghi, mức cấu trúc các bảng cơ sở dữ liệu, và tính năng mật mã hóa/giải mã các giao dịch trên đường truyền, quá trình trao đổi dữ liệu giữa các phân hệ, sao lưu bảo quản, bảo đảm sự toàn vẹn dữ liệu. Nhờ ứng dụng các tính năng ưu việt của công nghệ bioPKI, hệ C@FRIS được tăng cường thêm tính năng bảo mật, an ninh an toàn mà vẫn đảm bảo được các tính năng cơ bản của hệ thống.

Từ khóa: bioPKI, PKI, C@FRIS, AFIS, nhận dạng vân tay, bảo mật, an ninh, an toàn thông tin, sinh trắc, mô hình các mối đe dọa.

1. Giải pháp bioPKI trên mạng

Sinh trắc học nói chung và sinh trắc học vân tay ngày càng được chấp nhận rộng rãi do khả năng xác thực chủ thể một cách chính xác dựa vào các đặc trưng sinh học và các đặc trưng hành vi. Từ các hệ kiểm soát truy cập qui mô nhỏ dùng vân tay và ảnh khuôn mặt để quản lý nhân viên ra vào công sở đến hệ căn cước công dân qui mô từ hàng triệu đến hàng chục triệu bản ghi dùng đặc trưng đa sinh trắc như vân tay 10 ngón, ảnh khuôn mặt, ảnh tròng mắt, ... đều là những thí dụ thực tế điển hình của ứng dụng sinh trắc học.

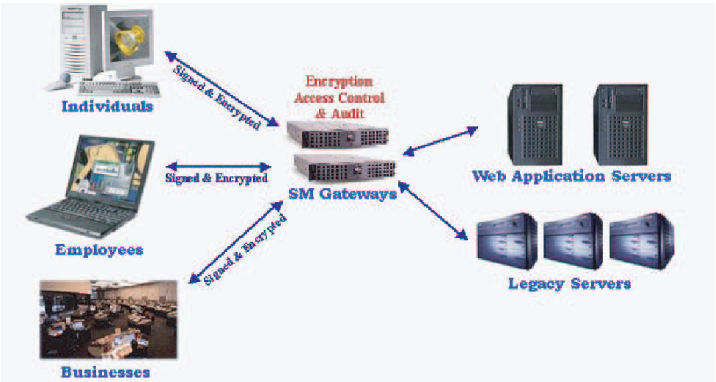
Công nghệ mật mã, mặt khác, được dùng để đảm bảo an ninh trong quá trình phát sinh, lưu trữ và truyền thông tin trên mạng. Công nghệ mật mã dùng cơ sở hạ tầng khóa công khai PKI là một thành tựu mới, với cơ chế quản lý và phân phối các cặp khóa riêng, khóa chung rất chặt chẽ nên đã và đang trở thành nền tảng bảo mật chung, được dùng để bảo mật cho các ứng dụng trên mạng INTERNET.

Hạn chế của công nghệ PKI truyền thống chính là việc dùng mật khẩu để truy cập tới khóa riêng. Mật khẩu thường không chứng minh được chính xác danh tính chủ thể, dễ bị

lộ, dễ bị người khác lợi dụng và bất tiện trong quản lý. So với mật khẩu, các đặc trưng sinh trắc học có ưu thế vì đảm bảo chính xác danh tính chủ thể, dễ quản lý. Tuy nhiên, các đặc trưng sinh trắc học cũng có những nhược điểm của nó, đó là khi bị làm giả, bị lợi dụng, thì không dễ dàng có đặc trưng sinh trắc khác để thay thế, sinh trắc bị lợi dụng có thể dùng để truy cập nhiều ứng dụng khác nhau, trong khi đó nếu mật khẩu bị lộ người ta có thể thay mật khẩu khác. Để hạn chế và khắc phục các hạn chế trên của sinh trắc học, giải pháp ứng dụng công nghệ bảo mật để bảo vệ công nghệ sinh trắc nhằm ngăn ngừa nhiều loại hình tấn công khác nhau đã được nhiều tác giả quan tâm nghiên cứu [5,6,7,9].

Giải pháp bioPKI trên mạng được hiểu là một ứng dụng bảo mật PKI dựa trên cơ chế đảm bảo cho người sử dụng được dùng các đặc trưng sinh trắc để truy cập đến khóa riêng, chứng minh chính xác danh tính chủ thể nhằm truy cập bảo mật từ xa tới máy chủ thông qua mạng, đồng thời được phép dùng đặc trưng sinh trắc để ký số và mật mã hóa để kiểm soát các tiến trình giao dịch, kiểm soát truy cập đến các tệp tin, biết được ai, cái gì, khi nào, ở đâu, tác động như thế nào với các tệp tin và các giao dịch đó.

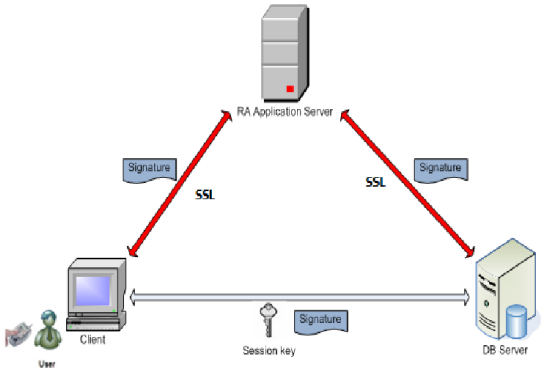
Trong một thời gian dài, công nghệ này mới chỉ được đề cập trên phương diện lý thuyết, mãi tới gần đây nó mới được hiện thực hóa. Giải pháp bioPKI do đề tài đề xuất là một trong những cố gắng đó. Hình 1.1 trình bày sơ đồ khái quát mô hình giải pháp bảo mật ứng dụng bioPKI trên mạng.



***Hình 1.1*- Sơ đồ khái quát mô hình giải pháp bảo mật ứng dụng bioPKI trên mạng.**

Việc xây dựng ứng dụng kiểm soát truy cập cơ sở dữ liệu (CSDL) trên nền hệ thống BioPKI sử dụng thẻ sinh trắc Bio-Etoken kết hợp với mã hóa và chữ ký số nhằm mục tiêu đảm bảo an ninh an toàn thông tin cho quá trình xác thực cũng như quá trình trao đổi dữ liệu.

Giải pháp đề xuất dựa trên mô hình bảo mật kiểm soát truy cập CSDL 3 yếu tố như sau [Hình 1.2]:



***Hình 1.2*- Mô hình hệ thống bảo mật kiểm soát truy cập CSDL ứng dụng bioPKI**

Trong đó:

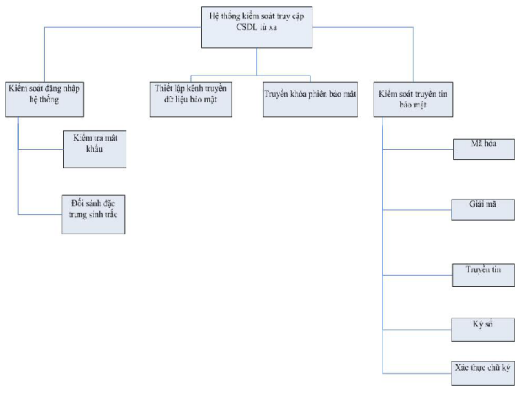
- **User**: Người sử dụng được phép truy cập từ xa qua mạng vào một máy chủ CSDL nếu được hệ thống BioPKI cấp khóa riêng, thẻ sinh trắc Bio-EToken và chứng thư, thẻ còn hiệu lực để có thể thực hiện việc mã hóa, giải mã, ký và xác thực chữ ký trong các giao dịch.
- **Client**: Máy trạm mà User sử dụng để truy cập từ xa qua mạng. Máy này phải được cài đặt phần mềm nhận dạng sinh trắc, trong trường hợp của chúng ta là dùng vân tay được kết nối với thiết bị có chức năng thu nhận vân tay sống, đầu đọc thẻ, được nối mạng với Application Server RA để trao đổi thông tin sau khi được ký, xác thực và mật mã hóa.
- **DB Server**: Máy chủ CSDL được bảo vệ truy cập từ xa. DB Server cũng được coi là một User của hệ thống nên cũng được cấp một khóa riêng và chứng thư.
- **RA Application Server:** Máy chủ dịch vụ ứng dụng, một thành phần của RA Server thuộc hệ thống BioPKI, cung cấp dịch vụ ứng dụng như: Kiểm tra tính xác thực của chứng thư số, download chứng thư số, sinh, quản lý và phân phối khóa phiên trong giao dịch giữa **Client** và DB Server.
- **Hạ tầng BioPKI:** Cung cấp các chứng thư số, kho chứng thư, các thẻ Bio-Etoken cho người dùng và các dịch vụ liên quan như kiểm tra, xác thực chứng thư, nhận chứng thư, …

Ưu thế bảo mật của giải pháp đề xuất:

- **Bảo mật username và password đăng nhập của user:** Dùng xác thực sinh trắc với thẻ Bio-EToken để tăng cường bảo mật password nhập từ bàn phím dựa trên nguyên tắc đối sánh tại chỗ bộ đặc điểm chi tiết trích chọn từ vân tay thu nhận online của người sử dụng với bộ đặc điểm chi tiết mẫu thu nhận trước đó (khi người sử dụng lần đầu đăng ký vào hệ thống). Nhờ dùng vân tay để xác minh tại chỗ danh tính người sử dụng khi đăng nhập hay truy cập tài nguyên hệ thống nên tránh được các trường hợp người này dùng username và password của người khác.
- **Tăng cường bảo mật trên đường truyền:** Nhờ sử dụng kênh mật SSL cho các giao dịch phân phối khóa phiên, đồng thời kết hợp thêm kỹ thuật mật mã hóa và giải mã đảm bảo tính toàn vẹn dữ liệu, ngăn ngừa được kiểu tấn công chèn người trung gian (man-in-the-middle). Với các giao dịch trao đổi dữ liệu sau khi có khóa phiên giữa Client và DB Server, dữ liệu được mã hóa đối xứng, được gắn thêm chữ ký số và có thể tiếp tục truyền qua kênh SSL. Với việc sử dụng chữ ký số ứng dụng còn cung cấp thêm tính năng chống chối bỏ trách nhiệm của **user**, cũng như chống các loại hình tấn công khác liên quan đến phiên làm việc của người dùng.

Bộ công cụ bioPKI để kiểm soát truy cập mạng

Trên cơ sở mô hình nêu trên, bộ công cụ bảo mật bioPKI được xây dựng bao gồm 4 chức năng chính: (1) Kiểm soát đăng nhập hệ thống, (2) Thiết lập kênh truyền dữ liệu bảo mật, (3) Truyền khóa phiên bảo mật, (4) Kiểm soát truyền dữ liệu bảo mật, bao gồm mật mã hóa/giải mã và ký số/xác thực chữ ký số.



***Hình 1.3*- Biểu đồ phân cấp chức năng ứng dụng kiểm soát truy cập mạng**

- **Chức năng kiểm soát đăng nhập hệ thống:**
  - Kiểm tra mật khẩu đăng nhập vào ứng dụng ở máy client của người dùng.

- Đối sánh đặc trưng sinh trắc: Sử dụng thiết bị live scanner để thu nhận vân tay sống của người sử dụng, sau đó trích chọn đặc điểm để đối sánh với bộ đặc điểm lưu trong thẻ E-Token của người đó.

- **Chức năng thiết lập kênh truyền tin bảo mật:**
  - Thiết lập kênh truyền dữ liệu bảo mật SSL tay ba: giữa RA Application Server và DB Server, giữa Client và RA Application Server, giữa Client và DBServer.
  - Nếu kết quả đăng nhập của User là thành công thì lấy được khóa riêng và chứng thư của User, khóa riêng và chứng thư sẽ được dùng để thiết lập kênh truyền dữ liệu bảo mật SSL giữa Client và RA Application Server, giữa Client và DBServer.
  - Kênh mật chỉ được thiết lập nếu mỗi bên đều được cung cấp chứng thư, khóa riêng. Trong quá trình thiết lập kênh sẽ sử dụng chứng thư của CA để tiến hành kiểm tra hiệu lực của chứng thư và khóa riêng này. Nếu vẫn còn hiệu lực, thì chúng sẽ được sử dụng để mã hóa và giải mã bất đối xứng các thông điệp đã bắt tay.

- **Chức năng truyền khóa phiên bảo mật:**
  - Việc đảm bảo tính mật của khóa phiên có ý nghĩa vô cùng quan trọng.
  - Khóa phiên do RA Application Server sinh ra sẽ được mã hóa khóa bất đối xứng và ký số trước khi được truyền trên kênh mật tới máy Client, DB Server.

- **Chức năng kiểm soát truyền dữ liệu bảo mật:**

Chiều từ DB Server tới Client:

- Đầu tiên DB Server sẽ mã hóa dữ liệu bằng khóa phiên (do RA Server Application gửi sang), sau đó thực hiện ký số lên dữ liệu mã hóa và gửi tới Client thông qua kênh truyền bảo mật SSL.
- Tại phía Client, khi nhận được dữ liệu, đầu tiên sẽ xác thực chữ ký của DB Server, nếu xác thực chữ ký thành công thì Client sẽ sử dụng khóa phiên (do RA Server Application gửi sang) để giải mã.
- Sau khi giải mã, nếu dữ liệu phù hợp với định dạnh quy định trước thì kết quả mà người dùng nhận được là chính xác do DB gửi sang.

Chiều từ Client đến DB Server:

- Client mã hóa dữ liệu bằng khóa phiên (do RA Server Application gửi sang), sau đó thực hiện ký số lên dữ liệu mã hóa và gửi tới DB Server thông qua kênh truyền bảo mật SSL.

- Tại phía DB Server, khi nhận được dữ liệu, đầu tiên sẽ xác thực chữ ký của Client, nếu xác thực chữ ký thành công thì DB Server sẽ sử dụng khóa phiên (do RA Server Application gửi sang) để giải mã.
- Sau khi giải mã, nếu dữ liệu phù hợp với định danh quy định trước thì kết quả mà DB Server nhận được chính xác là do Client gửi sang.

Bộ công cụ phát triển bioPKI SDK

Bộ công cụ SDK bioPKI được xây dựng dựa trên việc sử dụng:

- Ngôn ngữ phát triển hệ thống là C++ (VC++, .Framework 3.0) với lợi thế vừa hỗ trợ hướng đối tượng vừa tích hợp được các hàm viết bằng ngôn ngữ C trong thư viện OpenSSL.
- Thư viện mã nguồn mở OpenSSL để xây dựng các module mật mã hóa, giải mã, ký số, xác thực chữ ký và truyền thông điệp qua kênh SSL. Hơn nữa, thư viện OpenSSL còn là một thành phần của OpenCA.
- Hệ quản trị cơ sở dữ liệu được dùng là MySQL vì đây là hệ quản trị cơ sở dữ liệu mã nguồn mở và có hỗ trợ các hàm C, API để thực hiện truy vấn cơ sở dữ liệu.
- Ngoài ra, hệ thống cũng sử dụng các API có sẵn do hệ BioPKI cung cấp, cụ thể:

- Các APIs làm việc với thẻ sinh trắc Bio-Etoken.
- Các APIs ký và xác thực chữ ký số.
  - Giải pháp hệ thống: Xây dựng các module cho Client, RA Application Server và DB Server. Một số lớp quan trọng được sử dụng để viết các module này:
  - CMySQL: Lớp cho phép DB Server connect và thao tác với CSDL.
  - CSSLChannel: Lớp thực hiện thiết lập kênh SSL và gửi dữ liệu qua kênh mật.
  - CXMLProfile: Lớp thực hiện việc đọc ghi file định dạng XML khi thực hiện cấu hình cho các ứng dụng.
  - Rijndael: Lớp thực hiện mã AES (mã hóa đối xứng), được Client và DB Server sử dụng.

Cài đặt các thành phần của ứng dụng:

Client:

- Module đọc thẻ và xác thực sinh trắc (Sử dụng các API có sẵn do hệ BioPKI - OpenCA cung cấp).

- Các hàm băm, mã hóa và giải mã đối xứng bằng thuật toán AES mật khẩu truy cập từ xa bằng khóa phiên, mã hóa và giải mã bất đối xứng. Ở đây thuật toán mã hóa AES cho phép làm việc với khóa có độ dài bất kỳ. Sử dụng các hàm có sẵn của thư viện OpenSSL để thực hiện mã hóa và giải mã khóa bất đối xứng.
- Module ký và xác thực chữ ký: chữ ký của RA Application Server, chữ ký của DBServer (Sử dụng các API có sẵn do hệ BioPKI-OpenCA cung cấp).
- Module thiết lập kênh mật SSL. Sử dụng các hàm trong thư viện OpenSSL để thiết lập.

RA Application Server:

- Module dịch vụ liên quan đến chứng thư số (check valid, download…) tận dụng luôn của RA Server trong hệ thống BioPKI.
- Module sinh khóa phiên, quản lý, phân phối và hủy khóa phiên.
- Module thiết lập kênh mật SSL.

DBServer:

- Các hàm băm, mã hóa và giải mã đối xứng bằng thuật toán AES mật khẩu truy cập từ xa bằng khóa phiên, mã hóa và giải mã bất đối xứng.
- Module ký và xác thực chữ ký.
- Module làm việc với CSDL.
- Module thiết lập kênh mật SSL.

Kết quả cài đặt là Bộ các nhóm hàm chủ chốt được xây dựng đủ để triển khi bảo mật một hệ thống thông tin cụ thể ứng dụng công nghệ :

- Nhóm hàm sử dụng để thiết lập kênh mật SSL;
- Nhóm hàm thực hiện ký và xác thực chữ ký;
- Nhóm hàm mã hóa/giải mã khóa đối xứng AES;
- Nhóm hàm làm việc với CSDL;

Mô tả chi tiết về từng hàm cụ thể được trình bày trong Báo cáo đề tài Nhánh 3 [1].

2. Xác định yêu cầu bảo mật hệ thống C@FRIS

Ta giả thiết rằng việc xây dựng và ứng dụng C@FRIS để điện tử hóa hệ thống căn cước công dân (CCCD)/căn cước can phạm (CCCP) dùng mô hình mạng Client-Server truyền thống đã cơ bản giải quyết xong, tức là hệ C@FRIS đã triển khai cài đặt đầy đủ các

tính năng từ khâu thu nhận, đăng ký chỉ bản thông tin đầu vào, kiểm tra chất lượng dữ liệu, tổ chức dữ liệu đến khâu tra cứu, khai thác hệ thống (chưa được bảo mật).

Nhiệm vụ đặt ra là tổ chức thiết kế và cài đặt bổ sung cho hệ C@FRIS các tính năng bảo mật dùng công nghệ bioPKI. Để cài đặt các tính năng bảo mật, cần phải xem xét đầy đủ tất cả các khâu của hệ thống trên cơ sở một chính sách bảo mật nhất quán, tuy nhiên báo cáo này không có tham vọng trình bày đầy đủ toàn bộ giải pháp bảo mật mà chỉ một số kết quả cài đặt cho những công đoạn quan trọng nhất.

Trên mô hình truyền thống của một hệ thống căn cước, có hai tiến trình chính: Tiến trình xây dựng và tiến trình khai thác. Đối với tiến trình xây dựng, tức là đăng ký từ đầu hay đăng ký bổ sung đối tượng mới vào CSDL, hệ thống sau khi nhập dữ liệu đầu vào, cần kiểm tra đảm bảo chất lượng dữ liệu, sau đó tiến hành tra cứu đối tượng đăng ký mới để kiểm tra đối tượng đã được cấp số căn cước hay chưa, nếu đã được cấp thì cấp lại căn cước với số căn cước cũ và đồng thời cập nhật mới số liệu, nếu chưa được cấp thì cấp số căn cước mới. Đối với tiến trình khai thác, hệ thống tiếp nhận yêu cầu tra cứu từ xa trên mạng để xác minh căn cước. Có hai dạng yêu cầu cơ bản: Dạng thứ nhất là tra cứu chứng minh nhân dân (CMND) theo các trường dữ liệu cơ bản như: Số căn cước, họ, tên, năm sinh, tên bố, tên mẹ, rồi thẩm định (1:1) theo vân tay 2 ngón trỏ; Dạng thứ hai là tra cứu truy tìm danh tính cá thể đối tượng (1:N) chỉ theo chỉ bản 10 ngón (TP/TP). Các yêu cầu khai thác đều được diễn đạt dưới dạng các câu hỏi SQL có sử dụng các hàm đối sánh vân tay theo bộ điểm đặc trưng chi tiết.

Trên môi trường mạng INTERNET, hệ thống CCCD có thể phục vụ công tác cải cách thủ tục hành chính công dưới dạng các dịch vụ sau:

2.1. Dịch vụ đăng ký xin cấp CMND trên mạng INTERNET:

Trên trang WEB dịch vụ này, thủ tục xin cấp mới hay cấp đổi lại CMND dự kiến được tiến hành theo các bước sau:

- Công dân truy cập vào trang WEB, nhập thông tin vào Tờ khai CMND điện tử và ký xác nhận.
- Hệ thống tiếp nhận tờ khai online, mật mã hoá thông tin tờ khai và thể hiện dưới dạng mã vạch 2 chiều để công dân đăng ký in tờ khai ra máy in (có mã vạch 2 chiều cùng bản rõ tờ khai) cùng giấy hẹn đến trụ sở CA Quận/Huyện để giải quyết tiếp. Lúc này công dân đã khai các thông tin nhân thân cơ bản, chưa có ảnh và vân tay.

- Tại trụ sở CA Quận/Huyện, công dân chỉ cần trình tờ khai đã in ra, hệ thống giải mã mã vạch và đối chiếu với bản tờ khai rõ, nếu khớp, tiến hành lăn tay chụp ảnh (trong vòng 3-5 phút/1 công dân). Công dân lấy giấy hẹn để đến nhận CMND.

2.2. Dịch vụ Tra cứu xác minh CMND trên mạng INTERNET

Cơ quan công chứng, cơ quan thuế, hàng không, ngoại giao, công an quản lý hành chính, quản lý xuất nhập cảnh, cửa khẩu, ... có nhu cầu cần kiểm tra, xác minh nhanh danh tính công dân đều có thể đăng ký khai thác dịch vụ xác minh, đối chiếu thông tin trên CMND xuất trình với bản CMND gốc do cơ quan công an quản lý trên mạng để đề phòng các hiện tượng giả mạo danh tính trong giao dịch.

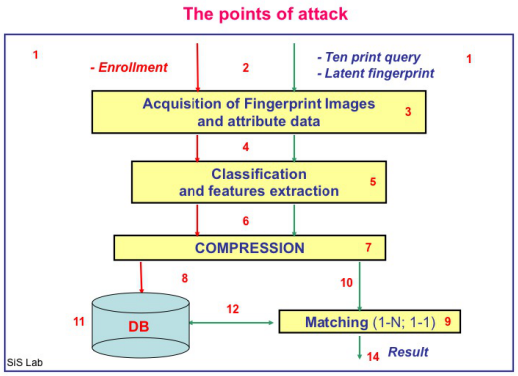
Yêu cầu bảo mật đối với một hệ nhận dạng vân tay tự động

Để triển khai các dịch vụ đăng ký xin cấp phát và kiểm tra chứng minh nhân dân trên mạng, hệ thống "hậu trường" cần đáp ứng được hai yêu cầu: Vừa đảm bảo nhanh chóng, thuận tiện cho nhân dân vừa đảm bảo yêu cầu nghiệp vụ, an ninh an toàn hệ thống. Ta có thể hình dung rằng việc lập phương án bảo mật cho một hệ thống tin học cũng tương tự như việc lập phương án bảo vệ một ngôi nhà. Chúng ta không chỉ quan tâm đến các cửa ra vào chính mà cần phải xem xét cả cửa sổ, cửa tum, các vị trí lắp quạt thông gió và nhiều điểm có thể đột nhập khác cũng như các phương thức đột nhập có thể tại từng điểm. Trên thực tế, không có một phương án bảo mật hoàn hảo mà chỉ có các phương án đáp ứng được yêu cầu đề ra. Điều quan trọng nhất trong bảo mật là thiết lập được mô hình các mối đe dọa và đưa ra phương án thiết kế phù hợp để ngăn ngừa được các mối đe dọa đó. Đối với việc bảo mật hệ thống nhận dạng vân tay cũng vậy, ta cần phải xây dựng mô hình các mối đe dọa và đưa ra giải pháp đảm bảo an ninh an toàn theo nghĩa ngăn ngừa được các phương thức tấn công điển hình trên mạng mà không gây thêm quá nhiều phiền toái cho người sử dụng. Sau đây là một số kiểu tấn công điển hình nhất đối với một hệ nhận dạng vân tay [9]:

- Kiểu tấn công làm đình trễ hoặc ngừng hẳn dịch vụ (Denial of Service): Ngăn hoặc đình lại không cho người sử dụng hợp pháp truy cập được vào hệ thống.
- Kiểu tấn công thay thế (Circumvention): Giả danh người sử dụng hợp pháp để truy cập bất hợp pháp vào hệ thống.
- Kiểu tấn công chối bỏ (Repudiation): Phủ nhận, chối bỏ trách nhiệm sau khi đã thực hiện một hành vi nào đó.

- Kiểu tấn công lây nhiễm hoặc lấy trộm (Contamination hay covert acquisition): Sao chép lại mật khẩu, làm giả vân tay, khuôn mặt, ... để đăng nhập hệ thống.
- Kiểu tấn công thông đồng với người sử dụng hợp pháp (Collusion).
- Kiểu tấn công cưỡng bức.

Tất cả các phương thức tấn công nói trên đều có thể xảy ra mọi lúc mọi nơi trong quá trình hoạt động của hệ thống, từ khâu thu nhận vân tay đầu vào, trao đổi dữ liệu đến các quá trình xử lý trích chọn đặc trưng, đối sánh, lưu vào CSDL và thông báo kết quả đầu ra [Hình 2.1].



***Hình 2.1*- Các điểm tấn công chủ yếu đối với một hệ nhận dạng vân tay**

Đối với khâu thu nhận, các phương thức tấn công điển hình thường là kiểu phá hoại, làm ngưng dịch vụ (chẳng hạn đập phá scanner), dùng vân tay giả mạo, cài sẵn vân tay trong bộ nhớ scanner hoặc trong các chip, ... Đối với các đường truyền, thường có các kiểu tấn công núp lấy dữ liệu để dùng lại (replay). Đối với các khâu trích chọn đặc trưng hay đối sánh, có thể bị các chương trình kiểu Troyan Horse thay thế, làm thay đổi kết quả.

Biện pháp kiểm soát thẩm quyền truy cập dùng đặc trưng sinh trắc học đảm bảo chính xác danh tính người sử dụng là giải pháp chung nhất để chống lại phương thức tấn công thay thế, lấy trộm mật khẩu và thông đồng. Biện pháp mật mã hóa kết hợp dùng chữ ký sinh trắc ngăn ngừa hiệu quả kiểu tấn công dùng vân tay giả, hay tìm cách cài sẵn vân tay vào trong bộ nhớ scanner hoặc trong các chip. Để đối phó với kiểu tấn công lấy cắp đặc trưng sinh trắc trên đường truyền mà không cần giải mã (replay) kiểu Troyan Horse ta chọn giải pháp kết hợp dùng kỹ thuật mật mã hóa và kỹ thuật kiểm chứng kiểu "đố-đáp" (challenge-response) hay kỹ thuật "đóng dấu thời gian" (Time Stamp) để xác thực.

Trên cơ sở phân tích các mối đe dọa và đề xuất giải pháp phòng chống nói trên, công nghệ bioPKI là công cụ hiệu quả để cài đặt các tính năng bảo mật cho hệ CCCD, giúp đáp ứng được một số yêu cầu cơ bản đề ra và cung cấp thêm tính năng bảo mật cho hệ thống:

- Thực hiện việc kiểm soát thẩm quyền truy cập dùng vân tay để đảm bảo đúng danh tính chủ thể, xác thực mật mã hai chiều cho mỗi phiên làm việc để đảm bảo sự toàn vẹn dữ liệu, dùng chữ ký số và chữ ký số sinh trắc để đảm bảo nguồn gốc xuất xứ, ngăn ngừa trường hợp chối bỏ trách nhiệm. Việc mật mã hóa dữ liệu không chỉ trong quá trình vận chuyển, truyền trên mạng mà còn trong các khâu xử lý, khai thác và vận hành hệ thống nhằm bảo mật chặt chẽ CSDL tránh bị lợi dụng, xâm nhập trái phép, kể cả khi bị sao chép hay bị lọt ra ngoài.
- Hệ thống có khả năng tự động lập nhật ký hệ thống, kiểm soát các tiến trình giao dịch, kiểm soát truy cập đến các tệp tin, biết được ai, cái gì, khi nào, ở đâu, tác động như thế nào với các tệp tin và các giao dịch đó, đảm bảo dễ dàng truy cứu trách nhiệm khi cần.

3. Kết quả ứng dụng bioPKI để bảo mật hệ C@FRIS

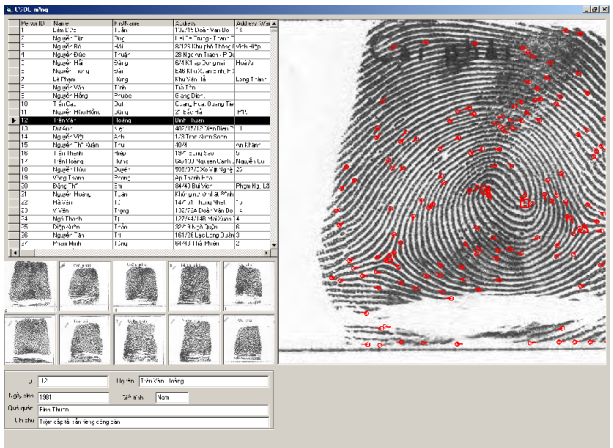
3.1. Phân hệ C@FRIS Scan bảo mật

Phân hệ phần mềm C@FRIS scan đảm nhận nhiệm vụ nhập chuyển đổi số hóa chỉ bản của hệ C@FRIS được cài đặt trên các máy trạm Client của mạng LAN được kết nối với máy chủ CSDL. Người sử dụng cần phải đăng ký để cấp thẩm quyền truy cập với vai trò nhân viên nhập chuyển đổi thông tin số hóa được phân quyền như sau:

- Kết nối máy trạm với máy chủ CSDL, khởi tạo bảng CSDL, điều khiển máy quét scanner nhập chuyển đổi số hóa chỉ bản và lưu kết quả vào CSDL.
- Tiến hành nhập thông tin thuộc tính về nhân thân đối tượng (số hồ sơ, họ tên, giới tính, năm sinh, nơi đăng ký HKTT, ... của đối tượng). Tiếp đó là nhập các thông tin về vân tay như: Dạng cơ bản, số đếm vân, ... và tự động cắt ảnh chỉ bản thành mười ngón riêng rẽ.
- Dùng bộ duyệt CSDL (BROWSER) để truy cập, chỉnh sửa, bổ sung các bản ghi dữ liệu thuộc tính.
- Nhập CSDL hợp chuẩn ANSI/NIST từ các hệ AFIS khác.
- Xuất CSDL C@FRIS sang dạng chuẩn ANSI/NIST để nhập vào hệ AFIS khác.

Tính năng bảo mật đã được cài đặt:

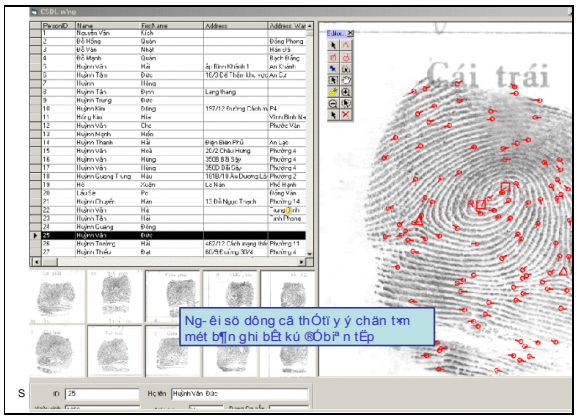
- Kiểm soát đăng nhập phần mềm C@FRIS Scan;
- Kiểm soát truy cập máy chủ CSDL;
- Người sử dụng với vai trò là nhân viên chuyển đổi thông tin số hóa có trách nhiệm ký số vào các trường, (hay để rút gọn có thể ký chung cho tổ hợp một số trường dữ liệu) do mình tạo ra, cụ thể là các trường: Số căn cước đối tượng, họ tên, giới tính, năm sinh, địa phương, mã số ngón, dạng cơ bản, số đếm vân, ảnh vân tay đối tượng.
- Chức năng xử lý trích chọn đặc điểm tự động do phân hệ trích chọn đặc điểm C@FRIS FE của hệ thống thực hiện nên phân hệ này là chủ thể chịu trách nhiệm ký, xử lý nén, mật mã hóa dữ liệu của trường lưu đặc điểm chi tiết của bản ghi tương ứng.
- Riêng trường ảnh gốc sau khi nhân viên nhập liệu ký chịu trách nhiệm cắt ảnh, hệ thống tiếp tục xử lý nén, mật mã hóa và ký xác nhận.
- Tất cả các giao tác của hệ thống và của nhân viên nhập chuyển đổi thông tin số hóa đều được ghi vào CSDL nhật ký hệ thống. Bản thân cơ sở dữ liệu này được bảo mật như "hộp đen" của hệ thống và chỉ người được cấp thẩm quyền bảo mật hệ thống mới truy cập được.



***Hình 3.1*- Tất cả các bản ghi CSDL đều được NSD ký sinh trắc, ảnh vân tay công dân và bộ đặc điểm chi tiết được hệ thống xử lý nén, mật mã hóa và ký xác nhận trách nhiệm**

3.2. Phân hệ "Biên tập và kiểm tra chất lượng" bảo mật

Phân hệ "**Biên tập và kiểm tra chất lượng**" được trang bị trình duyệt CSDL với nhiều công cụ tiện ích để người sử dụng được cấp thẩm quyền biên tập và kiểm tra chất lượng thực hiện các thao tác truy vấn CSDL trên máy chủ, truy cập đến từng bản ghi để biên tập các thông tin thuộc tính và đồ họa.



***Hình 3.2*- Biên tập đặc điểm chi tiết và ký sinh trắc vào bản ghi trước khi lưu vào CSDL**

- Bộ đặc điểm chi tiết ban đầu do hệ thống tự động xử lý nên hệ thống là chủ thể ký bảo mật trường dữ liệu này. Trường hợp bộ đặc điểm chi tiết được biên tập lại thì người có thẩm quyền biên tập là người ký (dùng chữ ký số) chịu trách nhiệm phần biên tập.
- Sau khi biên tập và ký lưu, chính hệ thống là chủ thể xử lý nén, mật mã hóa, nên hệ thống tiến hành ký xác nhận công đoạn này.
- Các bảng dữ liệu sau kiểm tra chất lượng được coi là hoàn chỉnh, cũng được hệ thống ký xác nhận để đảm bảo tính toàn vẹn và nguồn gốc dữ liệu.

3.3. Phân hệ "Tổ chức cơ sở dữ liệu" bảo mật

Phân hệ này đảm bảo chức năng quản lí và tổ chức CSDL cài đặt trên máy chủ của một mạng LAN tổ chức theo mô hình CLIENT-SEVER để phục vụ khai thác.

Người sử dụng được cấp thẩm quyền tổ chức CSDL được phép truy cập CSDL trên máy chủ, được phân loại, tổ chức thành nhiều bảng dẫn xuất, được đánh chỉ số phân cấp nhằm tăng tốc truy xuất dữ liệu. Các kết quả tổ chức CSDL đều được ký sinh trắc bởi quản trị viên và bởi hệ thống.

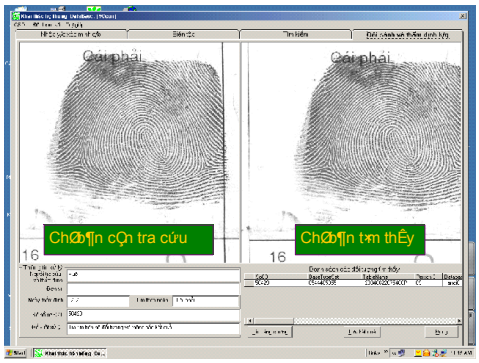
Trên các máy trạm, người được cấp thẩm quyền tổ chức CSDL được phép truy vấn CSDL bằng câu lệnh SQL SERVER, xử lý kết nối các bảng, đánh chỉ số, lập báo cáo, thống kê, kiểm kê hệ thống.

Tất cả các giao tác của quản trị viên được hệ thống tự động lưu vào CSDL nhật ký hệ thống.

3.4. Phân hệ "Tra tìm, Đối sánh" bảo mật

Người được cấp thẩm quyền tra tìm, đối sánh để xác minh căn cước, được phép đăng nhập phần mềm, truy cập đến máy chủ CSDL để tiến hành hai dạng yêu cầu chủ yếu sau:

- Xác minh theo chỉ bản vân tay 10 ngón.
- Xác minh theo số căn cước, họ tên, ngày tháng năm sinh, sau đó thẩm định theo vân tay 2 ngón trỏ.



***Hình 3.4*- Kết quả Tra tìm, Đối sánh TP-TP được ký sinh trắc, lưu vào CSDL kết quả tra cứu**

Người sử dụng với vai trò tra cứu, đối sánh được yêu cầu ký xác nhận lập yêu cầu tra cứu, xác nhận việc nhận kết quả tra cứu. Hệ thống ký xác nhận đã tiếp nhận yêu cầu, đã tra cứu và cung cấp kết quả.

4. Đánh giá, Kết luận

Công nghệ mật mã dùng cơ sở hạ tầng khóa công khai PKI là một thành tựu mới, với cơ chế quản lý và phân phối các cặp khóa riêng, khóa chung rất chặt chẽ nên đã và đang trở thành nền tảng bảo mật chung, được dùng để bảo mật cho các ứng dụng trên INTERNET. Hạn chế của công nghệ PKI truyền thống dựa trên việc dùng mật khẩu để

truy cập tới khóa riêng thường dễ bị lợi dụng đã được khắc phục bằng công nghệ bioPKI đảm bảo danh tính chủ thể chính xác hơn bằng công nghệ nhận dạng vân tay.

Tuy nhiên, bất kỳ một hệ thống được bảo mật nào cũng có thể bị bẻ gãy nếu đối phương có đủ điều kiện và thời gian. Một giải pháp bảo mật được coi là hữu hiệu chỉ khi nào nó mô hình hóa được đầy đủ các mối đe dọa hệ thống và đưa ra giải pháp phòng chống hữu hiệu mà không làm tăng thêm độ phức tạp hệ thống. Trong khuôn khổ đề tài nghiên cứu khoa học cấp nhà nước: ”*Nghiên cứu ứng dụng hệ thống kiểm soát truy cập mạng và an ninh thông tin dựa trên sinh trắc học sử dụng công nghệ nhúng*”, nhóm tác giả đã phát triển bộ công cụ bảo mật bioPKI và đưa vào ứng dụng để bảo mật cho hệ nhận dạng vân tay tự động C@FRIS. Báo cáo này tập trung trình bày kết quả xây dựng giải pháp và cài đặt tính năng bảo mật cho các công đoạn hoạt động chủ yếu của một hệ nhận dạng vân tay, bao gồm các khâu: kiểm soát xác thực đúng chủ thể đăng nhập hệ thống, truy cập cơ sở dữ liệu, tính năng dùng chữ ký số sinh trắc và xác thực chữ ký để đảm bảo vệ xuất xứ dữ liệu mức bản ghi, mức cấu trúc các bảng cơ sở dữ liệu, và tính năng mật mã hóa/giải mã các giao dịch trên đường truyền, khi trao đổi dữ liệu giữa các phân hệ, khi sao lưu bảo quản, bảo mật, bảo đảm sự toàn vẹn dữ liệu. Nhờ ứng dụng các tính năng ưu việt của công nghệ bioPKI, hệ C@FRIS đáp ứng được yêu cầu an ninh an toàn đề ra là ngăn ngừa được các loại hình tấn công điển hình đã tiên lượng được và cho phép cài đặt bổ sung nhanh chóng để chống lại các loại hình tấn công mới trong tương lai mà vẫn giữ được các tính năng cơ bản, đặc biệt là tính dễ dùng trong tất cả các khâu xây dựng, khai thác và vận hành hệ thống.

Tài liệu tham khảo (References)

[1] Nguyễn Thị Hoàng Lan và cộng sự, "Nghiên cứu ứng dụng hệ thống kiểm soát truy cập mạng và an ninh thông tin dựa trên sinh trắc học sử dụng công nghệ nhúng". Báo cáo đề tài nghiên cứu KHCN cấp nhà nước. Hà Nội T6/2010.

[2] William Stallings, "Cryptography and Network Security Principles and Practices, Fourth Edition". Prentice Hall, November 16, 2005.

[3] Johannes Buchmann, "Introduction to cryptography, second edition". Springer, 2003.

[4] Parvathi Ambalakat, "Security of Biometric Authentication Systems", 21st Computer Science Seminar SA1-T1-1, 2002.

[5] Pravir Chandra, Matt Messier, John Viega "Network Security with OpenSSL".

[6] Dobromir Todorov, "Mechanics Of User Identification and Authentication", Fundamentals of Identity Management.

[7] Lang Zhao, "A Role-based Access Control Security Model for Workflow Management System in an E-healthcare Enterprise".

[8] Nguyễn Ngọc Kỷ, Nguyễn Thị Hương Thủy, Nguyễn Thanh Phương, Nguyễn Việt Tiệp, "Kết quả nghiên cứu ứng dụng công nghệ nhận dạng vân tay để tự động hóa các hệ thống căn cước công dân và căn cước can phạm". Kỷ yếu Hội nghị CNTT CAND, Hà Nội 9-2004, tr. 187-189.

[9] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, "Handbook of fingerprint recognition", Springer-Verlag, New York, Berlin Heidelberg, 1st ed., 2003.

***