논문 2012-50-3-21

3차원 의료영상시스템을 위한 웹 PACS 기반 보안전송모듈의 설계 및 성능평가

(Design and Performance Evaluation of the Secure Transmission Module for Three-dimensional Medical Image System based on Web PACS)

김 정 채*, 유 선 국**

(Jungchae Kim and Sun Kook Yoo)

요 약

PAC는 디지털 의료영상을 위한 의료 시스템이며 PACS가 공용 네트워크를 이용한 웹 기반 서비스로 확장 될 수 있다. 이 경우 DICOM 파일은 개인의무기록을 포함하고 있기 때문에 악의적 사용자의 공격으로부터 보호되어야 한다. 그 위험성을 해결하기 위하여 우리는 유연한 IPSec을 이용하는 보안전송 시스템을 설계하였고, 웹 기반의 3차원 의료영상 시스템에 적용하였다. 그리고 대용량 DICOM 데이터 전송 시 적용되는 암호화 및 무결성 알고리즘을 변경하며 개발 된 시스템의 성능평가를 수행하였다. 이 때, 사용 된 알고리즘의 조합은 DES-MD5, DES-SHA1, 3DES-MD5, 그리고 3DES-SHA1이며, 암호화 전송은 실험을 위한 테스트베드에서 수행하였다. 실험 결과, 암호화를 적용하지 않은 경우에 비교하여 전반적으로 암호화 알고리즘에 의하여 영향을 받았다. DES의 경우 약 50%의 전송성능 저하를 보였으며, 3DES의 경우 약 65%의 전송성능 저하를 보였다. 또한 DICOM 볼륨데이터 전송 시 패킷 증가에 의한 오버헤드로 인한 네트워크 성능 감소가 발생함을 확인하였다. 결론적으로, 보안전송 시스템에 의한 메시지의 안전한 교환을 보장하기위한 서버 및 네트워크 성능의 저하가 발생하였다. 따라서 반드시 보호 되어야 할 의료영상에 대해서만 보안전송을 구성한다면 서버의 성능 저하 문제를 해결함과 동시에 안전한 웹 PACS를 구성 할 수 있을 것이다.

Abstract

PACS is a medical system for digital medical images, and PACS expand to web-based service using public network, DICOM files should be protected from the man-in-the-middle attack because they have personal medical record. To solve the problem, we designed flexible secure transmission system using IPSec and adopted to a web-based three-dimensional medical image system. And next, we performed the performance evaluation changing integrity and encryption algorithm using DICOM volume dataset. At that time, combinations of the algorithm was 'DES-MD5', 'DES-SHA1', '3DES-MD5', and '3DES-SHA1, and the experiment was performed on our test-bed. In experimental result, the overall performance was affected by encryption algorithms than integrity algorithms, DES was approximately 50% of throughput degradation and 3DES was about to 65% of throughput degradation. Also when DICOM volume dataset was transmitted using secure transmission system, the network performance degradation had shown because of increased packet overhead. As a result, server and network performance degradation occurs for secure transmission system by ensuring the secure exchange of messages. Thus, if the secure transmission system adopted to the medical images that should be protected, it could solve server performance gradation and compose secure web PACS.

Keywords : Web PACS, DICOM, IPSec, Secure network

* 학생회원, 연세대학교 일반대학원 생체공학협동과정
(Graduate School of Biomedical Engineering, Yonsei University, Seoul, Korea)
** 정회원, 연세대학교 의과대학 의학공학교실
(Department of Medical Engineering, College of Medicine, Yonsei University, Seoul, Korea)
※ 본 연구는 2012년도 정부(교육과학기술부) 한국연구재단(No. 2010-0023833), 지식경제부 한국산업기술진흥원의 전략기술인력양성사업(No.2012-8-1382)과 산업융합원천기술개발사업(10031977)으로 지원된 연구결과입니다.
접수일자:2012년12월4일, 수정완료일:2013년2월27일

Ⅰ. 서 론

의료 영상은 방사선 및 초음파 촬영에 의한 결과물로써 임상에서 환자의 질병에 대한 판단에 매우 중요한 역할을 한다. 이를 활용하기 위한 PACS (Picture Archiving and Communication System)는 디지털 의료 영상을 저장, 전송, 관리, 조회 할 수 있는 시스템이며, 현재까지 대형 병원을 중심으로 보급이 활발히 이루어져 필름을 이용한 과거의 진단 방식을 대체하고 있다. PACS에서 사용되는 의료영상은 DICOM(Digital Imaging and Communications in Medicine) 표준 기반의 파일 구조와 전송 프로토콜 및 의료 영상 처리와 관련 된 기술을 포함하고 있다. 특히, DICOM 파일에는 촬영 영상과 함께 환자의 개인정보, 그리고 영상 판독 결과 등을 저장 할 수 있다.[1,3] 이는, PACS에서 활용되는 DICOM 파일에 매우 중요한 개인 의료 정보가 포함되어 있음을 의미한다. 국내에서 최근 발의 된 개인의료정보보호법은 의료기록의 수집, 이용, 제공에 대한 엄격한 보안 및 관리를 요구하고 있으며, 국제적으로 HIPAA(Health Insurance Portability and Accountability Act)는 이미 전자 보건기록의 거래에 대하여 발생 할 수 있는 정보 침해를 방지하기 위한 보안 표준을 준수 할 것을 요구하고 있다.[4] 즉, 병원 정보 시스템의 디지털화로 인하여 의료 정보의 교환이 빈번하게 발생함에 따라 그 과정에서의 전송 되는 개인 의료 정보 보호에 대한 중요성이 높아지고 있는 실정이다. 그러나 HIPAA에서도 병원 내 네트워크 전송이나, 사설 전송망에서 사용 시 암호화는 옵션으로 정의하고 있으며, 국내에도 PACS와 관련한 보안과 관련 표준이 명확하게 제시되어 있지는 않은 상태이다.[2, 5] 이러한 문제에 대하여 국내에서 PACS에 대한 보안성능평가 가이드라인을 제시하고 있으나,[4, 6] 대부분 병원 내부망에서 PACS를 이용하여 전송되는 DICOM 파일에 대한 보안 수준은 방화벽에 의존하고 있는 실정이다.

Web PACS의 경우 병원 내부에서나 외부에서 PACS와 관련 된 의료 영상의 조회, 전송, 판독 등의 기능을 수행하기 위하여 사용 되는 인터페이스이다. 대부분 Full PACS를 설치하기 어려운 중소 병원의 경우 PACS Archiving 서버를 공유하고 Web PACS를 이용하여 업무를 수행하는 경우도 증가하고 있다.[3,4] 여기서 발생 할 수 있는 보안문제는 위와 같은 시스템이 증가하면서 공중망(Public Domain Network)로 DICOM 파일이 전송 될 때, 암호화되지 않은 파일의 내용이 유출 되어 악의적으로 사용 될 수 있는 가능성을 배제 할 수 없을 뿐 아니라, 방화벽 내부의 내부망에서도 악의적 사용자에 의하여 네트워크로 전송되는 DICOM 파일이 조회 및 조작 될 수 있다. 즉, 병원 내부에서도 전송되는 데이터가 암호화 되지 않으면 개인 의료 정보가 위험에 노출 될 가능성이 있다는 것이다.

본 연구에서는 PACS에 접근하여 의료영상을 조회하려는 사용자와 PACS Archiving 서버 사이에 전송되는 모든 데이터에 대하여 암호화를 수행함으로써 DICOM 파일이 저장소에서 호출 되어 전송되는 과정에서 의료정보가 유출 될 수 있는 가능성을 억제하고자 한다. 이를 위하여 Windows 서버 계열에서 사용 할 수 있는 'IPSec 제어 프로그램'을 개발하였으며, 이를 3차원 의료영상 모델링을 위한 웹 어플리케이션에 적용하였다. 위의 어플리케이션은 3차원 의료영상 모델을 이용하여 원격지의 전문의가 협진, 진단 또는 수술 계획 등에 활용하기 위한 어플리케이션이다. 특히 의료영상의 3차원 모델링은 대용량의 의료 영상 데이터 전송을 필요로 하기 때문에 개인정보를 포함한 다량의 DICOM 파일이 웹 서비스를 위해 공중망으로 전송 될 때 보호 되어야 한다.

다음 섹션에서는 본 연구에서 보안 네트워크 구성에 사용 한 IPSec(IP security protocol)을 SSL(Secure Socket Layer) / TLS(Transport Layer Security)의 특성과 비교하고 보안 네트워크 구성에 IPSec이 적합한 이유에 대하여 설명하고자 한다. Ⅲ장에서는 웹 기반 3차원 의료영상 모델링 어플리케이션에 대하여 간단히 소개하고, Ⅳ장에서 IPSec 제어 프로그램 개발과정과 Ⅴ장에서 서버 및 클라이언트 구축, 가상 시뮬레이션 환경 등 실험 방법에 대하여 설명한 다음 실험 결과 분석을 통하여 본 연구에서 구축한 암호화 시스템 성능 평가 및 분석을 통해 결론을 전개 하고자 한다.

Ⅱ. 본 론

1. IPSec과 SSL/TLS

Figure 1의 TCP/IP 프로토콜 스택을 보면, IPSec의 경우 네트워크 계층에서, SSL/TLS의 경우 전송계층에서 사용되고 있음을 확인할 수 있다. 두 프로토콜 모두 유사한 암호화(Encryption)와 인증(Authentication)에 대한 알고리즘을 이용하고 있으므로, 데이터의 암호화 방식에 는 큰 차이가 없으나 활용 방법은 차이가 있다.[8,9]

먼저, IPSec은 전송계층에서 전달되는 모든 패킷에 대하여 암호화를 제공 할 수 있으며, IP 주소 또는 포트 번호를 기반으로 암호화 패킷을 주고받을 대상을 선택할

응용계층(SSH)
전송계층(TLS/SSL)
네트워크계층(IPSec)
물리계층

그림 1. TCP/IP 프로토콜 스택과 암호화 프로토콜
Fig. 1. TCP/IP protocol stack and security protocols.

수 있다. 그리고 다양한 형태의 네트워크 토폴로지(Gateway-to-Gateway, Gateway - to-User, User - to-User)에 대하여 서비스를 제공하며, TCP와 UDP 같은 전송계층의 프로토콜이나 응용프로그램의 종류에 관계없이 보안 기능을 사용 할 수 있는 장점 있다. 그러나 라이브러리 자체를 개발함에 어려움이 있으며, 운영체제와 개발사에 따라 상호 운용이 불가능 할 수도 있는 점은 단점이라 할 수 있다.[10]

다음으로 SSL/TLS의 경우 특정 응용프로그램에 직접 포함하여 개발되는 형태이며, 특정 세션에 대한 패킷의 보안을 지원한다. 주로 웹 브라우저에서 해당 기능을 제공하기 때문에 웹 서비스 이용 시 주로활용 된다.[5] 이 경우 OpenSSL과 같은 오픈소스를 이용하여 프로젝트에 추가 할 수 있는 장점이 있으나, TCP만 사용 할 수 있다는 점과 사용자가 개발한 프로그램이나 SSL/TLS를 지원하는 응용프로그램에서만 보안 기능을 사용 할 수 있다는 단점이 있다.[7]

본 연구의 목표 시스템의 경우 기본적으로 웹 서버와의 통신은 TLS/SSL로 지원 가능하나, PACS Archiving 서버와 클라이언트 사이의 SQL 쿼리와 DICOM 파일전송은 TLS/SSL로 보안 기능을 지원하기 어려우므로 특정 네트워크 간에 보안 기능을 제공 할 수 있는 IPSec이 적합하다. 즉, 서버와 클라이언트 간 모든 패킷에 대한 암호화라는 본 연구의 목적으로는 정보 유출 가능성을 최소화하기 위하여 IPSec이 적절하다. 또한 특정 IP 대역에 대하여 동적으로 보안 네트워크를 구성 할 수 있다.

2. IPSec 제어 프로그램 개발

본 연구에서는 Windows 서버 계열에서 사용 할 수 있는 IPSec 제어 프로그램을 개발하였다. 해당 프로그램은 운영체제에 내장되어있는 IPSec 제어 클래스 및 레지스트리 구조를 설명한 Microsoft Development Network의 기술문서[10]와 기술문서에서 참조한 RFC2251[11]을 참조하여 개발하였다. 주요 함수 및 데이터구조를 Dynamic Linked Library 형태로 만들어 C++ 또는 C# 기반의 개발

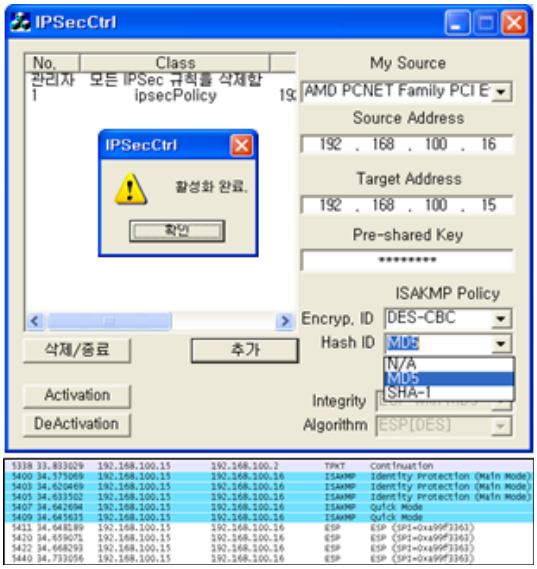

그림 2. 개발 된 IPSec 제어 프로그램
Fig. 2. The developed IPSec control manager

프로젝트에 적용 할 수 있도록 하였다.

Figure 2는 개발 된 라이브러리를 이용한 응용 프로그램의 예를 보여준다. 암호화(DES 또는 3DES)와 무결성(MD5 또는 SHA-1)을 위한 알고리즘을 선택 할 수 있도록 하였고, 암호화/복호화를 비밀키와 IPSec 규칙을 적용할 IP 주소를 입력 할 수 있도록 하였다. 본 프로그램이 정상 동작하는 것을 확인하기 위하여 PING 테스트를 수행하였으며, 그 결과 ICMP 메시지를 전송하기에 앞서 ISAKMP(Internet Security Association and Key Management Protocol)를 이용한 송수신 간 IPSec 정책 협상을 수행하는 것을 Figure 2에서 확인 할 수 있다.

3. 웹 기반 3차원 의료영상 모델링 어플리케이션 및 서비스 구성

웹 브라우저(Internet Explorer)에서 동작하는 3차원 가시화 모델링 프로그램은 Microsoft Visual Studio 2010에서 개발하였으며 .NET Framework 4.0 기반 WPF(Windows Presentation Foundation) 어플리케이션 개발 프로파일을 이용하였다. GDM2.0을 이용하여 DICOM 3.0 파일 포맷을 읽고 VTK 5.4를 이용하여 볼륨 모델을 생성하는데 활용하였다. 그리고 공중망에 연결 된 웹 서버에 사용자 등록, 권한 부여, 인증의 기능을 수행하는 사이트에 본 어플리케이션을 배포하였다. 웹 기반 3차원 가시화 모델링 응용프로그램에 사용자가 접근 할 수 있도록 웹 페이지를 생성하고, 해당 웹 페이지에서 응용프로그램이 실행 되도록 하였다.

Figure 3의 PACS Archiving 서버는 MySQL으로 데이

터베이스를 이용하여 대용량 CBCT (Cone beam Computed Tomography) 치아 데이터를 정보를 관리하도록 하였다. 그리고 서버 내부에 DICOM 파일 전송 관리 프로그램과 IPSec 제어 프로그램을 설치하고, 방화벽으로 보호 된 공중망에서 서비스 하도록 하였다.

Figure 4에 정리한 서비스 시나리오의 객체 간 메시지는 3 단계로 분류 할 수 있다. 1단계는 클라이언트가 웹 서버에 접속하여 서비스 활용 권한을 받는 단계이다. 즉, 권한을 받은 클라이언트(A,B)만 웹 서버로부터 3차원 의료영상 모델링 어플리케이션을 활용 할 수 있다. 이 때, 클라이언트(A,B)는 웹 서버로부터 공유키를 수신 받은 뒤 접속 대기 중인 상대방(A-B)의 정보를 수신 받는다. 공유키와 상대방의 IP 주소를 보유한 클라이언트는 자신의 운영체제에 필요한 IPSec 정책을 추가 및 활성화하여 클라이언트 간 암호화 네트워크를 구성 하게 된다.

2 단계에서는 클라이언트가 PACS Archiving 서버와의 IPSec 협상을 진행하고 DICOM 파일을 전송 받는 단계이다. 먼저, 웹 서버로부터 수신 받은 공유키를 이용하여 PACS Archiving 서버와의 암호화 통신을 위한 IPSec 정책을 추가하고 활성화 한다. IPSec 협상이 완료되면, 데이터베이스로부터 저장 된 DICOM 파일 목록을 호출하고 필요한 파일에 대한 전송 요청을 수행한다. PACS Archiving 서버는 비밀키를 이용하여 접속 요청을 한 클라이언트에 대해서만 인증을 수행한다.

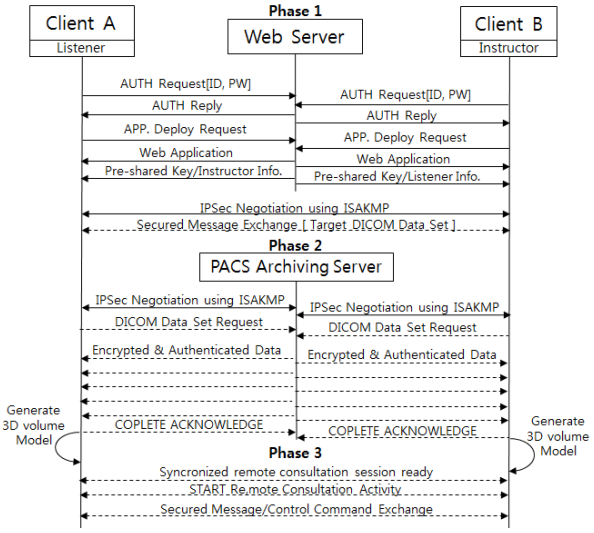

그림 4. 웹 PAC의 안전한 사용을 위한 서비스 시나리오

Fig. 4. The service scenario for secure web PACS.

이 때, IPSec 협상을 통하여 인증 받지 못한 클라이언트가 송신하는 패킷은 네트워크 계층에서 폐기한다. 클라이언트(A 또는 B)는 데이터베이스로부터 저장 된 DICOM 볼륨 데이터 세트 목록을 수신 받은 뒤 필요한 데이터 세트를 요청하면, PACS Archive 서버가 해당 데이터 세트를 클라이언트(A 또는 B)에게 TCP를 이용하여 전송한다. 이 때, 전송 시 모든 패킷에 대한 암호화 및 무결성 검사에 대한 기능은 네트워크 계층에서 담당한다.

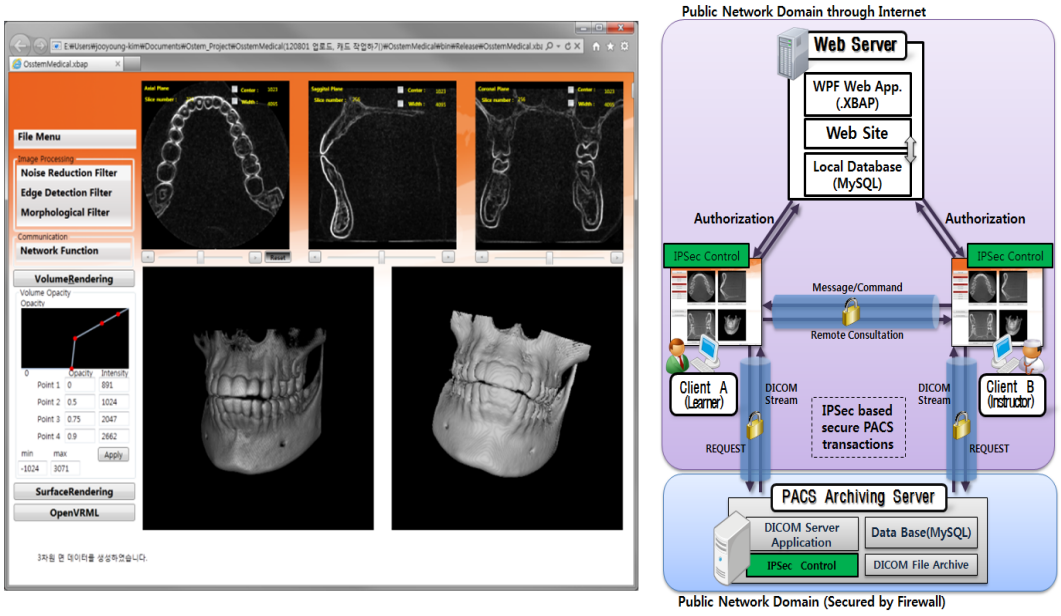

그림 3. 웹 기반 3차원 의료영상 모델링 어플리케이션 및 서비스 구성

Fig. 3. The web based 3-D medical images modeling application and the overall system architecture.

그리고 DICOM 볼륨 데이터 세트 전송 완료 후 각 클라이언트(A-B)는 동일한 세트에 대한 3차원 가시화 모델 생성 작업을 수행 할 수 있는 상태가 되며, 이때 서버와 각 사용자간의 메시지는 동적으로 구성 된 보안 네트워크에서 암호화 전송이 지원된다. 이 때, 서버는 암호화 전송을 필요로 하는 클라이언트에게 특정 IPSec 정책을 할당하여 보안 전송 서비스를 제공 할 수 있다.

Ⅲ. 실 험

1. 실험 설계

본 연구에서는 IPSec이 PACS Archiving 서버의 성능에 미치는 영향을 평가하여 제안 된 보안 시스템의 유용성을 평가하고자 한다. 객관적인 실험 환경을 보장하기 위하여 Figure 5의 테스트베드를 구축하였다. Table 1에 각 장비의 하드웨어 및 소프트웨어에 대한 상세 내용을 정리하였다. Router는 기가비트 이더넷을 지원하도록 포트 설정을 하였으며, Server와 Bridged host 역시 기가비트 이더넷을 지원해주는 NIC(Network Interface Card)를 설치하였다. 그 이유는 네트워크 대역폭을 최대로 지원하도록 함으로써, IPSec에 의한 대역폭의 변화 및 오버헤드의 변화를 정확하게 측정하기 위함이다.

Bridged host에 VMware를 설치하여 Virtual client를 생성하였으며, 클라이언트가 Virtual bridged network를 이용하여 Bridged host의 NIC를 통하여 물리적 네트워크에 접근하도록 하였다. 그러므로 Router의 측면에서 보면 Virtual client에 각각 Briged host와 다른 IP를 할당했기 때문에 각각 독립적인 단말기로 인식가능하다. 따라서 Server에 각 Virtual client에 대한 IPSec 정책을 등록 할 때 IP 주소에 따른 개별적인 정책 할당이 가능하다. 그리고 목표 시스템의 성능 평가를 위하여 Wireshark와

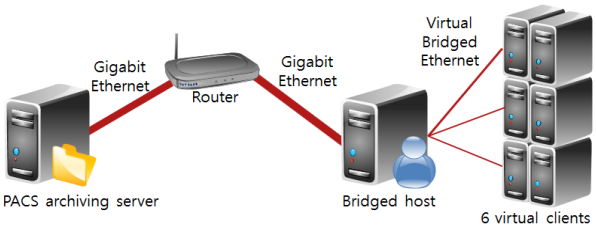

그림 5. 테스트 베드의 구성도
Fig. 5. The composition of test-bed

Server의 로그파일을 이용하였다. 실험1)은 Jperf를 이용하여 구성 된 테스트 베드의 네트워크 성능을 측정하는 것이다. 실험은 IPSec 정책이 할당 되지 않은 상태에서 대역폭을 측정하기 위해 병렬 스트림 개수를 변경하여 최대 성능을 발휘하는 조건을 찾는 것이다. 그리고 IPSec 정책을 암호화(DES/3DES) 알고리즘과 무결성(MD5/SHA-1) 알고리즘을 조합하여 Server와 Virtual client에 할당하여 각 조합별 성능측정을 수행하였다.

실험2)은 Server에 CBCT (Cone-Beam Computed Tomography) 볼륨 데이터 세트 4개를 저장 한 뒤, 각 Virtual client가 총 4개의 볼륨을 순차적으로 다운로드 하면서 Wireshark으로 패킷을 캡쳐하여 IPSec 적용 전후의 전송 성능 변화를 측정하였다.

2. 실험 결과 및 토의

실험1)은 JPerf 2.0.2를 이용하여 Server와 Virtual client 간 네트워크 성능을 측정하는 실험이다. 최대의 TCP 전송 성능이 발휘되는 조건을 찾기 위하여 병렬 스트림의 숫자를 1에서 10으로 변경하며 실험을 진행하였다. 실험에 사용 된 IPSec의 에 사용 될 암호화와 무결성 알고리즘의 조합은 'DES/MD5 (DM)', 'DES/SHA-1 (DS)', '3DES/MD5(3DM)', '3DES/SHA-1(3DS)'을 사용하였다. 실험의 대조군으로 IPSec을 사용하지 않는 상태

표 1. 테스트 베드 구성 상세
Table 1. The specification of test-bed

Name	Specification
Router	ipTIME N6004R : Ethernet Port (Gigabit Link Setting)
Server	Intel® CoreTM 2 Quad CPU 2,4 GHz, 3.37G RAM / Windows XP Pro. 32 bit SP3 Intel® 82566 DM-2 Gigabit Network Interface Card / Using Jumbo Frame (9014 BYTE)
Bridged host	Intel® Xeon® W3530 2.80 GHz, 16 G RAM / Window 7 Pro. 64 bit SP1 Intel® 82576LM-2 Gigabit Network Interface Card / Using Jumbo Frame (9014 BYTE)
Virtual client	Using VMWare® Workstation 8 on Bridged host Inherited Dual Core CPU, 1 G RAM / Windows XP Pro SP3 Virtual bridged ethernet bridged to host's gigabit ethernet.

'NONE(NO)'에서 우선 실험을 진행하였다. 실험 결과 'NO'의 경우 8개 이상의 병렬 스트림으로 측정하였을 때, 최대치의 95%에 근접하는 성능을 보였다.

'DM. DS' 경우 병렬스트림 개수가 7 이상 되었을 경우. '3DM, 3DS'의 경우 4 이상 되었을 경우 최대치의 95%에 근접하는 서버의 성능을 보였다. 즉, 각 알고리즘 조합에 따라 특정한 병렬 스트림 개수 이상을 생성하였을 경우 처리량(Throughput)의 증가는 확인 할 수 없었다. 이를 수치적으로 표현하기 위하여 병렬스트림 개수와 상관없이 알고리즘 조합 별 처리량의 최대값과 최소값의 비율을 계산하고 각 알고리즘 조합 별 비율을 계산하여 Table 2의 첫 번째 파라미터로 정리하였다. 이는 병렬 스트림의 개수 증가에 따른 네트워크 퍼포먼스의 차이를 측정하여 구성 된 테스트베드와 Server가 제공 할 수 있는 한계점을 찾기 위함이다. Table 2의 첫 번째 파라미터를 기준으로 예측한 대로 'NO'(= 2.889) 일 때 최대 성능을 확인 할 수 있으며, 'DM'(=1.832), 'DS'(=1.787), '3DM'(=1.279), '3DS'(=1.258) 순으로 서버의 병렬 처리 성능의 변화를 보여주었다. 암호화 알고리즘만으로 비교하면, 이론상 DES를 3회 반복하는 3DES가 가장 강한 암호화를 지원하기 때문에 서버의 처리 부하를 야기하여 처리량 감소 원인으로 작용하였음을 예측 할 수 있다. Table 2의 두 번째 파라미터로 처리량을 비교해보면 'DM'(=0.509)과 'DS'(=0.521)가 NO 대비 약 50% 정도 감소하였으며, 3DM(=0.351)과 3DS(=0.350)은 약 65%가 감소 한 것을 확인 할 수 있다. 이는 전반적으로 병렬스트림 개수와 관계없이 비슷한 추세를 보인다.

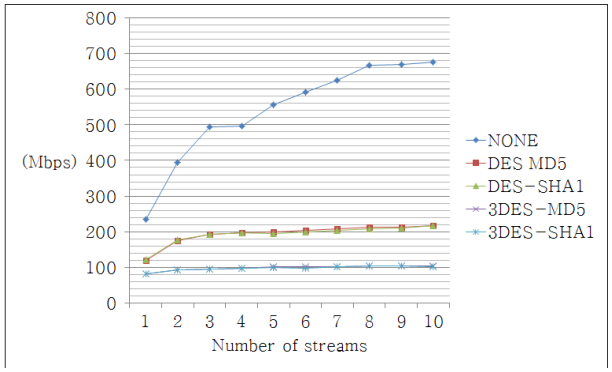

그림 6. 알고리즘 별 서버 전송성능 측정결과
Fig. 6. The result for throughput measurement of server each algorithm.

HMAC (Hash-based Message Authentication Code) 알고리즘으로 사용 된 MD5와 SHA-1를 기준으로 비교하면 SHA-1과 MD5 간 성능에 큰 차이가 없었다. 즉, Table 2의 두 파라미터로 Server의 성능 변화에 중요한 영향을 미치는 것은 암호화 알고리즘이라고 예측 할 수 있다.

실험 2)는 실제 본 연구에서 개발 한 웹 서비스를 이용하여 Table 3에 정리 한 DICOM 볼륨 세트를 전송 할 때 IPSec 알고리즘 조합을 변경하며 전송되는 패킷을 캡쳐하여, Server가 Virtual client에게 전송한 패킷만을 필터링한 결과를 정리한 것이다. 먼저, IPSec이 적용되지 않은 상태에서 측정 된 결과를 살펴보면 총 323,858 개의 패킷이 전달 된 것을 확인 할 수 있다. 그리고 총 489,958,593 바이트의 데이터가 전송되었으며, 평균 패킷 사이즈는 약 1513 바이트가 사용 되었다. 같은 실험 조건

표 2. 암호화와 무결성 알고리즘 간 비교
Table 2. The comparison among encryption and integrity algorithms.

Throughput	None	DES MD5	DES-SHA1	3DES-MD5	3DES-SHA1
MAX/MIN	2.889	1.832	1.787	1.279	1.258
Ratio	1.000	0.509	0.521	0.351	0.350

표 3. 실험 용 DICOM 볼륨 데이터 집합
Table 3. The DICOM volume dataset for experiment

Data set	Gender	Age	File Count	Total Size	Image Size	Format	Modality
#1	Male	26	216	108 MB	512x512	DICOM 3.0	CBCT
#2	Male	27	216	108 MB	512x512	DICOM 3.0	CBCT
#3	Male	30	251	125 MB	512x512	DICOM 3.0	CBCT
#4	Female	25	216	108 MB	512x512	DICOM 3.0	CBCT

표 4. DICOM 볼륨 데이터 전송 패킷 캡쳐 결과
Table 4. The result of packet capture while we had transmitted the four dataset

Statistical Parameter	NONE	DES-MD5	DES-SHA-1	3DES-MD5	3DES-SHA-1
Packets	323,858	784,662	783,804	870,490	878,836
Total Bytes	489,958,593	506,883,544	506,330,832	562,324,848	567,718,988
Avg Packets size	1512.88	645.99	645.99	645.99	645.99

에서 IPSec을 적용한 뒤 알고리즘조합을 변경하면서 패킷을 캡쳐 한 결과를 보면, 총 패킷의 수 기준으로 'DM'와 'DS'가 약 2.42배 증가하였고, '3DM'와 '3DS'가 약 2,.71배 증가하였다. 데이터와 헤더를 포함한 총 전송 된 정보의 량은 'DM'와 'DS'가 약 1.03배 증가하였고, '3DM'과 '3DS'가 약 1.15배 증가하였다. 반면, 평균 패킷 사이즈는 모든 알고리즘 조합에서 IPSec 적용 전 약 1513 바이트에서, 적용 후 약 646 바이트로 감소함을 보였다.

이론상 암호화 알고리즘 적용에 의한 원본 데이터 대비 암호화 된 데이터의 크기는 변하지 않는다. 따라서 본 실험에서는 평균 패킷 사이즈 감소에 의한 전송 패킷 량의 증가와 IPSec 적용에 의한 패킷 오버헤드의 증가로 인하여 Server의 전송 성능이 감소되었음을 확인 할 수 있었다. 성능 평가결과 암호화 및 복호화 과정에서 시스템의 처리 시간의 증가로 인한 성능의 감소도 영향을 미쳤을 것으로 예측 되지만, 이 영향은 평가하는 것은 사용 된 서버의 하드웨어 성능에 의해 결정되므로 절대적인 영향을 평가하기에는 무리가 있다.

Ⅳ. 결 론

PACS는 디지털화 된 의료영상 판독 시스템 도입에 따라서 활성화 되고 있으며, 향후 스마트폰과 같은 개인 단말의 성능과 인터페이스의 발전에 따라서 기존의 병원 내부의 안전한 네트워크를 벗어나 외부에서 접근하여 사용하고자하는 요구가 증가하게 될 것이다. 또한, 중소형 병원을 위주로 PACS를 DICOM 파일을 저장하는 서버를 공유하여 초기화 비용을 감소시키고, 웹을 사용자 인터페이스로 활용하는 Web PACS도 전략적으로 사용이 증가할 것이다[2]. 그러나 PACS를 이용하여 전달되는 DICOM 파일에는 환자의 방사선 영상이나 개인 정보, 그리고 판독결과와 같이 보호 되어야 할 정보가 포함되어 있기 때문에 전송 시 매우 신중하게 다루어져야 할 정보이다. 따라서 암호화 전송 기술을 개발하는 것이 필수이다. 그래서 우리는 IPSec을 직접 제어 할 수 있는 PACS archiving 서버를 개발하였고, 그 방법으로 클라이언트와 서버 간 End-to-End 기반 보안 네트워크 구성 프로그램을 개발하였다. 그 결과 패킷에 대한 암호화를 제공하여 공중망으로 전달되는 패킷이 악의적 사용자에게 유출 되더라도 정보를 보호 할 수 있었다. 그러나 서버와 네트워크 성능 측면에서 오버헤드의 발생으로 인한 서버 전송 성능이 감소하였다.

이미 IPSec으로 가상 사설망을 구축함으로써 보안 네트워크를 구성하는 방법은 이미 많이 알려져 있는 기술이다. 그러나 PACS를 사용하고자 하는 사용자의 위치가 점차 다양해지고 의료 영상 저장소의 위치가 다양해짐에 따라 이와 같은 방식으로 End-to-End간 IPSec을 적용한다면, DICOM 파일이 암호화 되지 않은 채 네트워크로 전달되는 구간을 최소화 할 수 있을 것이다. 또한 서버의 성능 저하 발생에 대안으로 반드시 암호화 전송을 요구하는 클라이언트에 대해 유연하게 IPSec을 이용한 보안 전송이 가능함과 동시에 서버의 성능저하를 최소화 할 수 있을 것이다.

참 고 문 헌

[1] 김천식, 윤은준, 조민호, 홍유식, "의료영상을 위한 복원 가능한 정보 은닉 및 메시지 인증," *전자공학회지 CI편*, 제47권, 제1호, 65-72쪽, 2010년 1월
[2] 임채균, 이기영, 임명재, 정용규, "의료정보보안의 현황과 전망," *전자공학회지*, 제37권, 제6호, 35-48쪽, 2010년 6월
[3] Korea Food and Drug Administration, (2007), Development of Imaging Performance Evaluation Standards of Netxt Generation PACS.
[4] Ministry of Information and Communication, (2003), Development of Security technology for Picture Archiving Communication System.
[5] F. Cao, H.K. Huang, X.Q. Zhou, (2003), "Medical image security in a HIPAA mandated PACS environment." *Computerized Medical Imaging and Graphics* 27, 2-3:185-96.
[6] Jae-Ho Jeong, Kyung-Rae Dong, Dae-Cheol Kweon, Gi-Gyeong Son, Hyun-Soo Kim, Hee-Doo Kang, (2008), "Research on a Validation Standard and the Actual Condition about Security Management in PACS." *Korean Society of Radiological Science* 31, 4:347-353.
[7] AbdelNasir Alshamsi, Takamichi Saito. 2005. "A Technical Comparison of IPSec and SSL." *Advanced Information Networking and Applications, 19th International Conference*, 2:395-98.
[8] Internet Engineering Task Force(IETF). 2004. "Ip security protocol." http://www.ietf.org/html.carters/ipsec-charter.html.
[9] Internet Engineering Task Force(IETF). 2004. "Transport layer security." http://www.ietf.org/html.charters/tls-charter.html.
[10] Microsoft MSDN. "IPSec Policy Creation/ Modification." 검색 2012년 8월 30일.

http://msdn.microsoft.com/en-us/library/cc232433(prot.20).aspx.
[11] Internet Engineering Task Force(IETF). 1997. “Lightweight Directory Access Protocol, RFC2251.”

저 자 소 개

김 정 채(학생회원)
2006년 경희대학교 동서의료공학과 학사
2006년～현재 연세대학교 대학원 생체공학협동과정 박사
<주관심분야 : 생체시스템 모델링, 생체계측 시스템>

유 선 국(정회원)-교신저자
1981년 연세대학교 전기공학과 학사
1985년 연세대학교 전기공학과 석사
1989년 연세대학교 전기공학과 박사
1995년～현재 연세대학교 의과대학 의학공학교실 교수
<주관심분야 : u-Health, 의료영상, 스마트 디바이스, 생체신호처리 및 패턴인식, 감성공학>