

Bài tập thực hành 1

1. Dựa vào kết quả khảo sát của bệnh viện Trung Ương Huế, hãy mô tả các thành phần cấu tạo CSHT CNTT của bệnh viện bao gồm:

a) Phần cứng:

Mạng nội bộ: Hệ thống đường dây và các thiết bị đính kèm, công nghệ cáp quang (3 đường dây chính – backbone)

Máy chủ: Để đảm bảo an toàn dữ liệu, hệ thống có một máy chủ chính và một máy backup. Hệ thống sao lưu dữ liệu được thực hiện qua máy con và CD-ROM hàng ngày.

Máy con: Khoảng 50 máy con tham gia vào hệ thống mạng, phục vụ các bộ phận và nhân viên trong bệnh viện.

Nguồn điện: Các bộ thiết bị mạng và máy tính đều được gắn vào hệ thống điện ưu tiên và hệ thống lưu trữ điện của bệnh viện.

b) Phần mềm:

Chương trình quản lý bệnh nhân: Tích hợp các chức năng quản lý từ lúc nhập viện đến khi ra viện, với việc cấp số nhập viện và tem nhập viện để quản lý chính xác và thuận tiện. Lưu trữ toàn bộ dữ liệu chuyên môn, phục vụ báo cáo và quản lý toàn bộ hoạt động của các khoa phòng.

Chương trình thu phí: Áp dụng hình thức thu phí tạm ứng nhiều lần và thanh toán một lần, công khai chi phí cho bệnh nhân và thực hiện chế độ miễn giảm cho đối tượng chính sách. Giúp quản lý tài chính bệnh viện minh bạch và hiệu quả.

Chương trình quản lý dược: Giúp quản lý lượng thuốc nhập, xuất, tồn hàng ngày, đảm bảo việc phân bổ thuốc cho bệnh nhân và các khoa phòng một cách chính xác và cập nhật.

c) Tài nguyên mạng:

Mạng nội bộ: Hệ thống mạng cáp quang với đường backbone chính bao phủ diện tích rộng lớn, kết nối tất cả máy con, máy chủ và các tòa nhà trong khu vực.

Hệ thống bảo mật: Các biện pháp bảo vệ mạng khỏi truy cập trái phép và giữ an toàn cho dữ liệu bệnh nhân, bao gồm hệ thống tường lửa, phần mềm chống virus, và mã hóa dữ liệu.

d) Dịch vụ khác

Hệ thống điện ưu tiên: Cung cấp nguồn điện ổn định và liên tục cho các thiết bị mạng, máy chủ, và máy con, đảm bảo hệ thống vận hành 24/7.

Hệ thống sao lưu và phục hồi dữ liệu: Hỗ trợ khôi phục dữ liệu trong trường hợp mất mát, đảm bảo dữ liệu bệnh viện được bảo vệ và dễ dàng khôi phục khi cần.

Dịch vụ hỗ trợ kỹ thuật: Đảm bảo hệ thống luôn được bảo trì và sửa chữa kịp thời khi gặp sự cố, hỗ trợ người dùng trong vận hành phần mềm và thiết bị.

Hệ thống camera giám sát: Hệ thống camera được lắp đặt ở các khu vực quan trọng như cổng ra vào, hành lang, khu vực điều trị và phòng lưu trữ hồ sơ, nhằm đảm bảo an toàn cho bệnh nhân, nhân viên, và tài sản của bệnh viện.

Thiết bị kiểm soát ra vào: Ở các khu vực chỉ cho phép nhân viên vào, có thể lắp đặt máy quét thẻ, máy quét vân tay, cửa tự động để giới hạn truy cập. Chỉ nhân viên được cấp quyền mới có thể vào các khu vực này, chẳng hạn như kho thuốc hay phòng lưu trữ hồ sơ y tế.

2. Trình bày tổng quan (khái niệm, phương thức hoạt động, chức năng) về các chủ đề sau:

a) Giao thức thực hiện bảo mật (protocol) Kerberos.

Khái niệm

Secure Socket Layer (SSL) là một giao thức bảo mật mã hóa kênh truyền giữa máy khách và máy chủ trên internet, đặc biệt phổ biến trong các giao dịch web. SSL đã phát triển thành Transport Layer Security (TLS), một phiên bản bảo mật cao hơn và được sử dụng rộng rãi ngày nay.

Phương thức hoạt động

SSL hoạt động thông qua việc sử dụng mã hóa bắt đối xứng và một chứng chỉ số (digital certificate) để đảm bảo tính toàn vẹn và bảo mật của kênh truyền:

1. **Bắt tay SSL (SSL Handshake):** Quá trình này bắt đầu khi máy khách kết nối đến máy chủ bằng cách yêu cầu một kết nối an toàn. Máy chủ sẽ gửi chứng chỉ SSL để xác thực danh tính.
2. **Thỏa thuận khóa phiên (Session Key Agreement):** Sau khi xác thực, cả hai bên sử dụng mã hóa bất đối xứng để tạo khóa phiên chung (symmetric key) dùng cho việc mã hóa toàn bộ phiên.
3. **Truyền thông mã hóa:** Toàn bộ dữ liệu truyền qua lại sau đó được mã hóa bằng khóa phiên để bảo đảm an toàn.

Chức năng

- **Mã hóa dữ liệu:** Đảm bảo rằng dữ liệu truyền tải không thể bị đọc trộm.
- **Xác thực máy chủ:** Bằng chứng nhận, người dùng có thể tin tưởng máy chủ họ đang kết nối.
- **Bảo vệ toàn vẹn dữ liệu:** Đảm bảo dữ liệu không bị thay đổi trong quá trình truyền.

b) Giao thức thực hiện bảo mật (protocol) Secure Socket Layer (SSL).

Khái niệm

Kerberos là một giao thức xác thực mạng nhằm bảo vệ các dịch vụ mạng khỏi các cuộc tấn công dựa trên giả mạo. Được phát triển bởi Viện Công nghệ Massachusetts (MIT), giao thức này sử dụng mã hóa đối xứng và một hệ thống cấp phát "vé" (tickets) để xác minh danh tính người dùng trong mạng máy tính.

Phương thức hoạt động

Kerberos hoạt động dựa trên một mô hình “trusted third-party” (bên thứ ba đáng tin cậy), trong đó Key Distribution Center (KDC) đóng vai trò là trung tâm phân phối khoá bí mật và là thành phần chủ yếu. Quá trình xác thực diễn ra như sau:

1. Người dùng gửi yêu cầu đến KDC để lấy vé chứng thực (Ticket Granting Ticket - TGT).
2. KDC gửi lại TGT cho người dùng nếu thông tin đăng nhập hợp lệ.
3. Khi người dùng cần truy cập dịch vụ, họ sẽ dùng TGT để lấy vé truy cập từ KDC.
4. Người dùng cung cấp vé này cho dịch vụ để xác minh và được phép truy cập.

Chức năng

- **Xác thực:** Đảm bảo rằng chỉ người dùng hợp lệ mới có quyền truy cập vào tài nguyên.
- **Bảo mật truyền thông:** Thông qua việc mã hóa các vé và dữ liệu xác thực.
- **Giảm thiểu rủi ro rò rỉ mật khẩu:** Vì người dùng không gửi trực tiếp mật khẩu qua mạng.

c) Giao thức thực hiện bảo mật (protocol) PGP.

Khái niệm

PGP là một phương thức mã hóa và giải mã dữ liệu, nổi bật trong việc bảo mật email và file. Được phát triển bởi Phil Zimmermann, PGP sử dụng một sự kết hợp của mã hóa khóa công khai và khóa riêng tư để bảo mật và xác thực dữ liệu.

Phương thức hoạt động

PGP hoạt động bằng cách sử dụng cặp khóa (public key và private key):

1. **Mã hóa email:** Người gửi sử dụng public key của người nhận để mã hóa email. Chỉ người nhận có private key tương ứng mới có thể giải mã.
2. **Ký số (Digital Signature):** Để đảm bảo tính xác thực, người gửi có thể ký số email bằng private key của mình. Người nhận sau đó có thể kiểm tra chữ ký này bằng public key của người gửi.
3. **Bảo mật lai (Hybrid Encryption):** PGP sử dụng mã hóa lai để tăng cường hiệu suất, tức là chỉ mã hóa khóa phiên bằng RSA (asymmetric) và sử dụng một thuật toán mã hóa đối xứng như AES để mã hóa dữ liệu.

Chức năng

- **Mã hóa nội dung:** Bảo mật nội dung thư điện tử và file trước sự truy cập trái phép.
- **Chữ ký số:** Đảm bảo tính xác thực của người gửi và toàn vẹn dữ liệu.
- **Quản lý khóa:** Cho phép người dùng trao đổi và quản lý khóa công khai một cách an toàn

d) Giao thức thực hiện bảo mật (protocol) S/MIME

Khái niệm

S/MIME là một tiêu chuẩn để bảo mật email, cung cấp các dịch vụ như xác thực, tính toàn vẹn dữ liệu, không thể phủ nhận, và mã hóa. Được phát triển bởi RSA Data Security, S/MIME dựa trên MIME để hỗ trợ mã hóa và chữ ký số cho email.

Phương thức hoạt động

S/MIME sử dụng một cơ sở hạ tầng khóa công khai (PKI) để quản lý và phân phối khóa:

- Mã hóa email:** Email và các tập tin đính kèm được mã hóa bằng cách sử dụng khóa công khai của người nhận.
- Chữ ký số:** Người gửi ký số email bằng khóa riêng của mình, và người nhận có thể xác minh tính xác thực của email bằng khóa công khai của người gửi.
- Chứng chỉ số:** Để xác thực danh tính của người gửi, S/MIME sử dụng chứng chỉ số được cấp bởi các tổ chức chứng nhận (Certificate Authorities - CA).

Chức năng

- Mã hóa nội dung:** Bảo vệ nội dung email khỏi việc bị đọc trộm.
- Chữ ký số:** Xác thực danh tính của người gửi, đảm bảo tính toàn vẹn của email.
- Khả năng tích hợp:** Được hỗ trợ rộng rãi trên các ứng dụng email như Microsoft Outlook, Apple Mail, giúp tăng cường bảo mật cho truyền thông qua email.