의료정보시스템상에서의 네트워크 보안기능 프레임워크와 보안 아키텍쳐 설계방법★

이대성* · 노시춘**

요 약

의료정보 네트워크 구조상에서는 트래픽 소통경로를 따라 악성코드 침투와 보안차단기능이 수행된다. 본 연구는 의료정보시스템 Network 보안 Infrastructure는 어떤 구조와 기준으로 설계되어야하는가에 대한 방법론 개발을 위해 보안기능을 설계한다. 의료정보시스템의 기능 프레임워크는 인프라 구조와 기능에 대한 기본골격과 체계이다. 기능 프레임워크 설계는 네트워크 구조 전반에 대한 골격을 형성하며 보안 방법론의 기본 구조를 형성한다. 기능 프레임워크가 구축됨으로서 인프라구조와 응용기능이 구현되기 때문이다. 보안기능 영역기준에 따라 차별화된 보안기능이 수행되고 보안메커니즘이 가동됨을 본 연구를 통해 제시하고자한다. 향후 클라우드 컴퓨팅 과 u-헬스케어 서비스등 도래하는 새로운 의료정보 환경에 대비하여 본 연구가 의료정보보안에 활용되기를 기대한다.

A Building Method of Security Architecture Framework on the Medical Information Network Environment

Daesung Lee* · SiChoon Noh**

Abstract

On health information network architecture, traffic along the path of traffic and security, blocking malicious code penetration is performed. The medical information system network security infrastructure study, which was whether to be designed based on the structure and methodology is designed to develop the security features. Health informati on system's functionality and capabilities framework for infrastructure is the backbone and structure. The design fea tures a framework for the overall network structure formation of the skeleton and forms the basic structure of the s ecurity methodology. Infrastructure capabilities to build the framework and the application functionality is being impl emented. Differentiated in accordance with security zones to perform security functions and security mechanisms tha t operate through this study is to present. u-Healthcare future advent of cloud computing and a new health informa tion environment, the medical information on the preparation of this study is expected to be utilized for security.

key words : Medical Information Network, Security Architecture, Framework,

접수일(2011년 09월 11일), 수정일(1차: 2011년 09월 19일) 게재확정일(2011년 09월 21일)

★ 본 연구는 지식경제부 지역혁신센터사업인 산업기술보호특화센터 지원으로 수행되었음.

* 경기대학교 산업기술보호특화센터

** 남서울대학교 컴퓨터학과 (교신저자)

1. 서 론

의료정보시스템은 의료활동을 지원하는 정보시스템 혹은 정보시스템의 집합이다. 의료정보시스템은 병원 내의 EHR (electronic health records)을 중심으로 의료와 직접적으로 관련된 작업들을 지원하는 전산시스템이다. 의료정보시스템은 전자 의무기록인 EHR이 필수적이고, 그 외에 임상용어 등에 관한 정리와 참조자료 및 임상모델 등이 필요하다. 방역 알고리즘은 구조 설계를 통해 구성된 종합 구조, 트래픽 소통 경로, 경로 방역망 구조, Tiers별 방역 기능 분담 구조를 기반으로한 바이러스 차단 기능 수행 매커니즘 구성에 관한 것이다. 설계된 방역 기능을 적용했을 때 단계별로 방역 구간이 설정되며 각 구간마다 방역을 수행할 수단인 보안 인프라가 필요하고 아울러 각 보안 인프라가 수행하는 방역 기능이 존재한다. 본 연구는 의료정보시스템 Network 보안Infrastructure 아키텍처는 어떤 구조와 기준으로 설계되어야하는가에 대한 방법론 개발을 위해 보안기능 효율성 측면에서 기능을 설계한다. 기능을 설계는 다원화된 네트워크 구조 환경에서 접속 지점의 다양화로 인해 인트라넷 내부 침투 가능 취약 지점이 광범위하게 확대 분포되어있다. 논문의 기술순서는 의료정보 기술적보안 당면 문제,의료정보시스템 업무 프레임워크 도출, 보안기능구조 프레임워크 설계, 결론의 순서이다.

2. 의료정보 기술적보안 당면 문제

2.1 기능구조 측면 : 네트워크보안 방역기능 설정의 문제

오늘날 의료정보 보안취약점 영역은 방역기술 측면, 인프라구조 측면, 관리나 운용절차 3개 측면으로 구분해볼 수 있다. 심각하게 문제되는 바이러스 침투 형태는 진단, 삭제, 유입 차단으로 해결할 수 없는 네트워크를 통한 확산이다. 현재까지의 중점 방역 방식인 백신기법은 전통적 침투 기법인 진단, 삭제, 유입 차단에는 효과적이지만 네트워크 확산 차단에는 극히 제한적 기능만을 발휘한다. 수많은 서버와 PC에서 바이러스를 삭제해도 네트워크 상에는 여전히 바이러스가 폭증하고 있다. 그렇기 때문에 최근의 백신 기술 발전에도 불구하고 웜 바이러스의 네트워크 확산에 대해서는 속수무책인 것이 현실이다. 따라서 네트워크 확산 기능에 대한 대책을 강구하지 않는 기존의 방역 체계는 방역 체계상 커다란 결함 요인이 된다[2][3].

2.2 Public Domain : 방역 방법론과 적용 기술상의 문제

다원화된 네트워크 구조는 접속 지점의 다양화로 인해 인트라넷 내부 침투 가능 취약 지점이 광범위하게 확대 분포되어 있다. 네트워크 관문, 서버, PC로 설정된 방역 구조는 방역 Zone을 네트워크 관문, 서버, PC로 한정시킴으로서 네트워크 상 유통되는 바이러스에 대한 차단 기능이 없다. 무엇보다도 1차 방어망을 통과했거나 내부 감염으로 서버, PC에 잠복한 바이러스의 인트라넷 내부 확산시 현재와 같은 서버, PC에 집중된 방역 체계로는 근본적 해결이 어렵다. 방역 매커니즘 상 클라이언트 위주 방역은 트로이 목마 등 최근 기승을 부리는 악성코드 감염 여부를 진단하고 치료하는 데는 효과를 나타내지만, 인터넷에 접속한 상태에서 공격용 패킷이 유입되거나 해킹 기술을 동반한 형태로 접속해오는 바이러스 움직임에 대한 감시 기능이 없어 취약한 상태이다[4][7].

2.3 Private Doman : 개인정보보호의 취약성

PHR 등 소비자 중심의 의료서비스 제공을 위한 핵심 서비스로 개인의 건강과 관련된 정보를 관리하여 안전한 의료정보의 공유·활용이 필수적이며 이를 안전하게 관리하기 위한 방법이 요구된다. 이에대한 기술적 대응방안으로 방화벽, IDS, IPS 등의 네트워크 보안시스템을 통한 의료정보시스템상에서 개인정보 유출, DRM과 같은 문서보안기술을 이용한 문서의 암호화와 기술적인 대응방안을 마련하여도 허용된 서비스들(HTTP, 이메일, FTP 등)을 통한 유출이 가능하다, PC보안프로그램 역시 PC보안프로그램의 무력화라든지 외부저장장치 사용허가를 가진 내부자 또는 컴퓨터에 의해 유출이 가능하다[5][6].

3. 의료정보시스템 프레임 구성도

의료정보시스템은 의료활동을 지원하는 정보시스템 혹은 정보시스템의 집합이다. 의료정보시스템은크게 PACS(PicturArchiving CommunicationSystem), EMR(Electronic Medical Record System),OCS(Order Communication System), 기타 네분야로 나뉜다. PACS는 CT나 MRI 등의 사진을 처리, 전달하는 시스템이고 EMR은 경우는 기존에 차트로 썼던 의사의 의무기록 정보를 컴퓨터로 처리, 전달하는 시스템 이다. OCS는 진료행위에서 발생한 약품 처방, 입원 등의 지시를 각 관련 부서에서 사용할 수 있게 처리하는 시스템이다. 의료정보시스템이 효율적으로 기능하기 위해서는 의사결정을 돕는 지원시스템 및 유연한 병원 업무흐름을 가능하게 하는 워크플로우 시스템과 같은 지원기능이 필요하다[8].

(그림1) 의료정보시스템 업무 프레임워크

4. 네트워크보안 기능과 보안 Architecture 설계

4.1 보안기능구조 프레임워크 정의

의료정보시스템의 기능구조 프레임워크는 인프라 구조와 기능에 대한 기본골격과 체계이다. 종합 프레임워크는 구현의 첫번째 단계 과업으로 수행되고 구조 전반에 대한 골격을 형성하며 수행 방법론의 기본 구조를 형성한다. 프레임워크가 필요한 이유는 프레임워크가 구축됨으로서 인프라 하부구조와 기능이 구현되기 때문이다. 프레임워크는 톱-다운(Top-down) 구조의 상층부를 형성하여 하위계층 아키텍처 구조를 가이드한다. 프레임워크를 구축하기 위해서는 먼저 현행 보안처리 방식의 문제점, 그 문제점에서 발췌되는 수정요소 그리고 이와 더불어 새로운 개념의 기능구조 요구사항이 결합되어 새로운 보안 아키텍처에 대한 설계 사상이 수립되어야 한다.

4.2 보안기능구조의 구체적인 설계 사상

<표1> 보안기능 프레임워크

기능 설계 사상
· 기존 구조 수정 요소 - 방역 기능 : 네트워크 경로상 확산 차단 기능 설정 - 적용 기술 : 네트워킹 기술과 바이러스 차단 기술 결합 - 네트워크 구조 : 다단계 경로 차단 도입 - 방역 Zone : 네트워크 전구간 확대 · 효율성 구조 요소 - 인프라 구조 관리 방식 : 통합 관리 구조 - 인프라 구조 구성 형태 : 고가용성 구조 - 시스템 기능 형식 : 자동화, 실시간 구조

■ 보안기능설계 :

설계사상의 설정, 침입차단 프레임워크 설계, 차단 기능 매커니즘 구성, 그리고 차단 네트워크 구조도 설계 등 4개 영영으로 구성된다.

■ 설계 사상 설정 :

인프라 구조가 지향하는 목표와 설계 범위를 정의하는 단계이다. 설계 사상 설정이 필요한 이유는 설계 사상을 통해 인프라 구조가 궁극적으로 달성해야할 범위를 명확히 하게 되고 설계의 기초 토대가 구체적으로 구축될 수 있기 때문이다.

■ 침입차단 프레임워크 설계 :

인프라 구조 설계 제반 체계를 구축하는 과정이다. 프레임워크에서는 개선 방법론, 개선의 절차와 단계, 개선 대상이 설정됨으로서 설계 작업의 가장 큰 틀이 마련된다. 프레임워크 설계가 필요한 이유는 프레임워

크 설계를 통해서 설계 사상이 추구하는 목표에 대한 달성 방법 근간이 형성될 수 있기 때문이다.

■ 보안도메인 설정 :

형상 결정요소를 기반으로 보안도메인을 설정 하여야한다. 검토될 수 있는 요소는 1. 외부 네트워크 -외부 라우터영역, 2. 외부 라우터 - 외부 스위치영역, 3. 외부 스위치 - 침입차단영역, 4. 침입차단 - 내부 게이트웨이영역, 5. 내부 게이트웨이 - 서버팜영역, 6. 내부 게이트웨이 - 클라이언트영역으로 6개 범위로 설정될 수 있다. 이때의 도메인은 외부 라우터 구간, 외부 스위치 구간, 침입차단 구간, 내부 게이트웨이 구간, 서버 구간, 클라이언트 구간으로 명명한다.

4.3 보안기능 매커니즘 구조 설계

■ 보안차단 기능 기본 구도

<표 2> 차단기능 기본구도 구성

방역 Zone	차단 기준 정보	차단 단계	차단 기능
· 트래픽 경로 · 정보 자원 · 하드웨어 리소스	· MAC 주소 · IP 주소 · 프로토콜 종류 · TCP,UDP 서비스 종류 · 컨텐츠 기반 · 트래픽볼륨	· 외부 관문 · 내부 관문 · 내부 게이트웨이 · 내부 네트워크	· 진단 · 삭제 · 거점 차단 · 치료 · 경로 차단

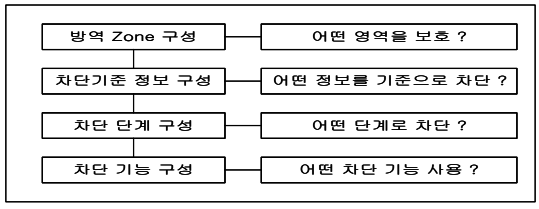
차단 기능 기본 구도는 방역 Zone별 차단, 차단 기준 정보별 차단, 차단 단계별 차단, 차단 기능별 차단으로 구성된다. 방역 Zone별 차단이란 방역을 해야할 영역별로 어떤 기준으로 범위를 설정하는가에 관한 것이다. 일반 구조는 하드웨어 리소스별 기준으로 방역 Zone을 구성했다. 일반 구조의 하드웨어 리소스 기준은 각종 서버와 클라이언트를 방역 대상으로 삼은 것이다. 개선구조에서는 방역 Zone을 트래픽 경로별로, 정보 자원별로, 하드웨어 리소스별로 세 개의 카테고리로 구분하여 설정했다. 먼저 트래픽 경로는 설계 프레임워크에서 제시한 바와 같이 트래픽 경로를 기준으로 외부 라우터 - 외부 스위치, 외부 라우터 - 침입차단시스템, 침입차단시스템 - DMZ, 침입차단시스템 - 내부 네트워크 등 4개 영역으로 편성한다. 그중 내부 네트워크는 게이트웨이 구간, 서버 구간, 클라이언트 구간으로 더 세부적 설정이 된다.

■ 차단 기준 정보 설정

차단 기준 정보를 설정하기 위해서는 Layer별 침투 형태를 검토한다. 고전적인 IP 주소 또는 포트 스캔에서 이제는 자신의 MAC이나 IP주소를 바꾸어서 침입을 시도하는 도구들이 사용되고 있다. 2계층 차단 기준 정보는 MAC 주소, 3계층 차단 기준 정보는 IP 주소, 4계층의 경우 하위 계층 기준 정보를 포함 TCP, UDP, ICMP 프로토콜 종류, TCP, UDP 포트 번호로 설정된다. 5계층에서부터 7계층까지의 기준 정보는 컨텐츠 기반 정보를 기본으로 한다. 컨텐츠 기반 정보는 제목, URL을 비롯 컨테츠 내용 중 키워드(Key Word) 기준으로 설정할 수 있고 이 경우는 보안 솔루션별로 선택 기능을 부여한다.

■ 차단 기능별 구성

차단 기능별 구성이란 차단 기능이 어떤 영역, 어떤 종류로 구성되는가에 대한 기능이다. 차단 기능은 현재 사용되어지고 있는 영역별로 패킷 스위칭, 패킷 필터링, 차단(Protection) 등으로 구성되는데 실제 현장에서는 이 같은 차단 기능이 순수한 차단 기능으로 구성되기도 하고 네트워킹 기능과 결합하거나 연동하여 구현되기도 한다. 따라서 오늘날의 차단 기술을 순수 보안 기능과 순수 네트워킹 기능으로 분리하기가 어렵고 상호 연동 작용을 통해서 이루어지는 것이 정석이 되었다.

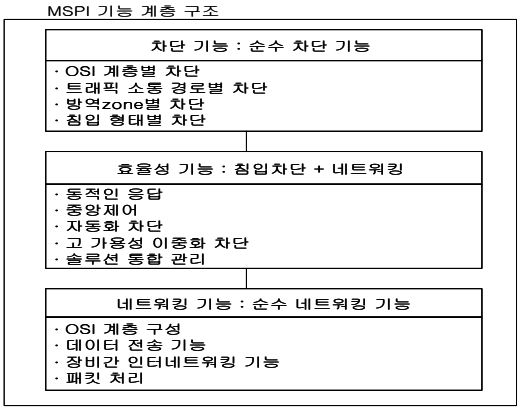


(그림2) 의료정보시스템 기능 프레임워크

■ 기능계층간 Interface

동작 매커니즘 구조는 (그림3)과 같이 네트워킹 기능, 효율성 기능, 침입차단 기능 3단계로 계층화된다.

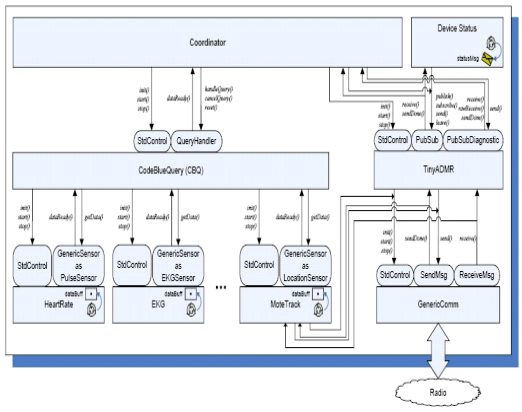
네트워킹 계층은 보안 인프라가 구성, 설정되는 기본 틀인 네트워킹 계층의 기능을 말한다. 네트워킹 기능은 OSI 7 layer별로 차별화된 네트워킹 기능 구조를 형성하고 이 구조상에서 라우팅, 스위칭, 브로드캐스팅 등 인터네트워킹 기능, 데이터 전송 기능 그리고 패킷 처리 기능을 수행한다. 네트워킹 기능의 영역 내에 효율성 기능과 침입차단 기능이 존재한다. 효율성 기능은 네트워킹 기능을 토대로 하지만 침입차단 기능 구현시 적용되어야 할 필수적인 지원 기능 또는 연관 기능이다. 효율성 기능은 성격상 3개 세부 영역으로 분류되는데 고가용성 기능, 통합 관리 기능 및 자동화 처리와 실시간 처리 기능이다. 침입차단 기능은 인프라 구조의 목적에 해당되는 바이러스와 각종 악성코드 침입차단 기능이다. 침입차단 기능은 OSI 계층별 차단, 트래픽 소통 경로별 차단, 방역 Zone별 차단으로 분류될 수 있다.이 같은 제반 단계의 결과는 차단 기능 구성으로 나타난다.



(그림3) 의료정보시스템 기능 프레임워크

■ 정보 Query

경로별 차단은 외부 라우터에서부터 최종 클라이언트까지의 트래픽 경로별로 수행되는 차단이다. 각 노드들은 특정센서, 데이터속도, 데이터 전송에 필요한 필터 상태등을 나타내는 Query(CBQ) layer를 이용하여 통신경로 설정한다. Dircted Difusion과 tiny DB를 이용하여 최종 사용자 디바이스(PDA나 Laptop)등에서 요구할 수 있고, 노드에게 쿼리에서 요구하는 데이터를 publish시키도록 요구할 수 있다. 그림에서 처럼 Software가 작동을 하고 내부적으로 쿼리는 두가지 컴포넌트로 이루어 질 수 있다. 첫째 Coordinator는 메시지를 받아 다양한 내부 커맨드를 이용하여 조정하고 컴포넌트로 데이터를 내보낸다. 컴포넌트는 쿼리 실행에 대한 테이블을 유지하고 쿼리실행 이벤트에 대하여 정리 한다.



(그림4) 의료정보 query interface

5. 기능구조의 방역성과 측정기준

<표3> 의료정보보안측정 프레임워크

차단 단계	측정기능 요구사항	성능 분석 대상
센싱	· 센싱구간외부 침투 발생 실적	· 침입 발생 실적 · 차단 실적
스위칭	· 외부 침투 발생 실적과 차단 실적	· 침입 발생 실적 · 차단 실적
패킷필터링	· 패킷 필터링 처리 실적과 시스템 Performance	· 패킷 필터링 실적
내부 게이트웨이	· 내부 게이트웨이 차단과 시스템 Performance	· 유해 트래픽 차단 실적 · 시스템 Performance
내부서버군	· 내부 서버군 차단과 시스템 Performance	· 바이러스차단실적 · 시스템 Performance
내부 네트워크 클라이언트	· 내부 클라이언트군 차단 실적	· 바이러스 차단 실적

기능구조도에 의한 방역성과는 웜 바이러스 방지와 웜 바이러스 차단 등 두 가지 측면이다. Layer 7 컨텐츠 필터링을 통하여 Query 대상 및 DDoS 공격에 대한 사전 차단과 신규 인터넷 웜 바이러스를 차단한다. 보안도메인은 정교한 부하 분산과 함께 유해 트래픽 차단과 데이터 필터링 기능을 통해 네트워크 환경을 최적화하고 있다. 스위칭기능은 Deep Inspection, 전체적인 트래픽 모니터링을 실시함으로서 종래의 로드 밸런싱 위주의 L4 기능에서 보안 기능을 구현하는 차세대의 스위칭 기능으로 분석된다.

5. 결 론

의료정보는 의료시스템의 기반구조로서 환자의 생명과 건강관리에 필요한 정보를 직접 관리하는 속성을 가진다. 의료정보보안은 의료시스템의 안전을 확보하고 환자 개인의 권리를 지키는 기 반을 확보해야 한다. 이런 목적으로 의료정보보안의 기능을 체계화하여 설계 하므로서 날로 증가하는 정보보안 위협에 대처해야 한다. 본 연구는 의료정보시스템상에서 보안을 강구하기 위한 근본 대응방법을 보안 기능설계의 틀에서 설계했다. 의료정보보안은 일회성 계획, 단기투자로 해결되지 않는다. 향후 클라우드 컴퓨팅 환경과u-헬스케어 서비스 환경 도래에 대비하여 본 연구가 의료정보보안 구축에 활용되기를 기대한다.

참고문헌

[1] Sichoon Noh, Dong Chun Lee, and Kuimam J.Kim, "Improved Structure Management of Gateway Firewall Systems for Effective Networks Security", Springer, 2003.

[2] Sichoon,Noh,Dong Chun Lee,"Assurance Method of High Availability in Information Security Infrastructure System", SCIE LNCS 3794,2005.12

[3] Sichoon,Noh,"Building of an Integrated Multilevel Virus Protection Infrastructure", IEEE Computer Society,2005.12.

[4] Sichoon,Noh,"A Securing Method of Multispectral Protection Infrastructure for Malicious Traffic in Intrne System", DCS, 2006.02

[5] CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care, David Malan, Thaddeus Fulford-Jones, Matt Welsh, and Steve Moulton. International Workshop on Wearable and Implantable Body Sensor Networks, April 2004.

[6] Biomedical telemedicine - CSCI E-170 January 11, 2005

[7] Healthwear:Medical Technology Becomes Wearable - 2004 IEEE

[8] Biomedical telemedicine - CSCI E-170 January 11, 2005

[9] Healthwear:Medical Technology Becomes Wearable - 2004 IEEE

[10] Vital Positioning System Product Page, Medical Intelligence website, Retrieved December28,2004. URL: http://www.medicalintelligence.ca/en/produits.html

[저 자 소 개]

이 대 성 (Daesung Lee)

1999년 2월 인하대학교
전자계산공학과 학사
2001년 2월 인하대학교
전자계산공학과 석사
2008년 2월 인하대학교
정보공학과 박사

email : xdilemma@naver.com

노 시 춘 (SiChoon Noh)

1987년2월 : 고려대학교
경영정보학(석사)
2005년2월 : 경기대학교
정보보호기술(박사)
2002년11월 : KT 시스템보안부장
2004년 12월 : KT 충청전산국장
2005년3월 ~현 재 : 남서울대학교
컴퓨터학과 교수
2011년2월 ~현 재 : 남서울대학교
IT융합연구소 연구위원

email : nsc321@nsu.ac.kr