IT 융합보안에서의 위협요소 분석

이근호
백석대학교 정보통신학부

Analysis of Threats Factor in IT Convergence Security

Keun-Ho Lee
Division of Information Communication, Baekseok University

요 약 정보통신기술 발전에 따라 많은 장치들간의 통신과 네트워킹의 수용이 이뤄지고 있다. 장치간의 통신을 위한 융합 사업이 빠르게 발전되어지고 있다. IT 융합 통신은 무선통신에서 차후 개척분야의 하나로 여겨지고 있다. 본 논문에서는 IT 융합 구조에서 M2M, 지능형 자동차, 스마트그리드, U-헬스케어에 대한 보안 위협요소를 분석하였다. 임베디드 시스템 보안, 포렌식 보안, 사용자 인증과 키관리 기법에 대한 IT 융합 보안의 방향을 제안하였다.

Abstract As the developing of the information communication technology, more and more devices are with the capacity of communication and networking. The convergence businesses which communicate with the devices have been developing rapidly. The IT convergence communication is viewed as one of the next frontiers in wireless communications. In this paper, we analyze detailed security threats against M2M(Machine to Machine), intelligent vehicle, smart grid and u-Healthcare in IT convergence architecture. We proposed a direction of the IT convergence security that imbedded system security, forensic security, user authentication and key management scheme.

• Key Words : Convergence Security, Machine to Machine, Intelligent Vehicle, Smart Grid, U-Healthcare

1. 서론

최근 정보통신분야는 유비쿼터스 환경으로 빠르게 변화가 진행되고 있다. 유비쿼터스 환경에는 최신 IT기술을 기반으로 여러 산업분야와의 연계를 통해 연구개발이 활발히 진행 중이다. 이러한 산업계간의 연구를 통해 여러 분야의 산업에 융합된 새로운 제품군과 다양한 서비스가 나오고 있다. 새로운 제품과 다양한 서비스의 활성화에 따른 새로운 보안 위협요소들이 대두되고 있다. 산업간의 융합이 활발하게 이루어지고 있는 분야는 장치와 기계간의 통신을 위한 M2M (Machine to Machine), IT 기술과 의료기술의 융합인 U-Healthcare, IT 기반의 송.변전, 배전 운영을 위한 Smart Grid, IT 기술이 자동차와 연계한 지능형 자동차 등 많은 분야에서 융합이 이뤄지고 있다.

M2M은 machine to machine, mobile to machine, 그리고 machine to mobile의 통신을 의미하며, 장치 및 기계들을 통해 우리의 일상생활 속에 널리 퍼져있는 기기 및 장비간의 네트워킹이다. M2M 통신은 기기 및 장치의 기구들을 통한 컴퓨팅과 전자 제품간에 정보를 제공할 수 있도록 연결해 사용하는 이동통신 사업자의 새로운 비즈니스 모델을 위한 새로운 통신 개념이다. M2M 통신을 통해 사람과 사물 사이의 상호작용을 통해 위치, 건강, 온도 등 다양한 데이터를 수집할 수 있다[1].

지능형 자동차는 텔레메틱스/ITS 연구 개발을 통해서 차량에 IT 기술을 접목하여 차량의 운전자와 탑승자에게 교통정보 안내, 긴급구난, 원격차량진단, 인터넷 서비스 등을 제공하여 Mobile Office의 움직이는 비즈니스 공간으로 발전되어 가는 융합분야이다[3,4].

Smart Grid는 전력 자원에 대한 효율적인 관리와 정보통신 정보기술과 융합되어 가정 및 산업에 전력 공급 및 수급을 위한 양방향성과 중앙관제를 통한 효율적인

전력 에너지 자원의 소비효율을 최적화 하고자 구현되고 있는 차세대 전력망으로서 융합의 한분야이다[5.6].

U-Healthcare는 IT분야와 의료 서비스 분야의 융합을 통하여 환자가 언제, 어디서나 자신의 건강상태가 의료진에 의해 모니터링되어 건강관리 와 의료서비스를 제공하는 차세대 의료서비스 분야이다[7.8].

본 논문에서는 융합분야의 대표적인 기술인 M2M통신, 지능형 자동차, Smart Grid, U-healthcare 기술 분야에 대한 내용을 살펴보고, 각 분야에서 융합에 따른 새로운 환경과 새로운 서비스에 따른 다양한 보안 위협요소들을 분석하고, IT 융합에서의 보안 위협요소에 대응하기 위한 방향을 제안하였다.

2. 관련연구

2.1 Machine to Machine

언제어디서나 원하는 정보를 쉽게 얻을 수 있는 개념이 우리 생활에 까지 파고들면서 새로운 유비쿼터스 서비스 산업이 크게 활성화되고 있다.

M2M(사물통신) 서비스는 표 1과 같이 산업, 환경, 사회의 영역으로 구분되어 지며, 주변의 사물이나 기기에 정보를 수집하고 통신을 가능하게 하는 장치를 설치한 후 이를 통하여 수집되거나 상호 공유되는 정보를 이용하여 사용자 혹은 사물 자체에게 정보를 제공하는 정보서비스의 개념이다[9].

[표 1] M2M 서비스 형태

서비스 영역	설명	예
산업	산업체, 회사 등과 같은 조직간에 발생하는 금전적/상업적인 활동 관련	제조, 물류, 뱅킹, 금융 감독, 중개 등
환경	자연환경에 대한 보호, 감시 및 개발 관련	농업, 축산업, 재활용, 환경 관리 서비스, 에너지 관리 등
사회	사회, 도시 및 사람 관련	헬스케어, 장애/노약자 보호 서비스, 교통, 치안 등

M2M에서의 적용할 수 있는 주요기술은 식별기술, 정보수집기능, 통신네트워크 기술, 지능화 기술, 소형화 기술이 필요하다.

식별기술은 사물들을 외부로부터 질의에 대응하거나 외부로의 질의를 가능하게 하는 식별자로써 전파를 이용하는 RFID 기술을 이용하고 있다. 정보수집기술은 사물의 물리적인 상태 정보와 주변 환경 정보를 수집하기 위해 센서기술과 센서가 탑재된 장치간의 네트워킹 기술을 이용하고 있다. 통신 네트워크 기술은 사물간의 정보 전송을 위한 통신은 유선과 무선, 이동통신 등으로 구분하며, 3G나 4G와 같은 이동통신기술을 사용하고, 무선랜과 유선네트워크를 사용하며, 배터리 소모를 줄일 수 있는 저전력 및 소형 기기를 위한 무선 통신 기술이 필수적이다. 지능화 기술은 사물에 내장된 정보처리 능력으로 자체적인 정보처리 능력과 외부 환경의 변화에 스스로 대응하는 기술이다. 소형화 기술은 모든 기기 및 사물에 통신과 컴퓨팅 장치가 탑재되어야 하므로 소형화가 필요하며 비용에 대한 절감이 필요하다[1].

2.2 지능형 자동차

지능형 자동차는 디지털 홈, 텔레매틱스, 지능형 로봇 등이 접목되어 네트워킹 및 인포테인먼트가 가능한 형태로 진화되고 있다. 특히 차량의 경우 IT와 컨버전스를 통해서 비즈니스 모델 뿐만 아니라 AM 시장을 확대하고 있다. C2E(Car to Enterprise), C2C(Car to Car), C2H(Car to Home)간의 다양한 서비스 모델을 제시하고 있다. 지능형 자동차의 서비스 구성요소는 그림 1와 같이 차량제어 시스템을 기반으로 실시간 제어 네트워크를 통해서 교통정보, 생활정보, 안전 , 원격 고객 관리, 엔터테인먼트, 보안 서비스를 제공한다.

[그림 1] 지능형 자동차 서비스 유형

이러한 서비스는 실시간 제어 네트워크를 통해 차량제어 시스템을 기반으로 구동하게 되어 있다[3].

2.3 Smart Grid

스마트 그리드는 전력 시스템과 IT 기술이 융합된 차세대 전력망으로서 발전, 송전, 배전, 소비에 이르기까지 전력을 실어 나르는 모든 설비 및 기기를 의미한다.

스마트 그리드는 표2와 같이 기존 전력망의 신뢰성, 효율성, 안전성을 필요로 하며, 전력 생산・소비 정보를 양방향・실시간으로 수평적으로 유통함으로써 에너지 효율을 최적화하고, 디지털을 기반으로 구현되어, 공급자와 수요자를 기반으로 운영된다[5].

[표 2] 스마트 그리드와 전력망 비교

구분	스마트 그리드	전력망
통신방향	양방향	단방향
전원방식	분산(수평적)	중앙집중(수직적)
구현구조	망(네트워크)	방사형
전력흐름	양방향	단방향
구현기술	디지털	아날로그
설비운영	공급자+수요자	전력공급자 중심
리스크관리	자동	수동

2.4 U-Healthcare

IT발전과 의료기기 기술의 발전에 따라 언제 어디서나 의료정보를 확인하는 U-Healthcare는 표 3처럼 소비자 위주의 네트워크화된 건강관리로서 의사와 환자가 의사결정을 하게 되며, 환자 데이터는 항상 접근이 가능하고 관리가 가능해야 한다. 인터넷 포탈을 중심으로 사용자의 운동, 신체 건강 상태, 다이어트 계획 등을 저장하고 이를 사용자와 전문가가 정보를 공유하면서 개인의 건강에 관심을 갖고 관리하는 형태의 서비스가 제공된다.

대부분의 헬스케어 서비스가 만성병 또는 증세를 가진 사용자가 자신의 신체 지수 등을 기록하여 정량적인 측정과 치료 활동을 더불어 건강 관리를 쉽게 해 주는 서비스가 공통적으로 제공된다[7].

[표 3] u-헬스케어와 전통적 의료서비스 비교

구분	U-헬스케어	전통적 의료
서비스 주체	소비자 위주	병원 등 전문기관
연계 구도	네트워크화	독립화
목적	건강관리	진단 및 치료
의사결정자	의사와 환자	의사
진료정보	접근 및 관리 상시 가능	제한적인 접근 및 관리

3. 융합보안에서의 보안 위협요소

융합 보안은 정보보안 또는 물리보안이 비 IT기술 또는 다른 산업과 융합되어 창출되는 보안 제품 및 서비스를 의미한다. 표 4는 지식경제부에서 발표한 융합보안 적용이 필요한 산업과 적용 가능한 기술 분야에 대한 내용이다[10].

[표 4] 융합보안 적용 분야와 기술

적용분야	기술 분야
운송보안	차량 지능키, 차량전자번호판, 차량블랙박스, 차량간 통신보안모듈, 차량통합보안관리, 승객용 스크리너, 조선 보안
로봇보안	보안로봇, 네트워크로봇 보안
금융보안	금융 ATM기기, OTP, 금융 IC카드
의료보안	의료영상보안제품, 의료 DB 공유보안시스템
건설보안	지능형 건물/오피스 침입감지, 홈네트워크 보안
국방보안	국방보안장비
산업보안	산업용 기기 보안

3.1 Machine to Machine 보안 위협요소

장치와 기계간에 사용되는 M2M 망에서는 기기나 기계간의 이동으로 인한 잦은 형태 변화와 무선 채널을 사용하는 구조적인 취약점을 가지고 있다. 빈번한 네트워크의 변화와 무선채널의 위험에 대한 안정적이고 효율적인 해결 방안이 요구된다. 안정적인 M2M 네트워크를 구성함에 있어 가장 중요한 사항 중의 하나는 보안관련 요소이다. 보안의 특성을 통한 가용성, 기밀성, 무결성, 인증, 부인봉쇄와 같은 보안 요구들을 충분히 만족할 수 있는 보안 프로토콜이 요구되어 지며 부합하는 보안 요소 기술 개발이 필요하다. 무선 채널을 통한 링크 사용과 제한된 자원, 물리적인 자원의 제한, 빈번하게 형태가 바뀌는 네트워크의 특성을 감안하여 다음의 고려사항을 살펴보아야 한다. 인가되지 않은 비밀 정보 접근, 기밀성 훼손을 도청과 네트워크 외부 적의 공격으로 인한 메시지 삭제 변조, 변질된 이동 Machine(compromised node)로부터 오는 부적절한 정보 및 공격이다.

M2M에서의 기밀성, 무결성, 프라이버시보호, 디바이스 인증, 시스템 가용성 등의 보안의 조건을 위해서는 다음의 보안 위협을 고려해야 한다.

- 기밀성 : M2M 통신 환경에서는 데이터 노출로 인한 위치, 개인정보, 과금 데이터 등의 민감한 정보를 전송을 하기 때문에 네트워크 어느 곳에서나 도청에 의해 수집되는 데이터 유출을 예방하기 위해 데이터의 기밀성을 보장해야 한다.

- 무결성 : 중간자(man-in-the-middle) 공격을 통한 데이터의 불법 변경 및 삭제, 위조된 데이터의 삽입 등에 대응하기 위한 무결성 보장이 필요하다.

- 가용성 : 서비스 거부공격(DoS)은 시스템의 가용성 및 생산성을 훼손함으로써 시스템 자원과 정보에 대한 접근 능력을 감소시킬 수 있다. 따라서 M2M 통신 환경에서도 주체 또는 디바이스들의 정보 접근 능력을 침해하지 않도록 시스템 가용성을 보장 할 수 있는 보안 메커니즘이 필요하다.

- 개인정보보호 : 사용자의 개인정보 수집 및 도용은 M2M 디바이스가 사람의 일상과 밀접하게 연관되어 있으므로 사용자와 관련된 정보를 기록하게 된다. 이러한 사용자 데이터들의 불법적으로 노출 되는 경우, 개인 프라이버시 침해 문제가 발생할 수 있으므로 이를 방지 할 수 있는 보안 메커니즘이 필요하다. 이동성을 제공을 위한 위치추적의 경우 M2M 디바이스는 디바이스의 위치정보 노출로 인해 디바이스 및 디바이스 소유자의 위치나 이동 경로가 노출될 가능성이 존재한다. 따라서 이동성을 제공하면서 추적 불가능성을 제공할 수 있는 보안 메커니즘이 필요하다[1,2].

3.2 지능형 자동차 보안 위협요소

지능형 자동차 서비스에서 다양한 위협 모델은 표 5와 같이 무선채널 및 송수신 데이터에 대한 공격과 차량 네트워크 및 통신구조에 대한 보안메커니즘으로 구분된다.

[표 5] 지능형 자동차 취약성

구분	설명
Jamming	일정네트워크 영역 내에서 다른 차량의 통신에 장애를 초래하는 신호를 발생시키는 공격
Forgery	거짓정보를 발생하는 공격 차량에 의해 일정 네트워크 영역내의 다른 차량들을 거짓정보로 오염시키는 위협
In-transit Traffic Tampering	주행중에 메시지 또는 정보의 전달 과정에서 Drop, Corrupt, Modify 를 통한 정보의 위변조 공격
Impersonation	차량의 상태 정보를 변경하여 다른 차량으로 하여금 오인하도록 하는 공격
Privacy Violation	시간, 위치, 차량, ID, 이동 정보 등의 차량과 관련된 개인 프라이버시 정보에 대한 침해
On-board Tampering	차량 내부의 다양한 정보에 대한 위변조 공격

지능형 자동차의 안전성을 보장하기 위해서는 Security Hardware, VPKI, Authentication, Certificate Revocation, Privacy의 보안 프레임워크 구성이 필요하다. 차량 통신 보안을 위한 하드웨어로는 ELP(전자번호판), EDR(차량용블랙박스), TPD(차량용 TPM, Advanced EDR), 정보 수집을 위한 센서 등이 필요하다. 차량간의 안전한 통신을 보장하기 위한 인프라를 위해 PKI 기반의 인증 인프라의 구축도 이뤄져야 한다. 각 자동차마다의 정당한 사용자 인증과 보안 처리에 의한 오버헤드를 줄이기 위한 암호화 알고리즘을 사용하고, 빠른 인증 처리를 위한 인증기술이 있어야 한다. 인증 인프라에서 생성된 키 관리나 폐기 및 갱신은 매우 중요하므로 효율적인 키 관리, 폐기, 갱신을 위한 연구가 중요하다. 차량 간의 통신을 통해서 다양한 정보(시간, 위치, 차량 ID, 주변 정보 등) 실시간으로 개인정보 및 차량 정보가 노출되므로 개인정보 및 프라이버시 침해 대응기술이 연구되어져야 한다[3,4].

3.3 Smart Grid 보안 위협요소

기존의 전력망과 달리 Smart Grid의 보안 위협 발생 요인은 양방향 서비스, 사용자 단에 공공 설비 접근 경로 존재, 지능형 전력망 구성 장비간의 상호운용 증가, 많은 수의 지능형 전력망 구성 장비, 보안이 결여된 제어시스템의 도입으로 위협이 발생한다.

Smart Grid는 정보통신망이 기존에 가지고 있는 소프트웨어적인 부분과 네트워크 및 데이터베이스, 하드웨어적인 부분에 이르기까지 취약성을 갖는다.

스마트 계량기, 센서, 고도화된 통신네트워크와 전력망에서 운용되면서, 정보보안, 네트워크 보호 등에 관한 다양한 리스크가 표 6과 같은 공격유형에 따라 높아지고 있다.

[표 6] Smart Grid 공격 유형

구분	공격유형
공격방법	Remote Finger Printing, IP Scanner, Port Scanner, Third Party Effect
	Trinoo Attack, TNF Attack, Stacheldraht, TFN2K Attack
	Remote Active Attack, Etc
	IP, E-mail, Web, ARP, DNS
	Syn Flooding, Smuf Attack, UDP Flooding, Brute-Force Attack, Land Attack, Teardroo
	Hub Attack, Switch Jamming, ARP Redirect, ICMP Redirect, ICMP Router Advertisement

전력망 구현을 위한 정보흐름 경로는 총 3단계의 SGD(Smart Grid Device), SGN(Smart Grid Network), CC(Concentration Center)로 구성되어 지며 각 단계별 보안 취약점은 다음과 같다.

- SGD(Smart Grid Device)

스마트계량기의 램, 디지털 주파수, 멀웨어 그리고 팜웨어를 중심으로 하는 공격이 이루어진다. 최근 세계적인 공격 추세가 램 공격으로 최종 공격의 형태가 나타난다. 이는 공격자가 해당 기기의 램을 직접 공격하여 계량기를 통해 생성된 정보를 분석하여 분석된 정보를 기반으로 계량기를 조작하여 무결성을 침해한다. 또한 무선 주파수 교란을 통한 전력 정보의 차단, 계량기에 탑재된 관리 소프트웨어를 공격하는 멀웨어 바이러스와 트로이 목마와 같이 시스템을 방해하기 위한 소프트웨어와 코드 공격을 통한 데이터・컴퓨터・네트워크를 위험에 노출시키는 위협이 존재한다.

- SGN(Smart Grid Network)

전력 정보를 전송하기 위해 Edge 네트워크의 Smart Sensor가 취합한 전력정보를 전력망과 정보통신망이 융합되어 구성된 네트워크망을 통해서 단위 네트워크 형태의 Ethernet 또는 그 이상의 정보 전송 경로인 CDMA, AP, GSM, BPL, WiFi, WiMax, PLC, RFID 등을 통해서 Concentration Center에 보낸다. 융합된 정보통신망은 제3자가 가장 많은 공격을 감행하는 공격의 주된 대상이 된다. DoS, DDoS, Sniffing, Spoofing, Hijacking(session) 이 공격이 발생한다.

- CC(Concentration Center)

CC는 전력 사용정보를 중앙 집중화로 전체 전력망 관리와 운영을 통해 전력 사용량 등과 같은 개인의 정보를 기반으로 과금 등의 최종 리포팅과 모니터링을 한다. Smart Grid의 경우는 중앙에서 전력망을 관리하고 특화되어진 서비스인 전력에 대한 소비자의 관리와 운영이 불가능함으로 중앙에 집중하는 형태를 요구한다. 중앙에 집중되므로 제 3자의 불법적인 접근의 가장 큰 최종 공격 대상이다[6].

3.4 U-Healthcare 보안 위협요소

u-Healthcare 환경에서는 다양한 보안 취약점과 위협요소들이 존재한다. 표 7과 같이 다양한 네트워크 환경에서 유무선 네트워크 기반 서비스에서 발생 가능한 보안 상취약점이 유사하게 전이되는 형태를 가지고 있다. 의료서비스는 정확한 진료를 받기 위해서 환자의 생체 정보를 포함한 개인의 질병 내력, 가족력, 신체적 특징 등의 개인 의료 정보에 대해 충분히 제공해야 한다. 환자 정보는 환자가 진료 목적에 따라 이동하므로 중복된 검사와 의료 조치가 반복되는 것을 막아야 한다.

이질적 의료 도메인 간 개인의 건강/의료 정보를 교환시, 인증된 도메인 간에 안전하게 가용한 정보만을 송수신하도록 지원할 수 있는 보안 기술이 필요하다.

[표 7] U-Healthcare 보안 위협 유형

구분	공격유형
원격검진	DoS, 불법접근, 도청, 프라이버시 침해, 메시지 위변조, 바이러스 공격
이동시	단말분실, 불법접근, 프라이버시 침해, 바이러스 공격, 서비스 방해
게이트웨이	DoS, 불법접근, 도청, 프라이버시 챔해, 메시지 위변조, Replay 공격, 위장

u-Healthcare 환경이 되면서 종래의ID/PWD나 공인인증서 기반뿐 아니라, 다양한 생체 식별 정보가 사용자 인증 방식으로 활용된다. 생체 인식/인증에 사용되는 고유한 식별값을 갖는 생체 정보는 그 정보의 변경이 쉽지 않으므로 생체정보의 노출로 더 이상 사용이 불가능한 경우에 대한 대비책이 있어야 한다. 또한 신체 손상으로 생체정보의 제공이 불가능한 경우에 대한 대체 수단의 제공 방법이 마련되어야 한다. 사용자 식별에 널리 사용

되어지고 있는 주민등록번호는 그 생성 특성상 번호만으로도 개인 정보 노출이 쉬어, 주민번호생성과 유출이 용이하다.

u-Healthcare 서비스를 구성하는 시스템 및 응용 서비스에 대한 안전성 평가는 매우 중요하다. 하드웨어 장비뿐 아니라 소프트웨어 솔루션과 관리적 측면의 정책도 포함한다. 의료 시스템의 특성을 반영한 의료 시스템의 보안 관리 기준은 많이 부족하다. 환자의 건강상태 및 생명 위협 영향을 기준으로 재검토된 의료 시스템의 안전성과 보안 평가 기준이 마련되어야 한다. u-Healthcare 서비스 구축시 정보 공유를 위한 상호호환성 보장을 포함한 보안 및 프라이버시 이슈에대한 고려가 필요하다.

4. IT 융합 보안위협 대응 방향

IT 융합 환경은 기계와 장치간의 통신 위주에서 발생하는 위협이 존재하고 있다. IT 융합에서는 인공지능과 임베디드 시스템을 통한 자동 인식 등의 기법이 연구 개발이 이뤄지고 있다. 기계 및 장치의 위치와 주변 정보 등을 감지하고 실시간 다양한 정보와 주변 상황에 대해 사용자가 신경 써야 할 것들을 기계나 장비가 알아서 자동적으로 작동하도록 프로그래밍 된다. 그러므로 임베디드 시스템 소프트웨어에 대한 보안이 뒤바침이 되지 않는다면 사고의 위험에 더욱더 증가할 것이다.

기계 및 장치 사용시에 사고가 발생하였을 경우 유리한 증거나 주변상황에 대한 정보가 중요한 판단 요소로 작용할 것이다. 주변 정보에 대한 조작 등은 다양한 법률에 위배되는 행위가 많이 이뤄 질 것이다. 주변 정보에 기록된 내용이 법적 증거 능력을 갖추기에 충분하다. 포렌식 기법을 통해 범죄의 사전 예방 및 범죄의 법적 증거 자료로서 개인의 정보보호를 보존할 수 있는 기법의 제공이 필요하다.

기계 및 장비의 정당한 소유자로서의 인증을 위한 생체인식 정보나 스마트키 인증 등을 통한 사용자 인증이 필요하다. 또한 자신의 신원을 밝히고 인증을 받는 일반적인 인증과 달리 기계나 장비 간에 주고받는 정보의 안전한 메시지의 인증은 프라이버시 보호를 위해 사용자의 신원을 드러내지 않으면서 메시지를 인증하며 신뢰성 있게 통신하기 위해서는 복잡하고 까다로운 요구조건을 만족시켜야 하는 어려움이 있어 이에 대한 효율성을 높일 수 있는 연구개발이 필요하다.

보안 요소가 첨가된 새로운 인증 모듈을 통해 모바일이나 PC에서도 장비나 기기에 대한 정보 상태를 볼 수 있도록 하고, 장비를 제어 할 수 있는 개인정보 유출을 방지하는 안전한 인증 모듈의 연구가 필요하다.

키관리에서는 공개키 암호기법의 우수성을 이용하여 각 네트워크 라우팅 정보와 데이터 트래픽에 대한 정보를 보호해야 한다. 기계 및 장치간에 그룹을 만들 수 있는 Cluster 기반으로 구성하여 Cluster 키를 통한 모든 클러스터 내에 위치한 기기에 대해 유일하게 존재하고 클러스터에 속하는 모든 이동 기기에게 분배한다. 이 키는 Cluster 내에 각 자동차들을 인증해주는 Cluster Head(CH) 에 의해 생성되어 시스템 공개키로 암호화되고 클러스터 멤버에게 분배된다. 각 이동 기기는 공개/개인키 쌍을 가지고 있으며, 키 관리를 위한 CA(Certification Authority)를 두어 키의 바인딩과 주기적인 갱신을 담당하도록 한다. CA는 공개/비밀 키 쌍을 가지고 있으며, 공개키는 다른 모든 기기에게 분배되고, 비밀키를 가지고 인증서를 서명 분배한다. 어떤 한 이동 기기가 더 이상 신뢰할 수 없거나 네트워크 영역을 벗어나게 되면 그 기기의 공개키는 폐지한다.

5. 결론

IT분야는 유비쿼터스 환경으로 빠르게 변화가 진행되고 있으며, 여러 산업분야와의 연계를 통해 연구개발이 활발히 진행 중이다. 이러한 산업계간의 연구를 통해 여러 분야의 산업에 융합된 새로운 제품군과 다양한 서비스가 나오고 있지만, 새로운 환경에 대한 보안의 위협요소는 더욱더 많아지고 있다. IT 융합에서 현재 가장 많이 활성화가 되고 산업간의 융합이 활발하게 이루어지고 있는 분야로 장치와 기계간의 통신을 위한 M2M (Machine to Machine)과 IT기술과 의료기술의 융합인 U-Healthcare, IT 기반의 송.변전, 배전 운영을 위한 Smart Grid 그리고 IT 기술이 자동차와 연계한 지능형 자동차 등 많은 분야에서 융합에 대한 내용을 살펴보았고, 그에 따른 새로운 보안 위협요소들을 분석하였다. 분석된 보안 위협요소를 통해 IT기반의 융합에서 공통적으로 대응할 수 있는 방향으로 임베디드 시스템 보안과 포렌식 보안, 사용자 및 기기 인증, 키관리의 향후 전개 방향에 대해서 제안하였다.

참 고 문 헌

[1] 김형준, “사물간 통신 네트워크의 이해”, 한국통신학회지, 제27권 제7호, pp. 21~28, 2010년, 6월

[2] 이근호, “M2M(Machine to Machine)통신에서의 보안 위협 분석”, 한국산학기술학회 2010년도 춘계학술발표논문집, 제11권, 제1호, pp. 416-419, 5월, 2010년.

[3] 최병철, 한승완, 정병호, 김정녀, “지능형 차량 보안 기술동향”, 전자통신동향분석 제22권 제1호, pp.114-118, 2007년, 2월.

[4] 윤필하, 이소희, 최호식, 이근호, 김수균, “M2M 발전에 따른 자동차보안 문제와 연구의 필요성”, 한국지식정보기술학회 2010년도 추계학술발표대회 논문집. 제5권,제2호, pp. 41-43, 2010년, 11월.

[5] 도윤미, 김선진, 허태욱, 박노성, 김현학, 홍승기, 서정해, 전종암, “스마트 그리드 기술 동향:전력망과 정보통신의 융합기술”, 전자통신동향분석, 제24권,제5호, pp.74~86, 2009년 10월.

[6] 서우석, 전문석, “스마트그리드 전력망과 정보통신망 융합 보안 방향”,한국전자통신학회논문지 제5권, 제5호, pp.477~486, 10월, 2010년.

[7] 김명남, 박희준, 권기룡, “u-헬스케어 서비스의 동향”, 한국멀티미디어학회지, 제13권,제2호, pp.1~9, 2009년, 6월.

[8] 송지은, 김신효, 정명애, 정교일, “u-헬스케어 보안 이슈 및 기술 동향”, 전자통신동향분석 제22권, 제1호, pp.119~129, 2월, 2007년.

[9] CERP-IoT(Cluster of European Research Projects on the Internet of Things), "Vision and Challenges for Realising the Internet of Things", 2010

[10] 김정덕, 김건우, 이용덕, “융합보안의 개념 정립과 접근 방법”, 정보보호학회지 제19권, 제6호, pp.68~73, 12월, 2009년

저 자 소 개

이 근 호(Keun-Ho Lee) **[종신회원]**

- 2006년 8월 : 고려대학교 컴퓨터학과 (이학박사)
- 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
- 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 전임강사
- 2010년 9월 ~ 현재 : 백석대학교 쿰인성개발원 팀장

<관심분야> : M2M 보안, 이동통신 보안, 융합 보안, 개인정보보호