HỌC VIỆN CÔNG NGHỆ BƯU
CHÍNH VIỄN THÔNG

NGUYỄN THẾ ANH

NGHIÊN CỨU GIẢI PHÁP NÂNG CAO BẢO MẬT CHO TRUNG TÂM TÍCH HỢP DỮ LIỆU CỤC DỰ TRỮ NHÀ NƯỚC KHU VỰC HÀ NỘI

Chuyên ngành: KỸ THUẬT VIỄN THÔNG
Mã số: 08.52.02.08

TÓM TẮT LUẬN VĂN THẠC SỸ
(Theo định hướng ứng dụng)

HÀ NỘI – 2021

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: TS. HOÀNG TRỌNG MINH

Người phản biện 1 : PGS.TS Nguyễn Hữu Trung

Người phản biện 2 : PGS.TS Lê Nhật Thăng

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: …….. giờ …… ngày …… tháng …… năm 2021

Có thể tìm hiểu luận văn tại:

Thư viện của Học viện Công nghệ Bưu chính Viễn thông

MỞ ĐẦU

Triển khai xây dựng giải pháp thử nghiệm cho một số ứng dụng đảm bảo an toàn và bảo mật thông tin cho Trung tâm tích hợp dữ liệu của Cục Dự trữ Nhà nước khu vực Hà Nội.

Với những lý do kể trên, tôi đã chọn đề tài luận văn là: "**Nghiên cứu giải phapr bảo mật cho trung tâm tích hợp dữ liệu Cục Dự trữ Nhà nước khu vực Hà Nội**".

Mục đích nghiên cứu

Nghiên cứu cơ bản về an ninh mạng, thuật ngữ bảo mật cơ bản, Mô tả các cuộc tấn công mạng phổ biến nhất, bao gồm tấn công Session, tấn công vi rút, phần mềm mã độc Trojan, từ chối dịch vụ và tràn bộ đệm, xác định các biện pháp phòng thủ cơ bản chống lại các cuộc tấn công đó, Đề xuất được những giải pháp đảm bảo an toàn và bảo mật cho Trung tâm tích hợp dữ liệu.

Luận văn được chia làm 3 chương:

Chương 1 Giới thiệu về an ninh mạng

Chương 2 Tấn công mạng

Chương 3 Xây dựng ứng dụng bảo mật cơ sở dữ liệu

CHƯƠNG 1 – GIỚI THIỆU VỀ AN NINH MẠNG

Tóm tắt: *Chương 1- Hiểu cơ bản về mạng , xác định các mối nguy hiểm phổ biến nhất đối với mạng, sử dụng thuật ngữ bảo mật cơ bản, tìm cách tiếp cận tốt nhất để bảo mật mạng cho Cục Dự trữ Nhà nước khu vực Hà Nội.*

1.1 Giới thiệu

1.1.1 Kiến thức cơ bản về mạng

Trước khi đi sâu vào cách bảo vệ mạng của Đơn vị, hãy khám phá mạng là gì có lẽ là một ý tưởng hay. Đối với nhiều độc giả, phần này sẽ là một bài đánh giá, nhưng đối với một số người, nó có thể là tài liệu mới.

+ Cấu trúc mạng cơ bản

Một số điểm kết nối phải tồn tại giữa mạng nội bộ và thế giới bên ngoài. Một rào cản được thiết lập giữa mạng đó và Internet, thường ở dạng tường lửa.

+ Các địa chỉ IP

Địa chỉ IP phiên bản 4 là một chuỗi bốn số có ba chữ số được phân tách bằng dấu chấm. (Ví dụ là 107.22.98.198.) Mỗi số có ba chữ số phải nằm trong khoảng từ 0 đến 255. Bạn có thể thấy rằng địa chỉ 107.22.98.466 sẽ không phải là địa chỉ hợp lệ.

Địa chỉ IP của một máy tính cho bạn biết rất nhiều điều về máy tính đó. Byte đầu tiên (hoặc số thập phân đầu tiên) trong một địa chỉ cho bạn biết máy đó thuộc lớp mạng nào.

+ Các địa chỉ MAC

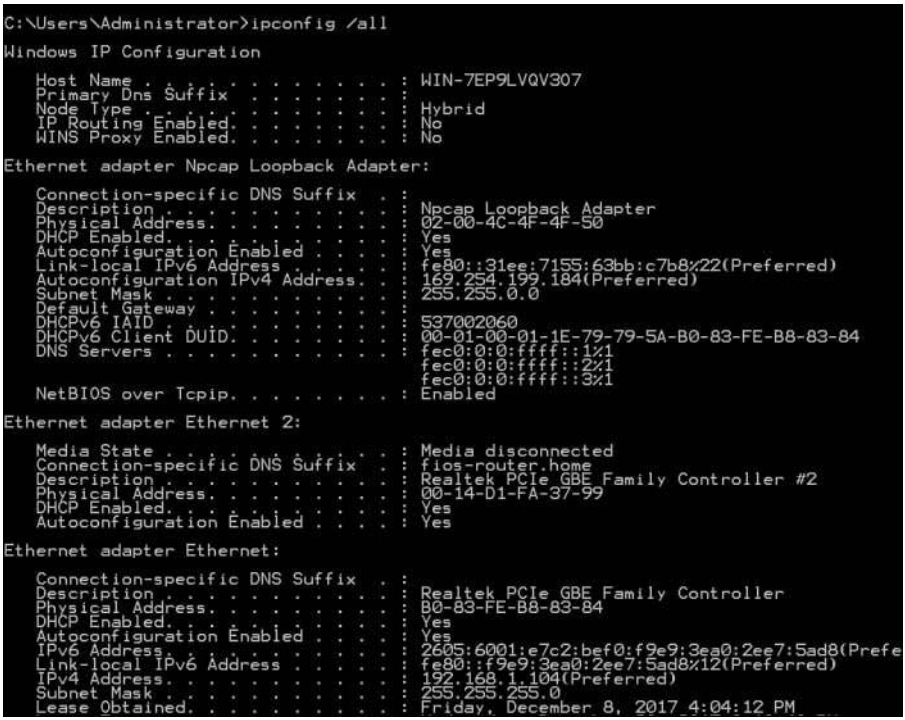
Các địa chỉ MAC là một chủ đề thú vị. (Bạn có thể nhận thấy rằng MAC cũng là một lớp con của lớp liên kết dữ liệu của mô hình OSI.) Địa chỉ MAC là một địa chỉ duy nhất cho một NIC. Mọi NIC trên thế giới đều có một địa chỉ duy nhất được biểu thị bằng số thập lục phân sáu byte.

Các loại truyền thông khác nhau tồn tại cho các mục đích khác nhau. Các kiểu truyền thông mạng khác nhau được gọi là *các giao thức*. Về cơ bản, một giao thức là một phương thức liên lạc đã được thỏa thuận. Trên thực tế, định nghĩa này chính xác là cách từ ngữ *giao thức* được sử dụng trong cách sử dụng tiêu chuẩn, không dùng máy tính. Mỗi giao thức có một mục đích cụ thể và thường hoạt động trên một cổng nhất định (nhiều cổng hơn một chút). Bảng 1-2 liệt kê một số giao thức quan trọng nhất.

+ ipconfig

Điều đầu tiên bạn muốn làm là lấy thông tin về hệ thống của riêng bạn. Để hoàn thành nhiệm vụ tìm kiếm sự thật này, bạn phải nhận được một dấu nhắc lệnh. Trong Windows, bạn thực hiện việc này bằng cách đi tới menu Bắt đầu, chọn Tất cả chương trình, sau đó chọn Phụ kiện. Bạn cũng có thể vào Start, Run và gõ **cmd** để nhận dấu nhắc lệnh. Trong Windows 10, bạn truy cập Tìm kiếm và nhập **cmd**. Bây giờ bạn có thể nhập **ipconfig**. (Bạn có thể nhập cùng một lệnh trong Unix hoặc Linux bằng cách nhập **ifconfig** từ shell.) Sau khi nhập **ipconfig** (**ifconfig** trong Linux), bạn sẽ thấy một cái gì đó giống như Hình 1-1.

Như bạn có thể thấy, bạn có thể sử dụng một số tùy chọn để tìm hiểu các chi tiết khác nhau về cấu hình máy tính của mình. Phương thức được sử dụng phổ biến nhất có lẽ là ipconfig/all, được hiển thị trong Hình 1-2.



HÌNH 1-2 Lệnh ipconfig/all

Bạn có thể thấy rằng tùy chọn này cung cấp cho bạn nhiều thông tin hơn. Ví dụ: ipconfig/all cung cấp tên máy tính của bạn, khi máy tính của bạn lấy được địa chỉ IP, v.v.

1.2 Mô hình OSI

Mô hình Kết nối Hệ thống Mở (OSI) mô tả cách các mạng giao tiếp (xem Bảng 1-3). Nó mô tả các giao thức và hoạt động khác nhau và cho biết các giao thức và hoạt động liên quan với nhau như thế nào. Mô hình này được chia thành bảy lớp. Ban đầu nó được phát triển bởi Tổ chức Tiêu chuẩn hóa Quốc tế (ISO) vào những năm 1980.

Lớp	**Mô tả**	**Các giao thức**
Application	Lớp này giao diện trực tiếp với các ứng dụng và thực hiện các dịch vụ ứng dụng chung cho các quy trình ứng dụng.	POP, SMTP, DNS, FTP, Telnet
Presentation	Lớp trình bày giải tỏa mối quan tâm của lớp ứng dụng liên quan đến sự khác biệt cú pháp trong biểu diễn dữ liệu trong hệ thống người dùng cuối.	Telnet, Biểu diễn dữ liệu mạng (NDR), Giao thức trình bày nhẹ (LPP)
Session	Lớp phiên cung cấp cơ chế quản lý cuộc đối thoại giữa các quy trình ứng dụng của người dùng cuối.	NetBIOS
Transport	Lớp này cung cấp khả năng kiểm soát giao tiếp đầu cuối.	TCP, UDP
Network	Lớp này định tuyến thông tin trong mạng.	IP, ARP, ICMP
Data link	Lớp này mô tả tổ chức hợp lý của các bit dữ liệu được truyền trên một phương tiện cụ thể. Lớp liên kết dữ liệu được chia thành hai lớp con: lớp Điều khiển truy cập phương tiện (MAC) và lớp Điều khiển liên kết lôgic (LLC).	SLIP, PPP
Physical	Lớp này mô tả các đặc tính	IEEE 1394,

	vật lý của các phương tiện truyền thông khác nhau, cũng như các đặc tính điện và diễn giải các tín hiệu được trao đổi. Nói cách khác, lớp vật lý là NIC thực tế, cáp Ethernet, v.v.	DSL, ISDN

Điều này có ý nghĩa gì đối với an ninh mạng?

Luận văn này đề cập đến vấn đề bảo mật từ nhiều góc độ, nhưng cuối cùng chỉ có ba địa điểm tồn tại để tấn công và do đó ba địa điểm bảo mật (lưu ý đây không phải là về các vectơ tấn công, trong số đó có rất nhiều):

- **Các điểm kết nối mạng:** Cho dù đó là bộ định tuyến hay tường lửa, bất kỳ nơi nào mà máy tính này kết nối với máy tính khác đều là nơi có thể bị tấn công và phải được bảo vệ. Khi xem xét tính bảo mật của hệ thống, trước tiên chúng ta nên xem xét các điểm kết nối.
- **Con người:** Con người luôn tiềm ẩn nguy cơ an ninh. Có thể do thiếu hiểu biết, có ý đồ xấu hoặc do lỗi đơn giản, mọi người trên hệ thống có thể xâm phạm tính bảo mật của hệ thống.

Khi bạn tiếp tục cuốn sách này, đừng quên mục đích cơ bản, đó là bảo mật các mạng và dữ liệu chúng lưu trữ và truyền.

1.3 Đánh giá các mối đe dọa có thể xảy ra đối với mạng

Về vấn đề này, dường như có hai thái độ cực đoan đối với bảo mật máy tính. Quan điểm đầu tiên cho rằng có rất ít mối nguy hiểm hoặc mối đe dọa thực sự tồn tại đối với hệ thống máy tính và phần lớn tin tức tiêu cực chỉ đơn giản là sự phản ánh của sự hoảng loạn không chính đáng.

+ Phân loại các mối đe dọa

Mạng của bạn chắc chắn phải đối mặt với các mối đe dọa bảo mật thực sự và những mối đe dọa này có thể tự biểu hiện dưới nhiều hình thức khác nhau. Có nhiều cách khác nhau mà người ta có thể chọn để phân loại các mối đe dọa khác nhau đối với hệ thống của bạn.

+ Từ chối dịch vụ

Loại tấn công thứ ba là ngăn chặn các cuộc tấn công, một ví dụ là tấn công từ chối dịch vụ (DoS). Trong cuộc tấn công này, kẻ tấn công không thực sự truy cập vào hệ thống mà chỉ đơn giản là chặn quyền truy cập vào hệ thống từ những người dùng hợp pháp. Theo lời của Trung tâm điều phối CERT (Nhóm ứng cứu khẩn cấp máy tính) (nhóm ứng phó sự cố bảo mật máy tính đầu tiên), "Một cuộc tấn công 'từ chối dịch vụ' được đặc trưng bởi một nỗ lực rõ ràng của những kẻ tấn công nhằm ngăn chặn những người dùng hợp pháp của một dịch vụ bằng cách sử dụng dịch vụ đó. " Một phương pháp chặn thường được sử dụng là làm ngập hệ thống được nhắm mục tiêu với rất nhiều yêu cầu kết nối sai đến mức nó không thể phản hồi các yêu cầu hợp pháp. DoS là một phương thức tấn công cực kỳ phổ biến, chỉ đứng sau phần mềm độc hại.

1.4 Chọn Phương pháp Tiếp cận An ninh Mạng

Các tổ chức có thể chọn từ một số cách tiếp cận đối với an ninh mạng. Một cách tiếp cận hoặc mô hình cụ thể sẽ ảnh hưởng đến tất cả các quyết định bảo mật tiếp theo và thiết lập âm thanh cho cơ sở hạ tầng an ninh mạng của toàn tổ chức.

+ Phương pháp tiếp cận bảo mật ngoại vi

Trong cách tiếp cận bảo mật theo chu vi, phần lớn các nỗ lực bảo mật đều tập trung vào chu vi của mạng. Trọng tâm này có thể bao gồm tường lửa, máy chủ proxy, chính sách mật khẩu và bất kỳ công nghệ hoặc quy trình nào khiến khả năng

truy cập trái phép vào mạng ít xảy ra hơn. Ít hoặc không có nỗ lực nào được thực hiện để bảo mật các hệ thống trong mạng. Trong cách tiếp cận này, vành đai được bảo đảm, nhưng các hệ thống khác nhau trong vành đai đó thường dễ bị tổn thương.

1.5 Kết luận chương

Các mối đe dọa đối với mạng ngày càng tăng. Chúng tôi đang thấy sự gia tăng về số lượng các cuộc tấn công hack và vi rút, cũng như các hình thức tấn công khác. Chương này đã giới thiệu cho bạn các khái niệm cơ bản về an ninh mạng, các lớp nguy hiểm chung và thuật ngữ bảo mật cơ bản. Các chương tiếp theo sẽ trình bày chi tiết về thông tin này.

Chương 2 – TẤN CÔNG MẠNG

Tóm tắt: *Mô tả các cuộc tấn công mạng phổ biến nhất, bao gồm tấn công Session, tấn công vi rút, phần mềm mã độc Trojan, từ chối dịch vụ và tràn bộ đệm, giải thích cách thực hiện các cuộc tấn công này, xác định các biện pháp phòng thủ cơ bản chống lại các cuộc tấn công đó, cấu hình hệ thống để ngăn chặn các cuộc tấn công từ chối dịch vụ.*

2.1 Giới thiệu

+ Hiểu các cuộc tấn công từ chối dịch vụ:

Khái niệm cơ bản của cuộc tấn công từ chối dịch vụ dựa trên thực tế là bất kỳ thiết bị nào cũng có giới hạn hoạt động. Thực tế này áp dụng cho tất cả các thiết bị, không chỉ hệ thống máy tính.

+ DoS in Action

Khái niệm về một cuộc tấn công từ chối dịch vụ rất đơn giản; tuy nhiên, hầu hết các nguyên tắc sẽ dễ nắm bắt hơn nếu người ta có thể xem một ví dụ cụ thể. Trong trường hợp này, bạn cần một cách an toàn để mô phỏng một cuộc tấn công DoS trong môi trường lớp học hoặc phòng thí nghiệm.

Nói chung, các phương pháp được sử dụng cho các cuộc tấn công DoS phức tạp hơn đáng kể so với hình minh họa. Mặc dù tất cả các cuộc tấn công DoS đều tìm cách làm quá tải máy mục tiêu, nhưng có rất nhiều cách để làm điều đó và có nhiều cách khác nhau để bắt đầu cuộc tấn công.

Khái niệm cơ bản đằng sau một cuộc tấn công DoS rất đơn giản. Vấn đề thực sự đối với kẻ tấn công là tránh bị bắt. Phần tiếp theo xem xét một số kiểu tấn công DoS cụ thể và xem xét các nghiên cứu điển hình cụ thể.

+ Tấn công Smurf

Cuộc tấn công Smurf là một kiểu tấn công DoS phổ biến. Nó được đặt tên theo ứng dụng lần đầu tiên được sử dụng để thực hiện cuộc tấn công này. Trong cuộc tấn công Smurf, một gói ICMP được gửi đến địa chỉ quảng bá của một mạng, nhưng địa chỉ trả về của nó đã bị thay đổi để phù hợp với một trong các máy tính trên mạng đó, rất có thể là một máy chủ chính.

+ Từ chối dịch vụ phản ánh phân tán

Như đã nêu trước đây, các cuộc tấn công từ chối dịch vụ phân tán đang trở nên phổ biến hơn. Hầu hết các cuộc tấn công như vậy dựa vào việc có được nhiều máy khác nhau (máy chủ hoặc máy trạm) để tấn công mục tiêu. Từ chối dịch vụ phản ánh phân tán (DRDoS) là một kiểu tấn công DoS đặc biệt. Như với tất cả các cuộc tấn công như vậy, nó được thực hiện bằng cách hacker có được một số máy để tấn công mục tiêu đã chọn.

+ Công cụ DoS

Một lý do khiến các cuộc tấn công DoS ngày càng trở nên phổ biến là do một số công cụ có sẵn để thực hiện các cuộc tấn công DoS. Các công cụ này có sẵn rộng rãi trên Internet và trong hầu hết các trường hợp đều được tải xuống miễn phí. Điều này có nghĩa là bất kỳ quản trị viên thận trọng nào cũng nên biết về chúng. Ngoài việc sử dụng rõ ràng chúng như một công cụ tấn công, chúng

+ Bảo vệ chống lại xâm nhập Session

Một hình thức tấn công khác là tấn công Session hoặc chiếm quyền điều khiển. Chiếm quyền điều khiển phiên TCP là một quá trình mà tin tặc chiếm quyền điều khiển phiên TCP giữa hai máy. Bởi vì xác thực thường chỉ được thực hiện khi bắt đầu phiên TCP, điều này cho phép hacker xâm nhập vào luồng giao tiếp và kiểm soát phiên.

+ Các Virút

Theo định nghĩa, virus máy tính là một chương trình tự sao chép. Nói chung, virus cũng có một số chức năng khó chịu khác, nhưng khả năng tự sao chép và lây lan nhanh chóng là những dấu hiệu nổi bật của nó. Sự phát triển này, trong và của chính nó, có thể là một vấn đề đối với một mạng bị nhiễm. Giun là loại virus có thể nhân lên mà không cần sự tương tác của con người.

+ Virus lây lan như thế nào?

Bạn đã thấy vi-rút có thể tác động đến hệ thống bị nhiễm như thế nào và đã xem xét một vài trường hợp thực tế. Rõ ràng chìa khóa để ngăn chặn vi rút máy tính là ngăn không cho nó lây lan sang các máy tính khác.

+ Phần mềm mã độc Trojan

Bạn đã thấy thuật ngữ *ngựa thành Troy* được sử dụng trong chương này, và bạn có thể đã biết nó là gì. Phần mềm mã độc Trojan là một chương trình trông có vẻ lành tính nhưng thực chất lại có mục đích xấu. Bạn có thể nhận hoặc tải xuống một chương trình có vẻ là một trò chơi hoặc tiện ích kinh doanh vô hại.

2.3 Giải pháp bảo mật SQL Server

2.3.1 Giới thiệu CSDL SQL Server

SQL Server là một hệ thống quản trị cơ sở dữ liệu quan hệ (RDBMS-Relation Database Management System) do Microsoft phát hành, sử dụng các lệnh Transact- SQL để trao đổi dữ liệu giữa Client PC và Server.

Một số đặc tính của SQL Server:

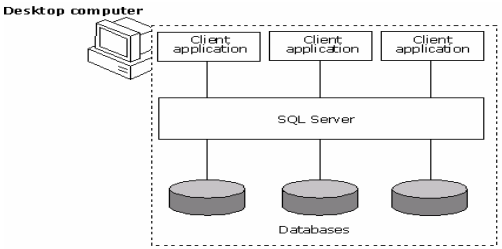
Có hệ thống phân quyền bảo mật tương thích đối với hệ thống bảo mật của công nghệ NT (Network Technology) và tích hợp với hệ thống bảo mật của Windows NT hoặc sử dụng hệ thống bảo vệ độc lập của SQLServer.

Hỗ trợ trong việc triển khai CSDL phân tán và phát triển ứng dụng trên mạng internet.

Kết nối qua mạng diện rộng: Thông qua đường truyền trên mạng xa để kết nối đến SQL Server.

Kết nối qua mạng Internet: Các ứng dụng kết nối thông qua máy chủ Internet, các dịch vụ IIS để thực hiện ứng dụng trên Internet (ví dụ C#.NET, VB.NET,...).

Trên một máy desktop thì sơ đồ kết nối trao đổi dữ liệu được thể hiện:



Hình 2.7 Mô hình desktop.

Theo mô hình này thì trên một desktop có nhiều ứng dụng và mỗi ứng dụng có thể thực hiện thao tác với nhiều CSDL khác nhau.

SQL Server sử dụng kỹ thuật SSL để thực hiện việc kết nối giữa client và server. Được phát triển bởi Netscape, ngày nay giao thức Secure Socket Layer (SSL) đã được sử dụng rộng rãi trên World Wide Web trong việc xác thực và mã hoá thông tin giữa client và server.

2.4. Kết luận chương

Chương này đã xem xét các mối đe dọa phổ biến nhất đối với hệ thống của bạn: tấn công vi rút, tấn công từ chối dịch vụ, phần mềm mã độc Trojan, chiếm quyền điều khiển phiên và tấn công tràn bộ đệm.

Trong mỗi trường hợp, các cơ chế phòng vệ khác nhau thuộc một trong hai loại: kỹ thuật hoặc thủ tục. Phòng vệ kỹ thuật là những hạng mục bạn có thể cài đặt hoặc cấu hình để làm cho hệ thống của mình an toàn hơn.

Chương 3 - **XÂY DỰNG ỨNG DỤNG BẢO MẬT CƠ SỞ DỮ LIỆU**

Tóm tắt: *Chương 3 Chương này đã tìm hiểu sơ lược về một trung tâm tích hợp dữ liệu, các vấn đề an ninh an toàn thường gặp phải, nghiên cứu một số giải pháp đã áp dụng trong việc đảm bảo an ninh cho trung tâm và cuối cùng là mục đích chính của luận văn.*

3.1. Giới thiệu hệ thống tích hợp dữ liệu

3.2. Giải pháp đảm bảo an toàn tại trung tâm

3.3. Phân tích ứng dụng

3.4. Phương pháp bảo mật cơ sở dữ liệu

Xây dựng tầng CSDL trung gian

Trong mô hình này, một CSDL trung gian (proxy) được xây dựng giữa ứng dụng và CSDL gốc (Sơ đồ 1). CSDL trung gian này có vai trò mã hóa dữ liệu trước khi cập nhật vào CSDL gốc, đồng thời giải mã dữ liệu trước khi cung cấp cho ứng dụng.

Sử dụng cơ chế sẵn có trong CSDL

1. Người sử dụng chỉ được quyền đọc dữ liệu ở dạng mã hóa (ciphertext). Quyền này phù hợp với những đối tượng cần quản lý CSDL mà không cần đọc nội dung dữ liệu.

2. Người sử dụng được quyền đọc dữ liệu ở dạng giải mã (plaintext).

Giải pháp nêu trên có lợi điểm đơn giản, dễ phát triển. Tuy nhiên, do các giới hạn về cơ chế view, trigger và cách thức quản trị dữ liệu, giải pháp này có những hạn chế sau:

Bảo vệ ứng dụng Máy trạm

+ Phát hiện và ngăn chặn chương trình độc hại:

Phát hiện và ngăn chặn chương trình độc hại thông thường được thực hiện bởi các ứng dụng bảo mật riêng rẽ như tường lửa, chống virus và chống spyware.

Tường lửa và khả năng kiểm soát chương trình - là chức năng quan trọng nhất bởi vì nó có thể kiểm soát được luồng tin đi vào/ra ở vùng nhân. Chỉ có tường lửa mới có thể ngăn được truy cập trái phép như mã độc, kiểm soát chương trình nào được phép truy cập mạng, và làm cho các máy trạm trở nên "vô hình" đối với hacker.

Bảo mật Web Service

Do ứng dụng thực hiện trao đổi thông tin trên mô hình Web Service nên việc bảo mật Web Service có thể áp dụng ở ba cấp độ:

Platform/transport-level (point-to-point) security.

Application-level (custom) security.

Message-level (end-to-end) security.

Mỗi phương pháp tiếp cận đều có những ưu, nhược điểm khác nhau, việc lựa chọn phương pháp phụ thuộc vào các đặc điểm của kiến trúc và nền tảng liên quan đến việc trao đổi thông điệp.

1. Platform/Transport Level (Point-to-Point) Security:

Các kênh vận chuyển giữa hai thiết bị đầu cuối (Web Service Client và Web Service) có thể sử dụng ở việc bảo mật giữa điểm - điểm.

- Một ứng dụng có thể sử dụng tiêu đề SOAP tùy chỉnh để xác thực thông tin với mỗi yêu cầu của Web service. Một cách chung hơn là qua ticket (hay giấy phép) trong tựa đề SOAP.

Đây là cách tiếp cận linh hoạt mềm dẻo và mạnh mẽ nhất và được sử dụng trong các Web service Exhancements cho .NET

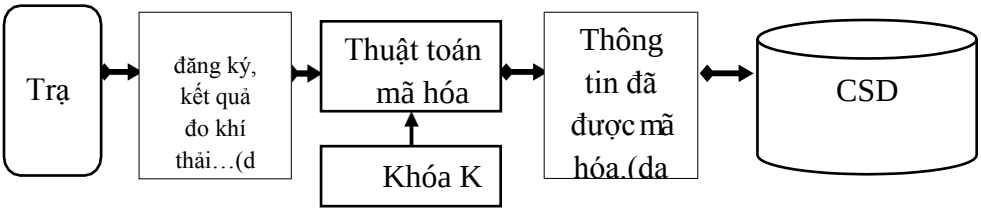
WS-Security mô tả thông số kỹ thuật cải tiến thông điệp SOAP, cung cấp tính toàn vẹn, bảo mật thông điệp và xác thực.

Xác thực được cung cấp trong thẻ bảo mật theo tiêu đề SOAP. Không có kiểu đặc tả nào của token được yêu cầu bởi WS-Security.

Bảo mật dữ liệu tại Cơ sở dữ liệu

Bảo mật dữ liệu tại Cơ sở dữ liệu tức là những thông tin được lưu trong Cơ sở dữ liệu phải được mã hóa để những người không có thẩm quyền không thể xem được. Do đó ứng dụng cần phải đáp ứng được những công việc như:

Mã hóa dữ liệu trước khi chèn vào CSDL:



Hình 3.1 Mã hóa dữ liệu trước khi chèn vào Cơ sở dữ liệu.

Tất cả các thông tin về đăng ký kiểm định, thông tin liên quan đến phương tiện đăng ký và các kết quả đo khí thải sẽ được mã hóa bằng thuật toán AES và lưu trong Cơ sở dữ liệu.

Quá trình chèn dữ liệu vào CSDL gồm có 3 giai đoạn chính:

1. Giai đoạn lấy thông tin từ bên Client gửi đến.
2. Giai đoạn sử dụng thuật toán mã hóa AES để mã hóa dữ liệu gửi đến với khóa K.
3. Giai đoạn lấy dữ liệu đã được mã hóa chèn vào CSDL.

Hiển thị dữ liệu trong Cơ sở dữ liệu sau khi đã được mã hóa:

Khi Trạm cần truy xuất thông tin đã đăng ký của một phương tiện thì cần truy xuất thông tin của phương tiện đó trên Văn phòng Cục, Thông tin trên cục do Web Service gửi về dưới dạng mã hóa (do thông tin lưu trong Cơ sở dữ liệu ở dưới dạng mã hóa).

Do đó quá trình thực hiện bao gồm có những bước sau:

1. Thứ nhất là lấy dữ liệu dưới dạng bãn mã trong Cơ sở dữ liệu.
2. Thứ hai là sử dụng thuật toán giải mã AES để giải mã dữ liệu vừa lấy với

   khóa giải mã K" người dùng nhập vào.
3. Thứ ba là hiển thị dữ liệu đã được giải mã.

Lấy thông tin khóa bí mật:

Thông tin khóa bí mật K sẽ được lưu dưới dạng file mã hóa trong các thiết bị lưu trữ như USB, CD, thẻ nhớ,...hoặc có thể nhập trực tiếp khóa khi chương trình yêu cầu.

Phân ra hai trường hợp chính:

Trường hợp nhập trực tiếp khóa vào trong chương trình, chương trình sẽ yêu cầu nhập khóa sau khi xác thực thành công.

Cụ thể như sau:

a. Quá trình tạo file khóa lưu trong thiết bị có serial như thẻ nhớ, USB,…

Lấy ra ID của thiết bị. Chọn ra một khóa được chỉ định kết hợp với thông tin GUID của ứng dụng rồi lưu vào file khóa (key.txt).

Mã hóa file khóa bằng thuật toán AES với khóa là ID của thiết bị.

Lưu file khóa lại ứng với thiết bị đó.

b. Quá trình lấy ra khóa trong thiết bị

3.5 DEMO về chương trình

- Nhập tên đăng nhập, mật khẩu, thông tin trạm đo:

Hình 3.2 Đăng nhập.

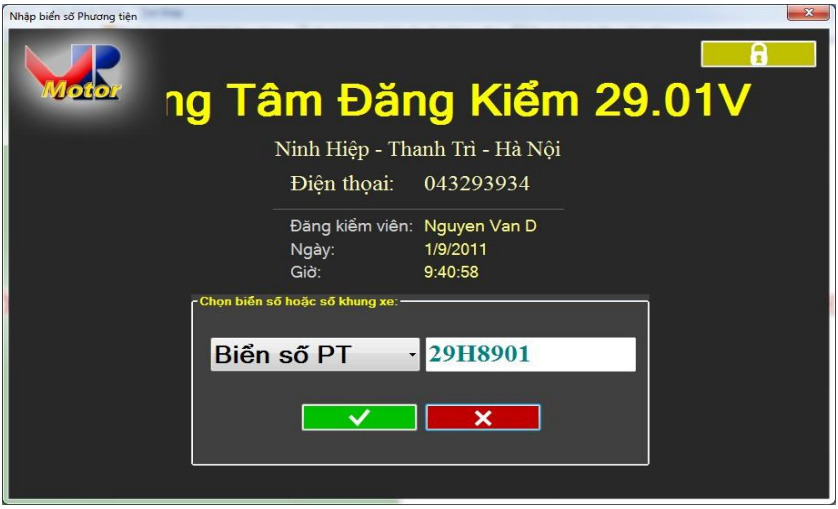
Quá trình xác thực diễn ra, quá trình này gồm có hai công đoạn chính là:

1. Xác thực Máy trạm với Máy chủ sử dụng kỹ thuật xác thực SSL.
2. Xác thực người dùng.

Nếu quá trình này thành công thì vào được chương trình, không thì không được vào. Khi đăng nhập thành công thì chương trình hiển thị hộp thoại yêu cầu nhập khóa bí mật.

Nếu bỏ qua bước nhập khóa bí mật hoặc nhập không đúng (khóa bí mật sẽ không được xác thực) thì vẫn vào được chương trình nhưng sẽ không thể thực hiện được chức năng nào như đăng ký mới phương tiện đến kiểm định hoặc đo khí thải của phương tiện.

- Tiến hành đăng ký kiểm định:

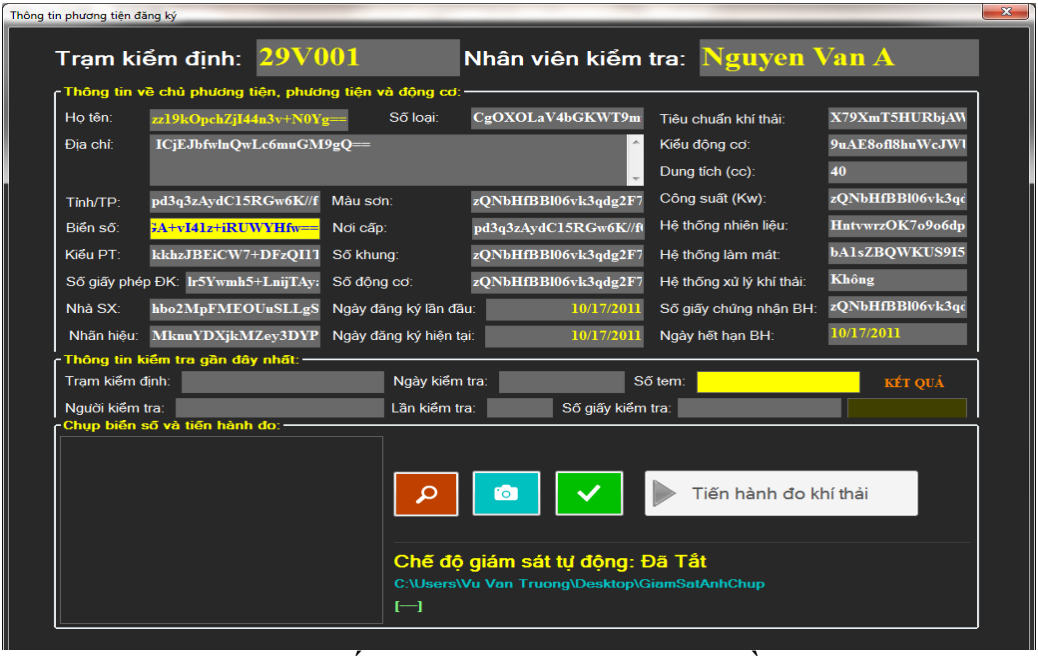


Hình 3.3 Đăng ký kiểm định.

- Thông tin phương tiện đã đăng ký:

Đối với trường hợp chưa nhập khóa bí mật thì do thông tin về biển số của phương tiện được lưu dưới dạng mã hóa trong cơ sở dữ liệu cho nên ở đây giả sử biết được thông tin biển số đã được mã hóa của một phương tiện bất kỳ thì khi nhập thông tin biển số (dạng đã mã hóa của phương tiện như xHna9ja==) thì thông tin đăng ký của phương tiện sẽ lấy ở cục về chưa được giải mã được hiển thị.

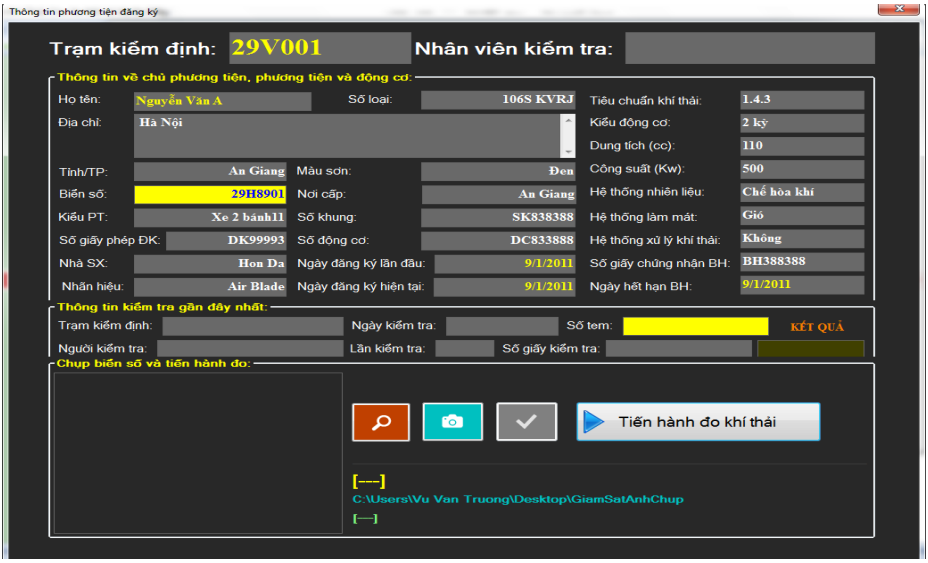
Ngược lại đối với trường hợp khóa bí mật được nhập chính xác thì để tiến hành kiểm định thì chỉ việc nhập biển số thì thông tin biển số sẽ được mã hóa bằng khóa bí mật và so sánh



trong cơ sở dữ liệu, nếu đúng thì Server sẽ trả về thông tin đăng ký của phương tiện dưới dạng mã hóa và thông tin này sau đó sẽ được giải mã bằng khóa bí mật để hiển thị trên màn hình.

Hình 3.4 Thông tin phương tiện đã đăng ký chưa giải mã.

Thông tin phương tiện đã đăng ký là thông tin được lấy từ Văn phòng Cục (đã mã hóa) về Trạm, sau đó được giải mã để hiển thị.



Hình 3.5 Thông tin phương tiện đã đăng ký đã giải mã.

Tương tự, sau khi đo kiểm định khí thải thì thông tin về kết quả kiểm định cũng được mã hóa trước khi gửi lên mạng qua Web Service, sau đó thông tin mã hóa được gửi lên Văn phòng Cục và lưu trong Cơ sở dữ liệu.

3.6 Kết luận chương

Trong những năm gần đây việc kiểm định và kiểm định khí thải ô tô, xe máy là việc rất quan trọng, năm trong chương trình làm giảm hiệu ứng nhà kính, giảm bớt xe ô tô, xe máy đã quá hạn sử dụng, không đảm bảo chất lượng khí thải khi tham gia giao thông.

Chương 3 ứng dụng một số giải pháp được nghiên cứu tại chương 2 để xây dựng ứng dụng, đảm bảo một số yêu cầu cơ bản về bảo vệ, bảo mật thông tin (ở đây là bảo mật CSDL ứng dụng).

KẾT LUẬN

Bảo đảm An toàn và Bảo mật cho Trung tâm tích hợp dữ liệu là một vấn đề đã và đang được quan tâm. Luận văn đã nghiên cứu một số giải pháp đảm bảo an ninh bao gồm an toàn và bảo mật cho Trung tâm tích hợp dữ liệu và ứng dụng một trong số những giải pháp đó xây dựng ứng dụng đảm bảo an ninh cho chương trình kiểm định khí thải cho Cục Dự trữ Nhà nước khu vực Hà Nội.

Tuy chương trình đã đạt được một số yêu cầu đặt ra. Nhưng việc bảo vệ thông tin chưa tiến hành triệt để như triển khai VPN để bảo vệ thông tin theo hướng truyền,... chương trình chỉ dừng lại việc thiết lập bảo vệ Cơ sở dữ liệu riêng lẻ, chưa có đồng bộ giữa các Máy chủ Cơ sở dữ liệu.

Mục đích của đề tài mới chỉ tập trung vào nghiên cứu một số vấn đề đảm bảo an toàn và bảo mật thông tin trong một trung tâm tích hợp dữ liệu nhỏ, ở đây là trung tâm của Cục Dự trữ Nhà nước khu vực Hà Nội. Trong tương lai sẽ cải tiến các tính năng của chương trình đáp ứng được một số vấn đề đã nêu trong phần hạn chế.