특집

의료정보보안의 현황과 전망

임채균 · 이기영 · 임명재 · 정용규 (을지대학교)

I. 서 론

최근 IT융합이 사회적인 트렌드가 되면서 타 산업과 IT 기술의 융합화, 내재화가 가속되고 있다. 전반적인 산업분야에서의 IT활용이 증대됨에 따라 새로운 기회요인으로 산업구조의 고도화, 새로운 서비스 및 신제품 개발, 신시장 창출이 부각되고 있다. 이러한 IT산업의 패러다임의 변화에 발맞춰 조선, 자동차, 의료, 섬유, 기계/항공, 건설, 국방, 에너지, 로봇, 조명산업은 10대 IT 융합산업으로써 전략적인 육성의 필요성이 높아졌다.

특히 IT+의료 분야는 지속적인 경제 발전과 고령화 사회 진입으로부터 발생되는 문제를 해결하고, 삶의 질 향상에 대한 요구에 따라 IT 기술을 활용한 새로운 의료 기기 및 u-Health 서비스의 새로운 시장 형성을 기대할 수 있다. u-Health는 원격 환자 모니터링과 같이 유무선 네트워킹 기술을 활용하여 언제, 어디서나 이용 가능한 건강관리 및 의료서비스로 병원에서 단발성 치료에 국한되었던 기존 서비스가 앞으로 가정 등 실생활 전 영역에서 제공될 수 있다. 하지만 이러한 IT기술의 도입으로 대부분의 의료정보시스템이 전산화되면서 의료기관간에도 의료정보의 교환 및 전송이 자주 발생함에 따라서, 의료정보 유출 및 보안에 대한 위험성이 커지고 있는 형편이다.

의료정보는 환자 진료정보와 관련된 전반적인 정보 모두를 의미하며, 기본적으로 환자 본인 이외에는 알리지 않는 것이 원칙이다. 현재 의료 체계상 각 의료기관이 전체 환자에 대한 의료정보의 보호 및 보안을 책임지고 있다. 그러나 최근에는 일반인도 본인에 대한 의료정보를 직접 관리하는 등 관심이 높아지는 경향을 보이고 있으므로, 기관뿐만 아니라 개인적인 영역에서도 정보보안에 대한 대책이 필요하다.

본 고에서는 IT와 의료 융합분야의 관점에서 u-Health 관련 국내외 시장 동향을 알아보며, 이러한 배경에서 의료정보보안을 유지하기 위한 고려사항과 정보보안기술 및 의료정보보호 기술 표준의 현황이 어떠한지, 또 향후 발전 방향에 관하여 살펴보고자 한다.

II. u-Health 관련 시장현황

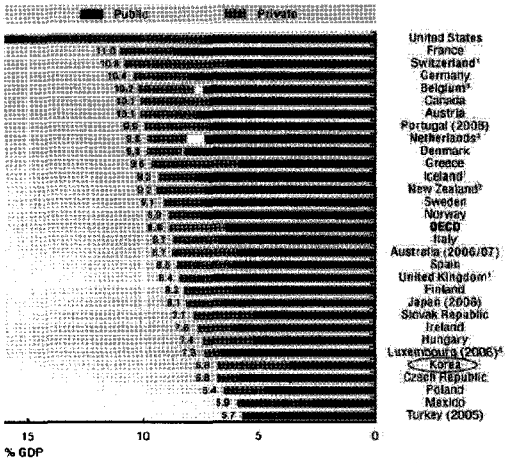
의료 산업은 인간 삶의 질을 좌우하는 기반산업으로 최근 의료시장 개방에 따라 국내외 경쟁 환경이 조성되기 시작하고 있다. 국내에서도 고령화 사회 진입과 빠른 사회적 변화로 인한 스트레스 증가, 식생활 변화로 인한 새로운 질병의 확대로 국내에서의 수요도 증가하고 있는 추세를 보인다.

그러나 국내 의료 산업은 선진국과 비교해 여전히 취약해 아직까지 상당 부분을 수입에 의존하고, 기술력도 선진국 대비 약 56% 수준으로 약 3~4년의 기술격차를 두고 있다. 이뿐만 아니라 국내 의료 관련기업들은 대부분 영세하고 투자 여력이 낮으며, 기술력 및 전문인력도 글로벌 기업과 비교할 때 매우 부족한 현실이다. 따라서 타 산업에 비해 시장규모가 작아 상대적으로 관심이 낮고, 산업에 대한 분석 및 정보 유통이 아직은 원활하지 못한 상태라고 할 수 있다.

또한 우리나라의 국민 의료비 지출은 <그림 1>과 같이 GDP 대비 약 6.8% 수준('07년 기준)으로 OECD 평균인 8.9%에 비해 낮은 것으로 나타났지만, 1980년의 4.1%, 2000년 4.9% 이후 매년 증가추세를 보이고 있다.

한편, 세계적인 경기침체에도 불구하고 세계 의료기기 시장은 2010년 약 2,350억 달러 규모를 형성할 전망이다. 그리고 국내 의료기기 시장 규모는 2007년에 이미 3조 원을 돌파해 세계 10위권을 형성하고 있으나, 수입의존도가 61.4% 수준을 차지하고 있다.

미래 성장동력으로 대두되는 u-Health 산업은 새로운 의료 패러다임이며, 헬스케어의 시간/공간적 제약을 완화시켰다. 해외에서는 선도 SW/HW/통신사업자들이 u-Health 시장의 주



자료 : Health at a Glance 2009, OECD, 2009.

〈그림 1〉 주요국 GDP 대비 의료비 비중

도권 확보를 위해 사업제휴 및 신규서비스 개발 등 지속적으로 사업영역을 확대 추진 중일 뿐만 아니라, 국내에서도 다양한 영역의 사업자들이 미래 성장사업으로 u-Health 사업을 추진하고 있다. 우리투자증권에서는 국내 잠재수요를 기준으로 u-Health 시장이 2012년 약 1.5~2조 원, 환자 모니터링서비스로 인한 건강보험지출과 환자 부담금 절감효과는 연간 1.4조 원이라고 전망하고 있다('10. 2. 25.).

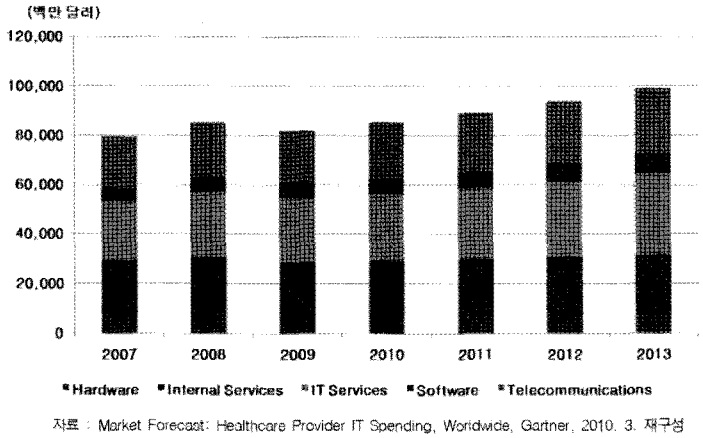
u-Health 산업은 기본적으로 병원 정보화에서부터 시작되기 때문에 기존 IT산업의 SI 및 솔루션 제공업체의 진출이 가장 우선적으로 가시화되고 있다. HP, IBM, MS, Oracle 등 글로벌 IT기업들의 의료시장 진출이 활발하게 진행되고 있으며, <표 1>은 '08년을 기준으로 이러한 주요 IT업체의 헬스케어 매출 현황을 나타낸다. HP가 약 54억 달러의 매출로 1순위를 달성하였으며, 그 뒤를 이어서 IBM이 약 46억 달러, MS가 약 28억 달러, Fujitsu가 약 20억 달러의 매출을 보이는 등 주요 IT업체들의 헬스케어 매출이 매년 급성장하고 있다는 사실을 알 수 있다.

〈표 1〉 주요 IT업체의 헬스케어 매출 현황 ('08년 기준)

(단위: 백만 달러)

순위	업체명	헬스케어 공급측	헬스케어 수요측	합계
1	HP	4,254.4	1,145.4	5,399.7
2	IBM	3,710.5	888.5	4,599.0
3	Microsoft	2,348.3	419.0	2,767.2
4	Fujitsu	1,765.7	216.6	1,982.3
5	Cisco	1,677.9	251.9	1,929.7
6	Dell	1,509.2	336.6	1,845.8
7	Ricoh	1,428.9	219.3	1,648.3
8	Oracle	1,272.3	122.9	1,395.2
9	Alcatel-Lucent	1,246.0	94.0	1,340.0
10	CSC	1,036.7	251.1	1,287.7

자료 : Worldwide Life Sciences, Healthcare Payer, and Healthcare Provider Revenues for the Top 25 IT Vendors, 2008, IDC, 2010. 3. 재구성



자료 : Market Forecast: Healthcare Provider IT Spending, Worldwide, Gartner, 2010. 3. 재구성

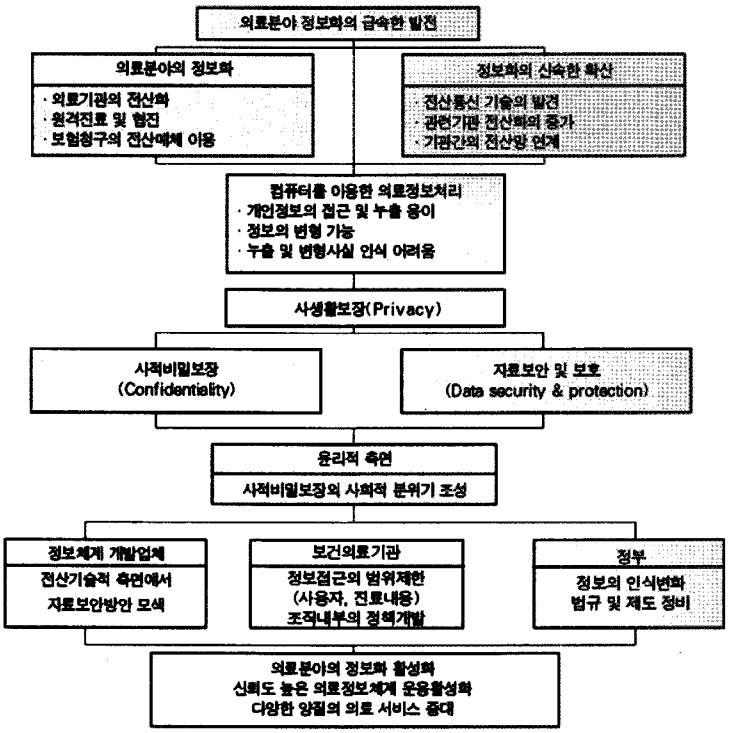
〈그림 2〉 헬스케어 공급자용 IT 시장 추이

<그림 2>는 헬스케어 공급자용 IT 시장에서 HW, SW, IT 서비스, 통신 부분에 대한 현황을 나타내고 있다. 전반적으로 지속적인 성장 추세를 보이며 2010년에는 약 850억 달러 규모를 형성하고, 2008년부터 2013년까지 약 3.1%의 CAGR을 기록할 전망이다.

III. 의료정보보안 및 보호

u-Health 시장의 확산과 더불어 환자 의료정보의 전산화가 진행됨에 따라서 <그림 3>과 같이 사생활 보장과 자료 보호의 측면에서 새로운 위험성이 등장하게 되었다.

전자 문서 등의 형태로 전산화된 의료정보는 환자의 의무기록에 관련된 정보로써, 환자의 건강력, 진단명, 질병 상태, 치료 경과, 그 외의 개인에 관한 신상정보 등을 포함하는 민감한 정보이다. 환자에게 있어서 이러한 의료정보의 노출은 정신적, 사회적, 경제적인 피해를 초래할 가능성이 있다. 따라서 사적 비밀보장의 측면에서도 환자 본인의 허가 없이 정보가 유출되지 않도록 자료를 보호하고 보안을 유지할 필요성이 있다. 하지만 "보호되어야 하는" 의료정보의 수준이 어



〈그림 3〉 환자비밀보호의 배경과 필요성

디까지인지 상대적인 개념이라는 문제가 있다. 따라서 의료정보를 보호하기 위한 명확한 지침이 다방면에 걸쳐 준비되어야 한다. 현재 법 제도적으로도 지침이 존재하고 있는데, 헌법 제17조에는 사생활을 보호할 권리가 있으며 형법 제317조 제1항에도 규정하고 있다. 그 외에도 수많은 의료법 · 의사 윤리지침서 등에도 기록되어 있다.

또한 의료정보의 기밀유지에는 몇 가지 난점들이 존재한다. 첫 번째는 대중성으로 인한 부분이며, 일반적으로 유명인사의 건강 상태나 치료내용들이 발표되는 것이다. 두 번째 난점은 보험회사 등의 제3자 지불집단이다. 일반인에게 부담되는 고가의 진료비를 지원하기 위하여 의료보험 체제가 있으나, 이를 증빙하기 위하여 보험과 관련된 별도의 의무 기록이 필요하게 된다. 행정 및 사무직원이나 보험업자 등을 통하여 의료정보 유출의 위험성이 증가할 뿐만 아니라, 보험 회사에 환자 정보를 제공하는 것 자체도 사적 비밀 보장에 위배되는 것이 아니냐는 문제 제기도 존재한다. 세 번째로는 의료 서비스의 제공 형태가 변화하게 된 것으로, 의료 분야가 세분화되고 많은 인력이 서비스 제공에 참여하게 되면서 발생한 문제이다. 합법적으로 다수의 보조 인력들이 의료 정보에 접근이 가능한데, 전문적인 의료진과는 달리 보조 인력에게는 명백한 윤리 강령이 없다는 점이 특히 문제이다.

만약 의료정보가 유출되어 불법적인 축적 및 이용되는 경우에는 환자의 정보 유통을 조정할 권리에 대한 침해이면서 사생활 침해에 해당된다. 또 임의로 정보에 대한 수정이 가해질 경우에는 부정확한 정보가 생성되는 추가적인 문제가

발생될 수 있다. 미국에서는 이러한 의료정보 유출의 피해를 자연적인 비밀 (Natural secret), 약속된 비밀 (Promised secret), 직업적인 비밀 (Professional secret)의 3가지로 구분하고 있다. 자연적인 비밀은 환자에 대한 의료정보 노출 시 자연적으로 피해가 발생되는 정보에 대한 비밀 보호를 의미하며, 약속된 비밀은 자연적인 비밀과 유사하지만 더 엄격한 비밀이 요구되기 때문에 약속이 필요하다. 직업적인 비밀의 경우에는 환자는 물론 직업인 자신과 사회 전체에 피해를 줄 수 있는 중요한 정보에 대한 비밀 보호로써, 대부분 법적으로 비밀 보호를 규정하고 있다.

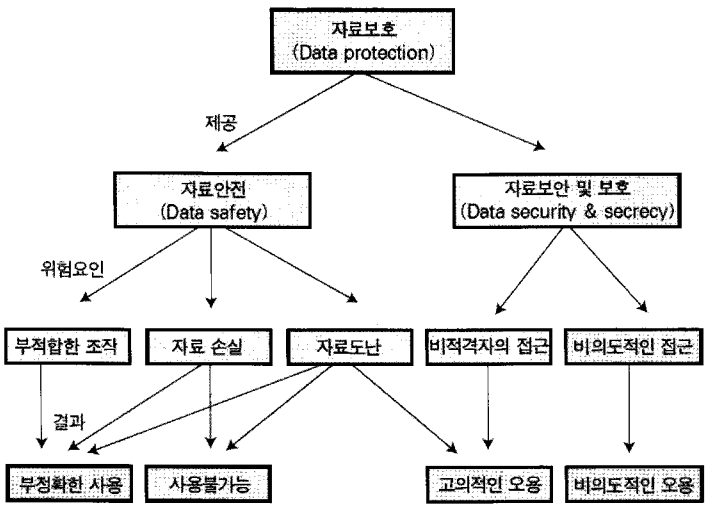
의료정보시스템의 전산화에 따라서 <그림 4>와 같이 기계나 프로그램이 포함하는 자료 보호의 위험성 측면도 고려해야 한다. 의료정보는 환자에 개인적인 정보부터 진료에 필요한 주요 정보 등을 포함하는 민감한 정보이므로 자료의 비밀성 (Confidentiality)이 중요하다. 하지만 전산화된 시스템에서 하드웨어적인 고장, 자료 갱신 시의 오류, 올바르지 않은 프로그램이나 기능의 사용, 통신 자원들의 잘못된 사용 등의 위험성으로 인한 자료의 손상이 발생하는지 주의할 필요가 있다.

Ⅳ. 정보보안 기술의 현황

본 장에서는 IT산업 분야에서 정보보안을 위하여 기존에 사용하던 기술에 대하여 살펴보기로 한다. 시스템의 침입자 혹은 원하지 않는 타인의 접근에 대해 기밀성을 보장하기 위한 기술은 크게 파일시스템을 암호화하는 기법과 전송할 데이터를 암호화하는 기법이 있다.

1. 암호화 파일시스템

암호화 파일시스템은 데이터의 관점에서 암호화하여 저장하는 기법으로, 개인이나 조직에서 기밀성을 보장해야하는 중요한 정보에 대한 보안 유지를 목적으로 개발되었다. 데이터 자체



〈그림 4〉 자료의 보호 및 오용의 위험

를 암호화하여 디스크에 저장하므로, 만약 디스크 자체의 도난이 발생하더라도 중요한 데이터의 유출을 방지할 수 있어 시스템의 물리적 보안보다 더 안전하다고 할 수 있다. 대표적으로는 Cryptographic File System (CFS), Transparent Cryptographic File System (TCFS), Cryptfs 그리고 Steganographic File System (StegFS) 등이 있다.

가. Cryptographic File System (CFS)

CFS는 1993년 AT&T Bell 연구소의 Matt Blaze가 NFS (Network File System) 내에 암호화 기능을 추가한 것이다. 암호화된 파일에 대해 표준 유닉스 파일시스템 인터페이스를 적용함으로써 시스템 수준에서의 보안 저장장치 (Secure storage)를 제공한다.

사용자는 보호하고자 하는 디렉토리를 암호화 키와 연관시켜 각 디렉토리마다 키를 명시한다. 이러한 디렉토리 내의 파일들은 더 이상의 사용자 개입 없이 명시된 키를 이용하여 암호화 및 복호화 된다. 평문 형태의 데이터는 절대로 디스크 상에 저장되지 않으며, 원격 파일 서버로의 전달도 이루어지지 않는다. 또한 CFS는 NFS와 같은 원격 파일시스템을 포함하여 사용 가능한 파일시스템을 수정하지 않고 이용할 수 있다. CFS의 기본개념은 시스템 내에서 신뢰되는 부분 (Trusted components)은 신뢰되지 않은 부분 (Untrusted components)으로 데이터를 전송하기 전에 무조건 암호화해야 한다는 것이다.

나. Transparent Cryptographic File System (TCFS)

이탈리아 Salero 대학에서 개발된 TCFS는 암호화 서비스와 파일시스템 사이에 더 깊은 통합을 제공함으로써 Matt Blaze의 CFS를 개선한 것이다. TCFS는 NFS를 기반으로 구현되었으며, 실제 많은 부분이 리눅스에서 발견되는 표준 NFS 구현으로부터 파생되었다. TCFS는 사용자가 그룹 내의 사용자들과 파일들을 안전하게 공유할 수 있도록 해 주는 좋은 특성이 있지만, 커널 패치의 필요 및 최소한의 키 관리 제공 등의 문제점이 있다.

기술적인 측면에서 보면, CFS는 사용자 영역에서 동작하는 반면, TCFS는 커널 영역에서 동작하므로 개선된 성능과 보안성을 제공한다.

다. Cryptfs

Cryptfs는 1998년 콜롬비아 대학의 Erez Zadok에 의해 Stackable Vnode Layer loadable kernel module로써 설계 및 구현된 파일시스템이다.

사용자에게 클라이언트 파일시스템을 '캡슐화' 함으로써 투명한 암호화 기능을 수행하며 커널 수준에서 동작한다. 커널 수준에서 동작한다는 것은 암호화 기능이 파일시스템의 일부가 되어 파일을 액세스 하는 모든 응용에 대해 일관된 암호화를 자동적으로 제공하고, 문맥 교환의 횟수를 줄일 수 있으며, 사용자 수준이나 NFS에 기반한 파일시스템 – CFS, TCFS 등 – 보다 효과적인 보안성 및 성능을 제공할 수 있음을 의미한다.

그리고, Cryptfs의 키는 사용자 ID 뿐만 아니라 프로세스 세션 ID에 기반한다는 점과, 커널 메모리의 액세스는 사용자 메모리보다 더 어렵다는 사실로써 좀 더 강한 보안성을 제공한다.

라. Steganographic File System (StegFS)

StegFS 역시 데이터를 암호화하여 사용자 데이터를 보호한다는 목적을 가지고 있고, 여기에 steganography(정보 은닉) 특성까지 추가한 파일시스템이다.

*Steganography*란 통신의 존재를 감추는 방법으로 통신하는 기술을 말하며, 주로 메시지를 잡음에 섞어 전송할 때 많이 사용된다.

암호화 방식은 공격자가 암호화된 메시지를 찾아내어 원래 내용을 볼 순 없지만, 수정 및 삭제가 가능하다. 하지만, steganography의 목적은 손상되지 않은 메시지 내에 보호하려는 메시지를 감추는 것이므로, 공격자는 감추어진 메시지를 찾아낼 수가 없다.

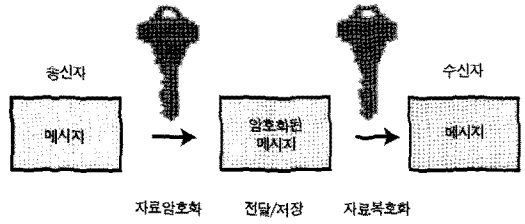
StegFS는 파일 블록들을 임의의 위치에 암호화된 블록들을 기록함으로써 임의의 데이터들 사이에 숨겨질 수 있고, 파일시스템에 기록되는 블록들이 많아질수록 원래 데이터 블록에 대한 overwrite 발생빈도가 높아진다. 따라서, 각 블록을 복구하기 위해 여러 개의 복사본이 필요하고, overwrite 되었을 경우 그렇지 않는 데이터 블록과 구분할 수 있는 방법들이 필요하게 된다.

StegFS semantic은 모든 표준 유닉스 파일시스템 semantic과 매우 유사하므로 하위 디렉토리, inodes, symbolic & hard links 등을 가지고, 시스템에서의 숨겨진 파일 손실 등과 같은 에러 상태가 일반 파일시스템에서의 매우 유사한 상황에서 조치되는 오류 코드를 통해 전달되어, 표준 소프트웨어는 자동적으로 적절한 조치가 가능하다.

2. 암호화 전송기법

암호화 전송기법은 데이터를 실제로 다른 장소에 위치한 개인이나 기관에 전송할 경우, 데이터를 암호화하여 메시지를 전송하는 기법이다. 기본적인 원리는 <그림 5>와 같이 송신자가 암호화 키를 이용하여 전달할 메시지를 암호화화여 전송하고, 이를 받은 수신자 측에서 복호화 키를 가지고 암호화된 메시지를 해독한다.

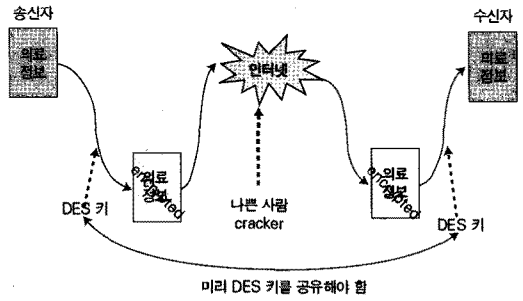
이러한 암호화 전송기법은 크게 대칭키 기반 기법과 비대칭키 (공개키) 기반 기법, 전자서명을 통한 인증기법이 있으며, 각 기법을 혼용하여 보안 수준을 향상시킨 기법들이 존재한다. 여기에서는 대표적으로 DES, RSA, 전자서명 등의 기법으로 의료정보를 암호화하여 전송하는 과정에 대하여 기술한다.



<그림 5> 자료 암호화 원리

가. Data Encryption Standard (DES)

1972년 미국 NBS (National Bureau of Standards, 현재 NIST)는 암호 기술의 필요성을 절감하고 미국 정부 규모의 표준적인 암호 알고리즘을 개발하기로 했다. 이에 1974년, IBM에서 루시퍼 암호 알고리즘을 제안했고, 이를 수정하여 1975년에 DES를 발표했다. DES는 블록 암호의 일종으로, 미국 NBS에서 1977년 국



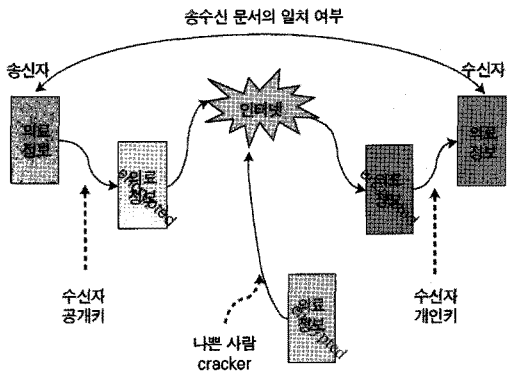
〈그림 6〉 DES 암호화

가 표준으로 정한 암호이다. DES는 대칭키 암호이며, 64비트 블록과 56비트의 키를 사용한다. 이 기법은 1997년까지 표준으로 사용되었으나, 현재 컴퓨터 환경에 비해 56비트의 키가 너무 짧기 때문에 무차별 대입으로도 쉽게 해독 가능한 취약점이 알려져 있다.

<그림 6>은 DES 암호화 기법을 적용하여 의료정보를 전송하는 과정을 도식화한 것이다. 송신자는 DES 키를 이용하여 의료정보를 암호화하여 전송하며, 수신자는 동일한 DES 키로 암호화된 의료정보를 복호화하게 된다. 이러한 대칭키 기반 알고리즘은 사전에 DES 키를 공유해야 한다. 이 때 외부의 침입자에게 DES 키가 유출된다면 침입자는 모든 정보를 해독하거나, 임의의 정보를 전송 가능하게 되는 문제점이 있다.

나. Rivest-Shamir-Adleman (RSA)

RSA는 공개키 기반 알고리즘의 하나이며, 1977년 Ron Rivest, Adi Shamir, Leonard Adleman의 연구에 의해 체계화되었으며, RSA라는 이름은 이들 3명의 이름 첫 글자를 딴 것이다. RSA는 큰 숫자의 소인수분해가 어렵다는 것에 안정성의 기반을 두고 있으며, 2개의 키를 사용한다. 공개키는 모두에게 알려져있으며 메시지를 암호화하는데 쓰이고, 암호화된 메시지는 개



〈그림 7〉 RSA 암호화

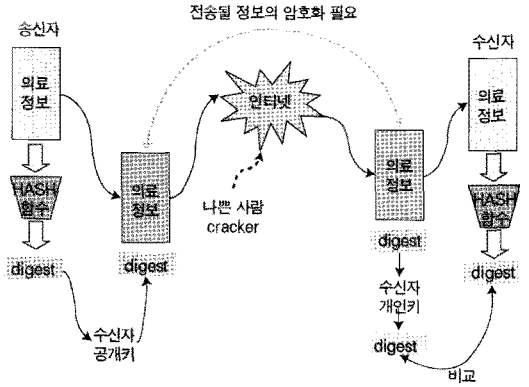
인키를 가진 자만이 복호화하여 볼 수 있다.

<그림 7>은 RSA 암호화를 적용한 전송과정을 나타낸다. 여기에서 외부의 침입자는 알려진 공개키를 통하여 임의의 정보를 암호화화여 전송하는 것이 가능하며, 별도의 인증이 없는 상태에서 수신자는 어떤 데이터가 안전한지 구별할 수 없다는 문제점을 지닌다.

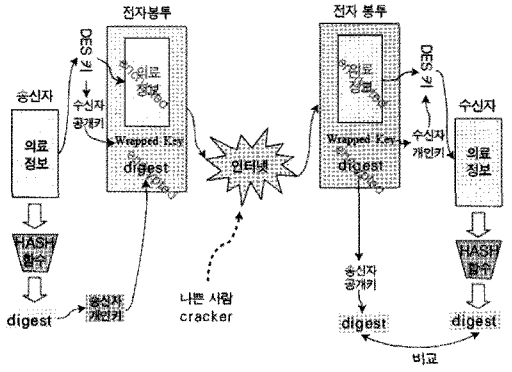
다. RSA+전자서명

앞서 기술하였듯이 송신자 식별에 대한 RSA의 취약점을 보완하기 위하여 전자서명을 도입한 기법이다. 전자서명은 서명자를 확인하고 전자문서에 서명을 하였음을 나타내는 데 이용하기 위하여 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 의미한다. 공개키 기반 구조 (PKI) 기술측면에서 전자서명이란 전자문서의 해쉬값(HASH)에 서명자의 암호화 키로 암호화한 것이다.

<그림 8>은 RSA와 전자서명을 혼합한 암호화 기법의 과정을 나타낸다. 의료정보의 해쉬값은 공개키로 암호화된 후, 의료정보와 함께 전송한다. 이러한 전자서명의 검증은 생성과정의 역변환이다. 수신자는 의료정보에 첨부된 해쉬값을



〈그림 8〉 RSA+전자서명

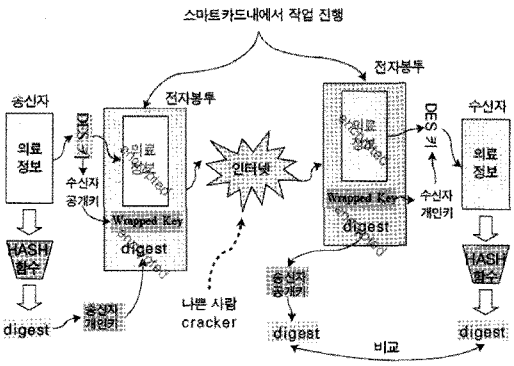


〈그림 9〉 DES+RSA, 공개키기반 전자서명

개인키로 복호화한 결과와 의료정보의 해쉬값을 비교하게 되며, 동일한 값이면 서명이 올바른 것이고 값이 서로 다르거나 변환에 오류가 있으면 서명이 틀린 것이다. 하지만 침입자에 의해서 의료정보가 노출이 될 수 있으므로 전송될 정보의 암호화가 필요하다.

라. 혼용 암호화 기법

정보에 대한 보안 수준을 보다 향상시키기 위하여 각종 암호화 알고리즘 및 전자서명을 혼용하여 사용하는 기법도 있다. <그림 9>는 DES와 RSA 암호화 알고리즘 및 공개키기반 전자서명을 결합한 기법을 도식화한 것이다. 이 기법은 송신자와 수신자 양측이 각각 공개키, 개인키를 가진다. 송신자 측에서는 해쉬값을 송신자 개인키로 암호화하여 전자서명을 한 후, DES 키로 암호화 한 의료정보와 수신자 공개키로 DES 키를 암호화한 Wrapped Key를 통합하여 전송한다. 수신자는 Wrapped Key를 수신자 개인키로 복호화하여 DES 키를 획득할 수 있으며, 암호화된 의료정보를 해독 가능하다. 전자서명된 해쉬값을 송신자 공개키로 복호화한 결과와 의료정보의 해쉬값을 비교하여 서명을 확인하는 기법이다.



〈그림 10〉 스마트카드, DES+RSA, 전자서명

하지만 이러한 복잡한 알고리즘을 적용하는 기법도 결국 송신자와 수신자 사이에는 인터넷을 통한 정보전송이 이루어지므로, 침입자가 이를 가로채는 위험성이 존재한다. 따라서 <그림 10>과 같이 스마트카드 내에서 작업을 수행한다면 높은 수준의 보안을 유지할 수 있다.

V. 의료정보보호 기술 표준

의료정보 기술 표준은 ISO/TC215, ASTM, HL7, DICOM 등과 같은 표준화 기구들의 활동을 통해 독자적, 상호 협력적으로 개발되고 있

다. 본 장에서는 의료정보보호 기술 표준을 위한 각 표준화 기구의 표준 내용에 관하여 기술한다.

1. ASTM E31.20

E1714-00, Standard Guide for Properties of a Universal Healthcare Identifier (UHID): 환자에 대한 유일한 식별성을 제공하며, 의료정보보호를 위한 보안 기술이 적용되어야 하는 UHID 속성에 대해 언급한다.

E1762-95 (2003), Standard Guide for Electronic Authentication of Health Care Information: 디지털 서명 과정의 특성, 속성, 최소 요구사항을 정의하며, 의료서비스에서 활용 가능한 서명 기술을 설명한다.

E1869-04, Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records: 기밀성, 프라이버시, 접근 그리고 개인을 식별할 수 있는 의료정보의 보안을 위한 원칙들을 언급한다.

E1985-98 (2005), Standard Guide for User Authentication and Authorization: 의료정보시스템을 사용하는 사용자 인증, 의료정보 문서의 접근이나 특정 작업을 허용하는 권한제어 메커니즘에 대한 내용이다.

E1986-98 (2005), Standard Guide for Information Access Privileges to Health Information: 건강정보와 관련된 환자 및 제공자의 권리에 대한 내용이 포함되어 있다.

E1987-98, Standard Guide for Individual Rights Regarding Health Information: 의료정보와 관련된 모든 개인에 대한 권리와 권리 운영 절차에 대해 기술한다.

E2084-00, Standard Specification for Authentication of Healthcare Information Using Digital Signature: 서명 및 해시 알고리즘, 공개키/비밀키의 관리, 암호키 및 인증서의 형식, 의료정보 문서에 대한 서명 방법 등이 주요 내용이다.

E2085-00a, Standard Guide on Security Framework for Healthcare Information: 의료정보에서 상호 운용성을 지원하는 프로토콜과 메시지 형식으로 기존 표준의 재사용 및 확장에 대해 정의한다.

E2086-00, Standard Guide for Internet and Intranet Healthcare Security: 인터넷 프로토콜을 사용하는 네트워크에서의 의료정보를 보호하기 위한 메커니즘에 대해 기술한다.

2. ISO/TC215 WG4

ISO/DIS 17090-1: Health informatics - Public Key Infrastructure-Part 1: Framework and overview: 헬스케어 환경의 PKI에 대한 기본 정의와 컴포넌트를 정의하고 상호 호환성 보장을 위한 요구사항, 보안 서비스 시나리오, PKI 에서 사용되는 인증서 종류 및 공개키 암호 기술 등을 설명한다.

ISO/DIS 17090-2: Health informatics - Public Key Infrastructure-Part 2: Certificate profile: 의료정보시스템 환경의 특성을 반영한 PKI 인증서 프로파일 명세서이다.

ISO/DIS 17090-3: Health informatics - Public Key Infrastructure-Part 3: Policy management of certification authority: 헬스케어 PKI 구축 및 운영의 가이드라인으로서, 인증서 정책의 구조 및 요구사항, 인증서 정책의 구조, 요구되는 보안 레벨, 보안 정책 내에 포함되어야 할 요구사항 등을 기술한다.

ISO/DIS 27799: Security Management in Health using ISO/IEC 17799: 의료정보시스템 환경에서 요구되는 전반적인 보안 기술에 대한 가이드라인과 같은 표준 문서로서 보안의 목표, 보안 대상 자원, 발생 가능한 공격 및 취약점, 요구되는 보안 기술 등을 포함한다.

ISO/TS 22600-1: Health informatics - Privilege management and access control-Part 1: Overview and policy management: 다자간 의료정보의 전달 및 공유가 이루어지는 환경에서 정보에 관한 권한관리 및 접근 제어 방법을 제시한 기술 표준으로서, 관리 대상 데이터 분석, 권한 정책 항목 분석, 권한 관리 시나리오 등을 주로 기술한다.

ISO/TS 22600-2: Health informatics . Privilege management and access control-Part 2: Formal models: 의료정보 권한 관리 모델(도메인 모델, 정책 모델, 역할 모델, 위임 모델, 접근 제어 모델 등)을 제시하고 있다.

3. HL7 SIG

HL7은 보안 특별 관심그룹(SIG)을 통해서 HL7 메시지가 라우터 중계로 통신하는 경우 발생 가능한 보안 위협을 하위 네트워크, 종단간 네트워크, 세션 중심 응용, 저장 및 전달 중심 응용 등 통신 계층에 따른 위협으로 분류하였다. 또한, 이들 각각에 대하여 인증, 권한 관리와 접근제어, 무결성 및 기밀성 보장, 부인방지 등 보안서비스 요구사항을 정리하였다. 현재 HL7 보안 기술위원회는 보안 서비스 프레임워크(HL7 Security Service Framework)와 HL7 EDI 통신보안에 관한 가이드(Standard Guide for Implementing HL7 EDI Communication Security) 작성의 필요성이 인식되고 있어 앞으로도 표준화 작업을 활발히 진행할 것으로 기대된다.

4. 의료정보보호 법 · 제도

의료정보보호 표준화는 위와 같은 기술적인 내용 이외에도 법 · 제도와 관련된 내용이 더 활발하게 이루어지고 있으며, 대표적으로는 미국의 건강보험 이전가능성 및 책임에 관한 법률(이하 HIPPA)이 있다. 이 법률에서 개인 프라이버시와 보안을 포함하는 개인의료정보보호에 대한 언급을 하고 있다. 또한 보호되어야 할 개인 건강의무기록(Protected Health Information)이라는 의미로 PHI로 명명하였으며, 개인 신원 확인 정보(이름, 사진, 주소, 주민번호 등 개인을 식별할 수 있는 모든 정보)와 의료기록, 치료비, 과거/현재/미래 병력 등이 이에 해당한다.

HIPPA 프라이버시 규칙이 가지는 의미는 특히 환자 개인에 대하여 개인건강기록 공개제한 요구 권리, 비밀연락과 건강 기록수정 요청 권리,

공개 내역에 대한 권리, 개인 건강 기록 조사 및 사본 입수 권리 및 침해 발생 시 진정서를 제출할 수 있음을 명시하고, 환자의 허가나 동의가 필요한 경우를 분명히 정의함으로써 의료정보의 제공시 프라이버시 침해를 최소화하고 법적 분쟁 소지를 없애는 효과를 주었다는 점이다.

그러나 HIPPA가 의료정보 프라이버시와 보안에 대해서 언급하고 있으나, 데이터의 소유권에 대해서는 언급하지 않아 진료자료의 소유권 문제가 발생할 소지가 있는 것이 사실이다. 즉, 휴·폐업으로 인한 해당 기관의 개인의료정보는 누구에게 귀속되어 관리되어져야 하는지에 대한 명확한 규정이 정립되어 있지 않고 프라이버시는 개인에 따라 매우 다르게 규정될 수 있는 사항이다. 따라서 국내 의료 관련 정보보호 법·제도 제정 및 보완 시에 의료 데이터의 보안 및 프라이버시뿐 아니라 소유권에 관한 문제도 반드시 심각하게 고려해야 한다.

국내의 경우 개인 의료정보보호, 원격 의료 시설, 전자 의무 기록 등과 관련, 처방 및 의료정보 등의 환자 비밀 준수 조항, 전자 의무 기록 관리 및 보관 의무화 등과 같은 현행 의료법 조항을 규정하고 있으며, 2006년 보건복지부는 보건 의료정보화 사업 추진과 관련하여 건강 정보보호 체계를 구축하기 위해 환자의 개인 의료정보보호 및 프라이버시 보호 권리, 개인 의료정보 취급자의 보호조치 의무와 책임, 의료정보 관리 절차 등을 포함한 개인의료정보보호법 제정을 위해 건강정보보호자문위원회를 운영 중이다.

VI. 향후 의료정보보안 기술

앞서 기술한 바와 같이 의료정보보안 기술은 의료정보시스템에 보안기술이 내재된 형태이며, 독자적으로 존재하는 기술이라고 보기 어렵다. 의료장비에서 기존 TCP/IP 기반의 인터넷 프로토콜이 지원되면서, 네트워크 장비 회사는 의료분야 정보보호에서도 이전에 사용하던 네트워크 정보보호 솔루션을 그대로 적용 가능하다고 판단하는 경향이 크다. 하지만 어디까지나 네트워크 보안 관점에서 기존 보안 장비와 큰 차이가 없을 뿐이며, 유비쿼터스 환경을 기반으로 하는 u-Health의 관점에서 중요한 개념인 헬스케어 보안과 사용자 프라이버시에 대한 고려가 포함되지 않았다.

u-Health 서비스에서 무선 네트워크에 대한 보안 문제는 단순히 네트워크에 대한 보안 이슈일 뿐이며, 의료정보화와 관련된 특별한 이슈라고 보기는 어렵다. 반면, 사회적으로 개인프라이버시 보호에 대해 관심이 높아지는 추세로, u-Health의 등장으로 인하여 개인 의료정보보호에 대한 우려가 심화되고 있다.

또한 통합적인 시스템에서 모든 의료정보를 관리하는 경우, 환자와 의료기관 종사자 간의 입장 차이로부터 의료 서비스의 편리성과 개인정보 보호 권한 사이의 상충이 발생될 수 있다. 데이터를 제공하는 환자 입장에서는 개인 의료정보에 대한 철저한 보호를 요구하지만, 의료진의 입장에서는 의료통계 및 임상연구에 전반적인 의료정보를 활용하여 치료 기법의 향상을 도모하기 때문이다. 이와 같이 의료서비스를 선진화하여 공공 이익에 기여하기 위해서는 개인 의료정보에 대한 일정 수준이상의 활용이 반드시 수반되게 된다.

u-Health를 활성화하며 편리성, 효율성, 상호운용성을 보장할 수 있는 의료서비스의 실현에는 표준화된 의료정보보호 기술 개발이 필수적

이다. 이뿐만 아니라 원격진료 등의 선진적인 의료 서비스를 제공하는 경우에도 보다 높은 신뢰성 및 정보 보안성을 통하여 사용자의 거부감을 최소화할 필요가 있다. 따라서 기술, 법·제도, 윤리적 등의 측면을 다각도로 고려하여 의료정보의 기밀성, 보안성은 물론 개인의 프라이버시까지 보호해야 한다. 체계적인 의료정보보호 표준화와 정보보호 기술의 완성이 달성된다면, 각종 센서, 무선 단말기 등의 결합으로 이루어진 네트워크를 기반으로 보다 지능화 및 고도화된 u-Health 서비스를 실현 가능할 것이다.

참고문헌

[1] 정보통신산업진흥원 통계분석팀, "10대 IT 융합 분야 동향 및 시사점", IT Insight, 2010-01호, 2010.04.

[2] Wikipedia, http://en.wikipedia.org/

[3] 대한의료정보학회, "보건의료정보학", 현문사, 2003.

[4] 임재덕, 은성경, 김정녀, "데이터 보호를 위한 암호화 파일시스템의 분석", 보안운영체제연구팀, 2001.08.

[5] 김신효, 송지은, 정명애, 정교일, "의료정보화 및 보안 기술 표준화 동향", 한국전자통신연구원 (ETRI), 전자통신동향분석 제 21권 제 6호, 2006.12.

저자소개

임 채 균

2007년 2월 언남고등학교
2007년 3월~2010년 5월 을지대학교 의료산업학부 재학 중

주관심 분야 : Ubiquitous, AI, Healthcare, Data Mining

이 기 영

1984년 3월 숭실대학교 전자계산학과(공학사)
1988년 3월 건국대학교 컴퓨터정보통신공학과(공학석사)
2005년 8월 건국대학교 컴퓨터정보통신공학과(공학박사)
1984년 3월~1991년 2월 한국해양연구원 연구원
1996년 3월~1998년 3월 한국컴퓨터정보학회 이사 및 서울동부지회장
2009년 1월~현재 한국인터넷방송통신학회 이사
2010년 1월~현재 대한전자공학회 컴퓨터소사이어티 이사

주관심 분야 : u-Healthcare, 공간 데이타베이스, GIS, LBS, USN, 텔레매틱스

저자소개

임 명 재

1998년 중앙대학교 공학박사
1992년~현재 을지대학교 의료산업학부 교수

주관심 분야 : SE 개발방법, HCI, U-Healthcare 등

정 용 규

1981년 2월 서울대학교 이학사
1994년 8월 연세대학교 공학석사
2003년 2월 경기대학교 이학박사
1994년 4월~현재 UN/CEFACT TBG3 위원
2001년 7월~현재 ISO TC154K 위원장
2007년 4월~현재 KS e비즈니스기술심의위원

주관심 분야 : 임상데이터분석, 지능형시스템, e-Trade