情 報 保 護 學 會 誌
第19卷 第3號, 2009. 6

융합보안 R&D 이슈 및 방향

정 수 환*

요 약

최근 IT기술이 각종 산업에 융합된 제품군에 다양한 보안 솔루션이 탑재되면서 융합보안 산업이 차세대 고부가가치 산업으로 부상하고 있다. 이종 산업간 융합은 사용자들에게 편리함을 제공해 주지만 이와 반대로 다양한 보안적인 이슈 사항을 야기 시켰다. 따라서 본고에서는 현재 부상하고 있는 차세대 융합산업에 대한 동향을 몇 가지 사례를 중심으로 분석 하였고, 또한 해당하는 융합산업 분야에서 발생하는 보안 이슈와 요구되는 보안기술을 분석하였다.

Ⅰ. 서 론

최근 IT기술이 각종 산업에 융합된 제품군에 다양한 보안 솔루션이 탑재되면서 융합보안 산업이 차세대 고부가가치 산업으로 부상하고 있다. 이에 따라 지난해 말 지식경제부는 '지식정보보안산업 진흥 종합계획'을 수립하였으며, 기존 정보보호를 정보보안·물리보안·융합보안 등 3개 원천 기술로 확대·개편하고 2013년까지 총 1,500억원의 R&D 자금을 투입하겠다고 발표하였다.

본고에서는 현재 화두가 되고 있는 융합산업의 몇 가지 사례를 제시하고 필요한 보안기술을 분석함으로써 국가 R&D 방향 설정 시 참고자료로 활용하고자 한다.

Ⅱ. 융합산업 동향 및 보안기술 분석

2.1 u-헬스케어

IT기술과 의료기술의 융합인 u-헬스케어는 차세대 미래 의료 서비스의 대표기술로, 시공의 제약 없이 질환의 예방부터 치료 및 사후관리까지 받을 수 있는 잠재적 성장이 매우 높은 융합산업이다. 특히, 일본 미쓰비시 종합연구소의 연구결과에 의하면 세계 u-헬스케어 시장은 오는 2010년 약 3,800억 달러 규모로 연간 평균 약 20% 이상 성장할 것으로 예측되고 있다.

우리나라의 경우 인구노령화가 급진전되고 건강에 대한 관심이 높아지면서 u-헬스케어는 미래 유망 먹거리 사업으로 떠오르고 있기는 하나, 현재 법제도적인 한계뿐만 아니라 안정적인 비즈니스 모델 부재 등 여러 가지 제약요인으로 인해 u-헬스케어 시장은 더디게 진행되고 있다.

u-헬스케어 서비스에서 보안상 가장 큰 제약요인은 바로 개인정보보호 문제이다. 데이터 송·수신시 전송되는 의료정보 및 서버에 저장되어 있는 개인정보 등이 유출될 경우 고용주·보험업자 등에게 악용될 소지가 크기 때문이다. 프라이버시를 보호하고 해킹 등으로부터 데이터의 안정성을 검증받기 위해서는 기 축적된 여러 가지 보안기술의 적용이 선결되어야 한다.

예를 들면, 건강/의료 정보에 대한 프라이버시보호 기술, 전자의무기록(EMR, Eletronic Medical Record) 등의 안전한 교환 및 공유 기술, 멀티 도메인 간 인증 및 ID관리 기술, 헬스케어시스템의 보안 정책관리 기술 등이 대표적인 u-헬스케어 서비스 상의 정보보안 기술이라 할 수 있다.

2.2 차량 블랙박스

IT기술이 자동차에 응용된 차량블랙박스의 경우, 사고순간을 영상을 통해 기록함으로써 명확한 책임규명이 가능하고, 운전자로 하여금 안전운전을 유도해 사고율을 줄여주는 역할을 수행하면서 최근 블루오션으로 떠

* 지식경제부 지식정보보안 Program Director, 숭실대학교 정보통신전자공학부 (souhwanj@ssu.ac.kr)

오르고 있는 융합산업 제품이다.

하지만 이런 효용성에도 불구하고 우리나라는 아직 차량용 블랙박스가 활성화되지 못했다. 그간 장비가 비쌌던 이유도 있으나, 관련법규도 아직 미흡한 실정이다. 미국이나 유럽 일부 국가에서는 이미 차량용 블랙박스를 의무화하는 법안을 구체화하고 있다. 유럽에선 2010년도부터 모든 차량에, 미국은 2011년부터 4.5톤 이하의 모든 차량에 블랙박스 장착을 의무화하는 것을 추진하고 있다.

현재 국내에 판매되고 있는 차량용 블랙박스의 기본 기능은 차량 내부 또는 외부 상황에 대한 영상 및 음성을 저장하는 것이다. 그러나 이에 따른 보안상 문제점도 부각되고 있다. 차량 내 룸미러에 장착되는 블랙박스는 운전석 외부뿐만 아니라 내부까지 영상과 음성을 기록하기 때문에 프라이버시 침해 및 통신비밀보호법 위반 소지가 있다.

이를 위해서, 차량 내외의 특정 공간 외에선 영상을 기록하지 못한다거나 영상기록의 목적 외 이용을 제한한다는 등의 관련법제도가 마련되어야 할 것이다. 또한 기술적으로는 프라이버시 마스킹 기술과 같이 수집된 영상정보 중 사생활 침해 가능성이 높은 영상 정보만을 선택적으로 실시간 암호화 하거나 마스킹 하는 기술 등이 뒷받침되어야 한다.

지난 2월 발족한 텔레매틱스산업협회 산하 '차량용 영상블랙박스 표준화 포럼'에서 차량 사고 시 법정에서 인정될 수 있는 표준 및 규격(안)을 마련한다고 발표한 바 있다. 본 포럼에도 초창기부터 보안전문가가 적극 참여하여 단말기에 대한 형식승인 및 인증체계 구축 등에 보안기술이 내장될 수 있도록 노력해야 할 것이다.

2.3 Smart Grid (지능형 전력망)

Smart Grid는 기존 전력망에 IT기술이 접목된 형태로서 차세대 유망 융합산업의 하나로 떠오르고 있다. 스마트그리드란, 지능형 장치(Intelligent Devices), 양방향 통신(Two-way Communications), 고급제어시스템(Advanced Control Systems) 등을 통해 전력망의 효율성, 신뢰성, 안정성을 높이기 위한 IT 기반의 송·변전, 배전 운영방식을 의미한다.

정보통신산업이 전력산업에까지 융합·확장되면서 정보통신 네트워크 및 기기에서 발생하고 있는 보안문제가 전력부문에서도 그대로 재현되고 있다. 실례로, 2007년 미국 에너지부의 아이다호 국립 연구소(Idaho National Laboratory)에서 전력망에 대한 사이버공격을 실험한 결과, 해커가 발전기를 통제하고 파괴할 수 있음을 여실히 보여주었고, 2008 RSA Conference(미국정보보안기술박람회)에서 한 보안 전문가는 전력업체 직원이 일반인이 흔히 사용하는 이메일 서비스를 이용하다가 악성프로그램을 자신의 컴퓨터에 다운로드하게 되고, 나아가 발전소 전체를 마비시키는 과정을 상세히 보여줬다.

우리나라도 과거에는 전력망 통제시스템이 폐쇄적으로 운영되어 공공 네트워크와 분리되어 있었으나, 점차 IP(Internet Protocol)기반 시스템에 의존하면서 보안상 문제점이 속속 제기되고 있다. 따라서 전력인프라에 대한 사이버공격을 방지하기 위해서는 기본적으로 전송되는 데이터의 무결성 및 신뢰성, 통신상의 기기 및 사용자에 대한 인증, 시스템의 보안정책 권한관리, 각종 네트워크 및 시스템 보안 기술 등이 적용되어야 할 것이다.

미국의 경우 Smart Grid 사업 추진 시, 에너지관련 업체뿐만 아니라 IT 기업, 보안기업의 컨소시엄 구성을 통해 점차 지능화·다양화되고 있는 사이버공격에 적절한 대응책 마련을 위해 고심 중이다. 우리나라도 스마트그리드 사업 추진 시 전력인프라의 사이버보안을 최우선정책으로 설정해야 할 것이다.

Ⅲ. 결 론

본고에서는 융합산업의 몇 가지 사례에서의 보안 문제점을 살펴보았다. 이러한 사례들을 참고하여 융합산업의 보안상 위협을 심도 있게 분석하여 차후 지식정보보안 R&D 방향 설정 시 활용되어야 할 것이다.

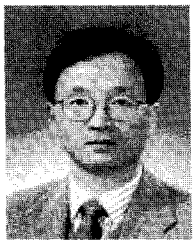
참고문헌

[1] Alfred C. Weaver, Samuel J. Dwyer Ⅲ, Andrew M. Snyder, et, al., "Federated Secure Trust Networks for Distributed Healthcare IT Services," IEEE International Conference on Industrial Informatics, August 2003.

[2] 송지은, 김신효, 정명애, "u-헬스케어 서비스에서 의료정보보호", 정보보호학회지, 17(1), pp. 47-55,

2007. 2.
[3] 김창복, 이상순, 이병수, "상황인식 기반의 적응형 u-헬스케어 보안체계에 대한 연구", 한국정보기술학회논문지, 6(4), pp. 37-46, 2008. 8.
[4] 문상춘, "에너지 절감형 주택의 스마트 공간 구축", 전력전자학회지, 14(2), pp. 27-31, 2009. 4.

〈著者紹介〉



정 수 환 (Souhwan Jung)
정회원

1985년: 서울대학교 전자공학과 졸업
1987년: 서울대학교 전자공학과 석사
1996년: University of Washington 전자공학 박사
1997년~현재: 숭실대학교 정보통신전자공학부 부교수
2009년~현재: 지식경제부 지식정보보안 PD
<관심분야> 이동인터넷 보안, 네트워크 보안, VoIP 보안, RFID/USN 보안