USN 활성화를 위한 정보보호 요구사항

한국정보보호진흥원 이응용, 박광진

차 례

요 약

향후 도래할 유비쿼터스 환경에서 USN(Ubiquitous Sensor Network)은 홈네트워크, 텔레매틱스, RFID 서비스 등의 기본 인프라를 형성할 것이다. 무선망 기반의 USN은 다양한 정보보호 취약성을 내재하고 있어, USN 기반으로 제공되는 지능화 서비스에서 이용자들이 경험하는 위협은 현재의 정보화 역기능보다 훨씬 심각하게 대두될 것으로 우려된다. 미래에는 실생활에 관련된 위협이 증가하면서 이용자들이 보안 및 프라이버시 이슈에 대해 더욱 민감해 질 것이다. 그러므로 이러한 이용자들에 보안 및 프라이버시에 대한 만족할 만한 수준의 제도적, 기술적 대안을 제시하지 못하면 USN의 활용화가 지연되고 관련 서비스의 확산 자체가 무산될 가능성도 배제할 수 없다. 따라서 USN이 사회기반 인프라로 뿌리내리기 위해서는 이용자 보호를 위한 적절한 정보보호 대응마련이 필수적인 요건이라 할 수 있다.

이에 본 연구에서는 USN의 적용확산으로 발생할 있는 정보보호 위협요소를 분석해보고, 이에 대한 핵심적인 정보보호 요구사항을 도출하고자 한다.

Ⅰ. 서 론

20세기 후반 시작된 IT혁명은 우리 사회의 모습을 획기적으로 바꿔 놓았다. USN 기반으로 실현되고 유비쿼터스 혁명으로 인해 우리사회의 삶은 더욱 많은 변화가 예상된다. 유비쿼터스 컴퓨팅은 언제 어디서나, 모두가 컴퓨터를 사용할 수 있는 환경을 의미한다. 유비쿼터스 혁명이 진행

됨에 따라 우리 삶 전체에 걸쳐 혁명이 시작되며 우리 삶의 모습은 기존과는 전혀 다르게 바뀔 것으로 예상된다. 예를 들어 홈네트워크 환경이 구축되면 정보가전이 네트워크로 연결되어, 언제 어디서나 무선으로 정보가전을 작동할 수 있고, 가정의 각종 센서들은 환경을 측정해서 자동으로 습도, 온도 등을 조절할 수 있을 것이다. 광대역 융합망이 구축되고, 차세대 이동통신이 확산되면 언제, 어디서나 양질의 디지털 콘텐츠 서비스를 고속으로 받을 수 있게 될 것이다. 또한 RFID의 확산으로 개인별 맞춤형 서비스를 제공받는 것이 가능해지며 이를 바탕으로 다양한 신규 유비쿼터스 비즈니스가 출현할 것으로 예상된다.

USN 인프라 및 서비스는 유비쿼터스 사회가 지향하는 지능화되고, 윤택한 삶을 추구할 수 있도록 지원하겠지만, 이전에 경험하지 못한 더욱 심각한 사회경제적 역기능을 유발할 수 있다. 다양한 휴대 정보기기를 이용한 정보수집 및 유출 위험, 정보기기의 오작동으로 인한 현실세계의 위험, RFID 활용증가로 인한 개인의 프라이버스 침해 등 각종 정보화 역기능들이 더욱 광범위하고 심각한 위협으로 다가올 수 있다. 이에 따라 USN 구축초기에 정보보호 위협을 예측하여 사전적으로 대응하는 것이 필요하다. 이에 본 연구는 UNS 적용이 확산되면서 증가하게 될 정보보호 위협요소들을 분석하고, 위협에 대응하기 위한 기술적, 법제도적, 문화적 측면의 정보보호 요구사항을 제시하고자 한다.

Ⅱ. USN의 정보보호 위협요소

USN은 센서 및 기기가 주위환경에서 정보를 수집하고 무선 네트워크를 통해서 정보를 전달한다. 유선환경과 마찬가지로 정보보호의 요소인 기밀성, 무결성, 가용성은 USN 정보보호에서 중요한 위치를 차지한다. 그러나 USN은 무선 인프라를 기반으로 서비스를 제공하면서 정보보호 대상이 HWW, P2P, Ad-Hoc 네트워크, RFID 등으로 지속적으로 확대된다. 또한 이용자의 정보보호에 대한 요구수준이 증가하면서 시스템과 네트워크에 대한 정보보호 뿐만아니라 USN 서비스의 안전 및 신뢰성 등이 요구된다.

1. HWW 디바이스의 위협요소

USN 환경에서는 다양한 무선휴대기기인 HWW(HandHeld and Wearable Wireless)의 사용이 증가한다. 이러한 HWW는 소형 및 이동성으로 인해서 다양한 제약요인이 발생한다. 즉 PC는 전력을 공급받는 환경에서 사용되나 HWW는 지속적으로 전력을 공급받지 못하는 상황이 발생한다. 저용량의 RAM, 저속 프로세서, 저장장치의 부재로 인한 하드웨어 제약을 수반하며, 무선통신의 전송범위가 기술적인 요인으로 인해 제한적이다. 또한 디바이스의 잦은 이동으로 인해 일시적인(Transient) 통신이 발생하여 네트워크는 빈번한 통신장애를 경험할 수 있다. 이와 같은 HWW의 제약요인으로 인해 다양한 정보보호 이슈가 발생한다.

첫째, HWW는 기밀성 손상위험이 높다. 유선환경에서는 공개키 기반의 암호방식(Public Key Cryptography)을 사용한다. 하지만 HWW 환경에서는 디바이스의 계산능력의 한계로 실효성이 낮고, 암호화에 필요한 계산은 전력소모 제약요인을 가중시킬 수 있다. 이로 인해 HWW를 사용하는 컴퓨팅 환경에서는 상호간에 비밀키를 교환하는 대칭키방식의 암호화(Symmetric Cryptography) 방식의 사용이 요구된다.

둘째, HWW는 유선환경에 비해서 접근통제가 어렵다. HWW의 이동성으로 인해 네트워크에 연결된 수많은 접근통제 채널에 대하여 분산통제를 하기 때문에 중앙집중식으로 통제하는 유선환

경에 비해서 공격위협의 노출이 심화될 수 있다.

셋째 HWW는 시스템 보안의 유지가 어렵다. HWW 디바이스가 직접통신 범위를 벗어난 범위의 디바이스와 통신하는 경우에 시스템 보안이 주요위협으로 대두될 수 있다. 통신경로의 길이가 증가하면 Man-in-the-middle과 같은 공격위협 가능성이 증가한다. HWW 디바이스에 탑재한 응용시스템은 디바이스의 계산능력의 한계 및 저장 공간의 제한으로 인해 Runtime Bound 검사와 같은 검사기능의 부재로 버퍼 오버 플로우 공격 등에 노출될 수 있다.

2. Ad-Hoc Network 위협요소

Bluetooth와 같은 무선전파기술의 발전으로 Ad-Hoc 네트워크라 불리는 새로운 개념의 네트워크 방식이 출연하였다. Ad-Hoc 네트워크는 무선 이용자들이 통신을 위해 공통의 무선전파 범위에서 네트워크 위상을 설정하는데 참여한다. Ad-Hoc 네트워크안의 노드들은 직접 무선 링크 및 Multihop 라우팅을 통해서 무선전파 범위내의 다른 노드와 통신한다. Ah-Hoc 무선 네트워크는 정의된 기반구조가 없으며, 모든 네트워크 서비스가 임기응변식으로 생성된다. 그러므로 기반구조의 지원이 부족하고, 무선접근 공격에 노출되기 쉬운 취약점을 내재하고 있다. Ad-Hoc 네트워크 위상은 노드의 이동성으로 인해 매우 동적이고, 노드의 멤버쉽이 무작위로 빠르게 변화하여 동적인 보안 솔루션이 요구된다.

Ad-Hoc 네트워크에서 도청, 위·변조, DoS 공격 등이 용이하다. Ad-Hoc 네트워크는 특정한 악성 노드 및 거짓행위 노드가 다른 노드의 서비스를 방해할 수 있다. 방화벽이나 접근통제시스템의 부재로 Ad-Hoc 네트워크의 노드들은 다른 노드로부터 접근해오는 공격에 매우 취약하다. 노드의 아이덴티티 위조, 기밀정보 유출 등이 가능하다. Ad-Hoc 네트워크가 지원하는 라우팅 프로토콜은 각각의 디바이스가 릴레이처럼 사용되기 때문에 공격에 더욱 취약하다. 라우팅 정보의 변조는 전체 네트워크를 손상시킬 수 있다. 또한 손상된 노드는 다른 노드에 악성정보를 퍼트리고, 이로 인해 심각한 위험을 초래할 수 있다. 이런 유형의 공격으로 기밀성, 무결성, 가용성, 프라이버시와 같은 기본적인 정보보호 특성이 쉽게 손상될 수 있다.

3. P2P 활용증가로 인한 위험요소

USN 네트워크에서는 다양한 센서, 기기들이 지능화되고, 전자거래의 주체로 등장하면서, 사람과 사람과의 P2P, 기기와 기기간의 M2M(Machine-To-Machine) 등 다양한 상호작용이 발생한다. P2P는 편리함으로 인해 사용이 점차로 증가되고, 미래에는 모든 사물에 컴퓨팅이 내장되면서 미래의 컴퓨팅 환경의 중심으로 자리잡아 갈 것이다. 반면 P2P 시스템은 기술적·사회적 측면의 다양한 이슈를 양산할 수 있다.

첫째, P2P를 이용한 바이러스 감염정보의 유포위험이 증가한다. 이용자가 P2P 시스템을 통해서 불필요한 정보를 검색하거나, 바이러스 감염정보를 자신의 컴퓨터에 다운로드하여 실행하게 되면 바이러스의 유포가 빠르게 확산될 수 있다. 특히 P2P 프로그램은 불필요한 정보자원접근을 가능하게 하여 컴퓨터에 백도어를 제공하는 수단으로도 이용될 수 있다.

둘째, P2P에 사용되는 데이터의 분산화로 인해 데이터 무결성 손상의 위험이 존재한다. P2P 시스템에는 동일한 데이터를 많은 사람이 중복적으로 사용하여, 데이터의 변경 및 갱신이 발생하면서 P2P 정보의 무결성 손상 위험이 높아진다.

셋째, 디지털저작권 침해가 확산될 수 있다. P2P 시스템의 정보검색 및 교환의 편리성과 인터넷 고속화가 진행되어 P2P 시스템을 활용한 인터넷 저작권 침해가 빠르게 증가할 수 있다. Sy

mantec은 전세계에서 현재 사용하고 있는 자사의 백신프로그램의 약 50%가 인터넷을 통한 불법 복사본으로 추정하고 있으며, Business Software Alliance는 전세계에서 소프트웨어 저작권 침해로 인한 손실규모를 130억 달러 규모로 추정하고 있다. 최근 Business Software Alliance의 소프트웨어 Piracy 실험에서도 P2P 시스템에서 Microsoft의 Office XP, Adobe의 GoLive 등의 프로그램을 빠르게 찾을 수 있었다.

넷째, P2P를 이용한 시스템의 신뢰성 확보의 어려움이 존재한다. 전자상거래는 여러 계층으로 구성된 인증기관 및 전자서명을 사용하여 거래의 신뢰성을 확보하고 있다. 그렇지만 P2P시스템은 단일계층에서 단말기간의 직접통신 방식이므로 다계층의 인증기관 및 전자서명 적용을 통한 사용자간의 신뢰성 확보에 애로점이 존재한다.

4. RFID(Radio Frequency Identification)를 이용한 서비스의 프라이버시 침해 위험

산업계는 유비쿼터스 환경의 핵심적인 기술로 인식되는 RFID의 신속한 도입을 추진하고 있다. 특히 유통업계는 RFID 부착제품이 센서를 통과하는 즉시 구입물품 명세, 가격, 유통경로 등이 즉석에 파악할 수 있기 때문에 재고관리 및 도난방지를 위해 RFID 도입을 적극 추진하고 있다. IT업계는 기업들의 효율적인 물류망 구축 및 재고관리 수단으로 급부상한 RFID 시장을 선점하기 위해 제품을 다수 출시하고 있다.

반면 RFID를 이용한 개인정보의 수집 및 이용이 증가하면서 개인정보의 오·남용으로 인한 프라이버시 침해위협이 유비쿼터스 환경에 대한 두려움을 생성하는 중대요소로 작용하고 있다. 전세계 네트워크와 RFID 리더가 연결되면 RFID 부착제품의 소지자가 인식하지 못하는 사이 자신의 행위, 위치, 구매패턴 등의 추적이 가능해져, 개인행위의 익명성이 심각하게 저해될 수 있다. 또한 정부조직이 시민행위를 감독 및 감시하기 위해 수집정보를 사용하거나, 해커나 범죄자가 불법적으로 수집정보를 사용할 가능성이 있다. RFID의 프라이버시 침해위험에 대하여 미국의 캘리포니아 주의회는 RFID의 프라이버시 침해위험 관련 청문회를 개최한 바 있다. 또한 소비자단체들은 RFID 기술이 사람, 제품, 현금의 추적에 사용되어 개인의 프라이버시 침해위험이 매우 높음을 지적하며, 산업계의 RFID 도입에 강력히 반대하고 있는 상황이다.

RFID의 활용으로 인한 프라이버시 침해위험과 시민사회의 반응에 대한 유통업계 및 물류업계의 사례를 살펴본다. 유통업계는 제품추적을 위해 RFID 사용하려 하고 있다. 세계 최대 유통업체 월마트는 지난 월마트 매장에서 RFID 기술을 이용하여 판매현황 및 절도피해 등을 실시간 파악하는 매장관리시스템을 시험할 계획이라고 발표한 바 있다. 그러나 소비자 단체의 프라이버시 침해우려 등을 강하게 주장하면서 시험계획을 취소하였다. 그렇지만 월마트는 RFID를 이용한 매장관리를 포기한 후, 재고 및 물류관리만을 위해 주요 100개 공급자에게 2005년까지 RFID를 부착한 제품을 공급하도록 지침을 전달함으로써, RFID 활용 의지를 버리지 않고 있다.

의료업계에서는 제품추적을 위해 RFID를 사용하려 한다. 의류업체인 베네통(Benetton)은 RFID 태그를 제품에 부착하여 고객이름과 신용카드 번호를 의류의 일련번호에 연결시켜 고객의 쇼핑 습관정보를 수집하고자 하였다. 그러나 베네통은 CASPIN(Consumer Against Supermarket Privacy Invation and Numbering)과 같은 프라이버시 단체의 강력한 반대에 직면하여 의류의 RFID 태그 부착을 유보한 바 있다. 현재 CASPIN은 수퍼마켓 프라이버시 침해 대책 소비자 연

합인 민간조직으로 고객의 프라이버시 보호를 위해 유통업자의 고객감시계획을 반대하고 있으며, RFID 프라이버시 침해위협에 대한 지속적인 모니터링 및 시민 홍보를 수행하고 있다.

5. ID Theft 및 디지털저작권 침해

유비쿼터스 환경에서는 RFID 태그를 부착한 사물, 기기 등이 USN으로 연결되어, 기기를 주체로 정보의 상호교환 및 전자거래가 급격히 증가할 것으로 예상된다. 전자거래의 주체인 사물, 기기들은 각각 고유의 ID로 상호작용을 한다. 다른 사람 및 기기의 ID를 도용하여 전자거래 및 상호작용을 수행하는 ID Theft가 현재보다 더욱 심각한 사회문제를 확대될 것이다. ID Theft는 프라이버시 침해뿐만 아니라 타인에게 심각한 경제적인 손실을 가할 수 있다. 이는 Off-line에서 타인의 통장번호와 패스워드를 훔쳐서 타인의 계좌에서 돈을 인출하는 것과 유사하다. 그러므로 다양한 기기가 제공하는 정보의 정확성을 확인하고, 불법적인 정보유출을 방지하기 위한 신뢰성 있는 기기인증이 필요하다. 기기인증은 개별 또는 인터넷을 포함하여 유무선 네트워크에 연결된 기기가 실제로 등록된 바로 그 기기인지를 확인한다. ID Theft를 방지하기 위한 법률적 노력도 요구된다.

또한 다양한 전자거래 주체가 제공하는 서비스의 신뢰성을 확보하기 위해 자격, 권한 등 디지털저작권에 대한 증명이 필요하다. 공인인증서 등을 이용한 일반적인 이용자 인증은 이용자의 신원확인 기능만을 제공하고 있어 디지털저작권 보호기능을 제공하지 못한다. 디지털컨텐츠의 활용이 증가하고, 다양한 거래주체들이 디지털컨텐츠를 생성하고 유통하는 환경에서는 디지털저작권에 대한 분쟁사례가 증가할 것으로 예상되므로, 이에 대한 효율적인 대처방안이 필요하다. 또한 전자거래 규모가 커지고, 횟수도 빈번해지면서 거래내역, 로그 등 보존해야 하는 증거기록도 급격하게 증가하여 거래증명을 위한 효율적 관리체계가 요구된다.

6. 사이버 위협이 현실세계의 사람의 안전과 생명을 위협

유비쿼터스 사회에서 일상생활의 모든 정보기기들이 상호연결되면 사이버 위협이 현실세계로 전이 될 가능성이 더욱 높아진다. USN를 기반으로 제공되는 다양한 서비스에서 유사한 문제점이 발생할 것으로 예상되므로, 본고에는 미래의 이용자가 텔레매틱스 서비스에서 경험하는 위협을 중심으로 미래의 안전위협을 살펴본다. 텔레매틱스는 자동차에 통신장치를 부착하고, 자동차의 부품에 센서를 부착하여 정보서비스, 안전서비스, 교통정보서비스 등을 제공한다.

운전자는 시속 70KM로 달리면서 운전석에 앉아 있다. 운전자는 차량을 길 모퉁이로 돌린다. 차를 회전하기 위해 전체 도로상태, 차량 주변환경, 차량내 장비상태 정보를 살펴본다. 차량내 응용시스템은 카메라 센서, 차량내 교신시스템, 전자지도, 위치추적 위성, 도로통신기지국, 다른 차량으로부터 지속적으로 정보를 수집한다. 차량내 통제 장비는 센서로부터 획득한 정보를 검증, 통합, 분석, 처리하여 운전자에게 정보를 제공한다.

운전자가 가려고 하는 길 모퉁이에 사고가 발생하였고, 운전자는 아직 이를 인식하지 못하는 상황이 발생한다. 지능화된 안전시스템인 ADAS는 차량이 직면한 위험을 감지하고 운전자에게 음성으로 경고한다. 운전자는 차량의 통제를 받으면서, 차량의 경고신호 및 능동적인 지원을 받지만 독자적으로 행동할 수 있음을 항상 인식하고 있다. 운전자는 시스템의 경고에 따라 차량속도를

줄이고, 사고위치에 도달하기 전에 안전하게 차를 멈출 수 있었다. 그리고 뒤에 오는 다른 차들에게 즉시 경고 메시지를 전송한다.

운전자는 위험상황에 대처할 수 있는 정교한 안전시스템을 차에 장착하고 있음을 알고 있다. 위험의 중대성 및 시급성에 따라 시스템은 자신에게 상황을 알리고, 경고하며, 능동적으로 도와서 위험을 피할 수 있도록 돕는다. 시스템의 개입이 사고를 완전히 해결하지 못하는 경우에, 지능적이지만 수동적인 안전 응용시스템이 운전자 및 상대방의 안전을 보호하기 위해 최선의 방법을 취한다. 시스템은 또한 자동적으로 사고의 심각성 및 위치를 표시하는 비상시스템에게 제공한다.

※ ADAS(Advanced Driver Assistance Systems: 운전지원시스템): 차량외부로부터 정보를 획득하여 시스템의 사고발생 위험을 감지하여 운전자에게 경고하여 적절한 행동을 취할 수 있도록 지원. 운전자가 사고를 피할 수 없는 상황에서는 기존의 수동적인 안전시스템을 최적으로 활용할 수 있도록 정보를 제공한다.

위에서 텔레매틱스 서비스를 이용했을 때 제공하는 다양한 안전서비스를 시나리오를 통해서 살펴보았다. 이러한 안전서비스는 사람의 안전과 생명을 위협하는 요소로 작용할 수 있다. 텔레매틱스는 이동통신망 및 이동기기 등 무선환경으로 인한 취약성이 내재하고 있다. 보안취약성을 이용하여 무선네트워크에 유통되는 위치정보, 교통정보를 위변조하거나, 전송이 지연되면 다양한 현실세계의 위험이 가능하다. 즉 운전자의 안전과 관련된 긴급구난 정보의 전송오류 및 지연이 발생하면, 운전자는 적시에 안전서비스를 제공받을 수 없게 된다. 또한 공격자가 텔레매틱스 네트워크에 침투하여 오류 교통상황정보를 유포하면 일부지역에 교통체증을 유발할 수 있고, 텔레매틱스에서 위치파악을 위해서 사용하는 GPS 시스템의 장애가 발생하면 운전자는 도로에서 잘못된 경로로 운전할 수 있다.

Ⅲ. USN 환경의 정보보호 요구사항

이 장에서는 앞에서 지적한 정보보호 위협 요소에 대응하여 필요한 기술적, 법제도적, 문화적 측면의 요구사항을 제시하고자 한다.

1. UNS 무선인프라 보호를 위한 기술적 요구사항

USN의 인프라의 안전한 이용을 위해서 다양한 기술적인 요구사항이 필요하다. 정보보호의 기본특성이 기밀성, 무결성, 가용성, 인증 측면에서 살펴보고, USN의 고유한 특성인 최신성 측면에서 고려하여 본다.

첫째, USN에서 유통하는 정보의 기밀성 보호가 필요하다. USN은 근접한 다른 네트워크에 센서탐지를 노출시키지 말아야 한다. 많은 애플리케이션(예, 키분배)에서 단말노드는 매우 민감한 정보를 교환한다. 정보의 기밀성 보호를 위한 가장 일반적인 방법이 암호화이다. 암호키는 단지 목적하는 수신자만이 알 수 있도록 함으로써 기밀성을 유지한다. 교환 패턴이 노출될 수 있는 상황에서는 단말노드와 다른 노드와 안전 채널이 필요하다.

둘째, USN에서 유통하는 메시지의 원천을 확인하기 위한 인증이 필요하다. USN에서 공격자가 무선환경의 취약성을 활용하여 쉽게 메시지를 삽입할 있으므로, 수신자는 의사결정과정에 사용하는 데이터의 원천소스를 확인할 필요가 있다. 이때, 메시지 인증은 수신자에게 수신한 데이터

가 의도한 송신자로부터 왔는지를 확인할 수 있도록 한다. 양자간 교환하는 통신에서는 데이터 인증은 단순한 대칭 메커니즘을 사용함으로써 가능하다. 송신자와 수신자가 모든 통신 데이터의 MAC(Message Authentication Code)를 계산함으로써 비밀키를 공유한다.

이런 유형의 인증은 네트워크에서의 매우 강력한 신뢰를 가정하지 않는다면 브로드캐스트(Broadcast)에는 적용되기 어렵다. 한 송신자가 인증된 데이터를 상호신뢰가 부족한 수신자에게 전달하는 경우에 대칭적인 MAC의 사용은 안전하지 못하다. 특정한 수신자가 MAC 키를 알게 된다면 메시지를 변조해서 다른 사람에게 보낼 수 있다. 그러므로 브로드캐스트 방식의 인증을 위해서는 비대칭적 메카니즘이 필요하다.

셋째, USN에서 유통하는 정보의 변조를 방조하기 위해 데이터 무결성 보호를 위한 기술이 요구된다. 통신에서 데이터의 무결성은 수신자가 수신한 데이터가 전송도중에 변조되지 않았음을 보장한다. 데이터의 무결성은 데이터의 인증을 통해서 가능하다.

넷째, USN에서 데이터의 최신성 보장이 필요하다. USN에서 시간의 변화에 따른 다양한 형태의 정보를 교환하게 되면, 데이터의 기밀성과 인증만으로 충분하지 못하다. 각각의 메시지가 최신(fresh)임을 보장해야 한다. 데이터의 최신성은 데이터가 최근에 만들어져서 공격자가 이전(Old) 메시지로 교체하지 않았음을 의미한다.

다섯째 USN 서비스의 가용성 확보가 필요하다. 센서 네트워크는 센서노드의 불필요한 계산(예, 키관리메시지 계산 및 처리 등)으로부터 보호하여 전력소모를 최소화하고, 센서네트워크의 생명을 최대한 연장해야 한다. 모든 네트워크의 가용성 유지를 위해 중앙의 키관리 노드와 같은 중요지점이 장애를 초래하지 않도록 보호하는 것이 매우 중요하다. 센서네트워크를 가용성을 저해하지 않는 수준의 보안 요구사항이 필요하다.

2. USN 서비스 보호를 위한 기술적 요구사항

복잡하고 고도화된 기능을 제공하는 USN 서비스의 안전성 확보를 위해서는 사람의 안전과 관련된 텔레매틱스, 홈네트워크 등에 사용되는 정보기기의 안전성 확보가 우선되어야 한다. 또한 기밀성 보장이 어려운 무선환경에 필요한 안전한 정보유통 경로를 확보해야 한다.

먼저 유비쿼터스 환경의 안전성 확보를 위해 새로운 정보기기 제작단계부터 안전성을 확보할 수 있는 안전기준을 마련해야 하며 블루투스나 WPAN 등 다양한 네트워크망에서 사용될 수 있는 보안프레임워크의 적용도 검토해 볼 수 있다. 개별 기기의 문제뿐 아니라 운영과정에서 나타날 수 있는 장애를 방지하기 위해 유비쿼터스 응용서비스 BCP(Business Continuity Planning) 체계 구축도 병행되어야 한다.

또한 정보기기로 인한 침해사고가 발생했을 때 스스로 위험을 인식하고 이를 능동적으로 대응할 수 있는 기술개발도 중요한 문제이다. 그리고 이러한 보안기술에 대한 표준화가 필요하다.

다음은 안전한 정보유통경로를 확보하기 위해 다양한 이동정보기기에 적용가능한 경량의 암호기술을 개발하여 적용해야 한다. '스마트 먼지'와 같은 초미립 센서들이 가지고 있는 무선통신 기능과 프로세싱 기술에 적용될 수 있는 초경량 암호 기술의 개발은 최근 보안기술 전문가들의 관심분야이다. 이종기기나 다양한 응용 서비스 상호간의 운용성을 보장하는 동시에 디지털컨텐츠의 불법유통을 방지할 수 있는 보안기술을 탑재하도록 하고, 탑재된 디지털컨테츠 보호기술의 안전성을 검증할 수 있는 기준이나 체계마련이 필요하다.

USN 환경은 사람 · 사물 · 기기가 모두 상호작

용을 함에 따라 서비스제공자, 서비스이용자, 서비스관리자에 대한 구분이 모호해 질 수 있다. 이를 초기부터 체계적으로 관리하기 위해서는 USN 구축에 참여하는 이해당사자가 모여 협의를 할 수 있는 USN 시큐리티 포럼 운영이 효과적일 수 있다. 이를 통해 기술개발 및 발전에 맞추어 기술에 대한 진보적인 의견수렴과 당사자들의 적극적인 의견개진이 가능하다.

3. USN 보호를 위한 법제도 측면의 요구사항

USN으로 대표되는 미래의 지능기반사회는 유연한 사회구조를 형성하고 사회가치가 다원화된다. 더욱이 IT 기술은 변화되는 사회구조에 맞는 규범이나 제도를 정착시킬 틈도 없이 빠르게 발달한다. 다음에서 법이나 제도가 IT기술에 후행할 수밖에 없는 상황에서 USN의 안전을 확보하기 위한 법제도적 요구사항에 대하여 제시한다.

첫째, USN 인프라 보호를 위한 법 제도적 개선이 필요하다. USN이 구축되면 홈네트워크 등이 현실화되면서 현실세계의 위험이 높아질 것으로 예상된다. 따라서 홈네트워크, 텔레매틱스, 휴대인터넷 등 새롭게 등장하는 환경에 적합하도록 정보통신 기반구조 관련 법안에 대한 정비가 필요하다.

둘째, 통합인증 관련 법안의 정비가 필요하다. USN을 통해 다양한 기기 및 센서들이 전자거래의 주체로 등장하게 된다. 현행 전자서명법은 이용자 신원인증에 관한 사항만을 정의하고 있기 때문에 다양한 거래주체인 기기 및 센서 등에 대한 신원확인, 거래증명 등에 대한 사항을 규정하지 못하고 있다. 이에따라 미래의 다양한 기기 및 센서 인증, ID Theft 처벌규정, 사회공학적 해킹방지 방지 등을 포괄하는 통합인증 관련 법안에 대한 연구가 필요하다.

셋째, 프라이버시보호 관련 법안의 정비가 필요하다. 종합적인 개인정보보호 체계를 정립하기 위해 기존의 공공 및 민간에 기관에 산재한 개인정보보호 관련법안에 대한 정비가 필요하다. 또한 지능기반사회에서는 USN을 통해 위치정보, 생체정보, 의료정보 등 과도한 개인정보가 수집되기 때문에 이러한 정보의 수집 및 유통에 대한 체계적 법률규제가 없으면 개인의 프라이버시 침해 위험이 매우 높게 된다. 따라서 이러한 문제점을 해결하기 위해 개인정보침해 예방 및 대응을 위한 법제도적 연구가 필요하다.

넷째로는 디지털 컨텐츠의 건전한 유통을 위한 디지털저작권 관련 법안의 정비가 필요하다. 디지털TV, 위성 DMB 등 매체의 디지털화가 가속화되고 디지털 콘텐츠의 유통이 증가함에 따라 저작권 보호 및 불법복제가 증가하고 있다. 지능기반사회에서는 기존 방송매체뿐 아니라 무선단말과 인터넷까지 매체가 확대되고 채널이 다양해짐에 따라 한번 제작된 디지털 컨텐츠의 활용범위가 넓어 불법복제 위협은 더욱 높아지고 있다. 지능기반사회에서 우수한 컨텐츠의 제작 및 배급을 촉진하기 위해서는 디지털저작권 보호를 위한 법제도적 연구가 필요하다.

4. USN 보호를 위한 문화적 요구사항

유비쿼터스 시대에 가상사회와 현실세계의 경계가 모호해지는 지능화된 서비스는 기술적 신뢰와 인간적 신뢰라는 이중적 신뢰를 바탕으로 한다. 이러한 이중적 신뢰가 파괴 혹은 손상되는 것이 정보보호의 위협이라면 이러한 위협에 대한 대응책 역시 기술적인 대응으로만 해결하는 것이 아니라 이중적이어야 함을 의미한다. 사이버상의 해킹·바이러스에 대한 기술적인 대응 및 핵심적인 보안기술의 개발 등은 기술적 대응책이고, 개인의 프라이버시 보호를 위한 이용자들 스스로의 자정능력 향상, 인간적 신뢰 구현을 위한 문화적인 대응책이다. 이에 USN 환경의 정보보호를 강

화하기 위한 문화적인 요구사항을 살펴본다.

첫째, 이용자들의 정보보호 실천의식 고취가 필요하다. USN 환경은 현재와는 달리 생활속에 내재된 컴퓨터가(Embedded Computer) 언제나 어디로든 연결되어 있는 환경이다. 이러한 환경에서 이용자의 생활에서 빈번하게 발생가능한 모든 위협을 기술적으로 완벽하게 해결하는 방안은 불가능할 것이며, 이용자 개개인의 정보보호에 대한 의식을 높이고, 정보보호를 실천하는 노력이 요구된다. 최근 미국의 NCSP(National Cyber Security Partnership)fmf 통해 Top10 Cyber Security Tips를 정하여 일반 이용자에게 홍보하고 있으며 우리나라도 '정보보호 실천수칙'을 정하여 홍보를 강화하고 있다.

둘째, USN 환경의 개인정보의 집중화 현상에서 인간기본권을 지키기 위한 개인의 정보통제권에 대한 인식을 강화해야 한다. 종래의 인간의 기본권이 전쟁이나 독재상황하에서 보호받는 권리라는 고전적인 의미였다면 과학기술이 발전하면서 인간권의 기본은 인간복제나 환경문제, 디지털 시대의 프라이버시 문제까지 그 개념을 확장시키고 있다. USN 환경이 구현되면 센서를 통해 수집된 방대한 양의 데이터베이스는 사회적 기간망을 통해 서로 연동·관리됨으로써 개인의 사생활이 위협받고 자칫하면 전자감시사회를 초래할 수 있다. 개인의 민감한 정보를 보호하기 위한 PET(Privacy Enhanced Technology) 기술 등이 개발되고 있으나 이것은 부분적 대책에 지나지 않으며 자신의 정보를 적극적으로 지키기 위한 이용자들의 자기통제권 강화가 필요하다.

셋째, 디지털 컨텐츠의 불법적인 사용을 막아 디지털산업기반을 강화시킬 수 있는 네티즌들의 의식이 강화되어야 한다. 디지털 기술의 발달은 단순히 통신과 방송 미디어 기술분야 뿐만아니라 산업, 소비 전 분야에 걸친 변화를 수반한다. 즉 디지털 컨텐츠가 한번 생산되면 다양한 미디어를 통해 전파될 수 있어 One Source Multi Use의 특성과 복제가 손쉽다는 특성을 지닌다. 디지털 환경에서 디지털 컨텐츠는 가치사슬상 최상위 영역으로 디지털 컨텐츠의 불법복제는 전체 디지털 산업에 영향을 미칠 수 있음을 의미한다. 건전한 디지털 유통환경을 가꾸어 나갈 수 있는지에 대한 네티즌들의 책임과 실천이 필요하다.

Ⅲ. 결 론

USN의 인프라와 서비스가 확대되면 주위의 환경이 개인화된 서비스를 제공하는 지능기반사회가 본격적으로 도래한다. USN의 다양한 서비스의 혜택으로 인해 현세대는 라이프스타일의 획기적인 변화가 예상되는데 이것은 편재한 컴퓨팅 디바이스가 USN를 이용해 지능화된 서비스를 일반인들이 쉽고 편하게 사용할 수 있는 환경이 구축되기 때문이다.

그러나 생활이 편리해진다는 것은, 증가하는 유비쿼터스 위협에 대비하여 준비해야 할 것도 많고, 지켜야 할 것도 많아진다는 의미이다. 안전한 미래사회를 위해서는 IT발전과 더불어 정보보호의 필수적으로 요구되며, 현재보다는 미래에 더욱 중요해진다.

이에 본 연구에서는 USN 환경에서 예상되는 HWW, Ad-Hoc Network, P2P, RFID 보안 및 프라이버시 위협, 디지털 저작권 침해 위협, 사이버위협이 현실세계로 전이하면서 발생하는 안전 위협 등 다양한 측면의 미래위협을 살펴보았다.

또한 이러한 미래위협을 조기에 예측하여 방어하기 위한 정보보호 요구사항을 기술적, 법제도적, 문화적 측면의 요구사항을 살펴보았다. USN 활성화를 위한 기술적, 법제도적, 문화적 측면의 정보보호 요구사항은 상호보완적이기 때문에 세 가지 요소가 충분히 만족할 때 실현될 수 있

을 것이다. 본고에서 제안한 내용들은 USN 활성화를 위한 정보보호 정책방향 수립, 정보보호 기술개발 및 산업육성 전략 마련을 위한 기초자료로 활용될 수 있을 것으로 생각하며, 향후 USN의 다양한 서비스별로 사례연구, 통제방식(Security Governance), 산업육성 방안 등에 대한 추가적인 연구가 필요할 것으로 사료된다.

참 고 문 헌

[1] IST, "A Dependability Roadmap for the information Society in Europe: Part 1-An Insight into the Future", 2003

[2] IST, "Dependability Roadmap for the information Society in Europe: Part 2-Appraisal of related IST Roadmaps", 2003

[3] IST, "A Dependability Roadmap for the information Society in Europe: Part 3-Towards a Dependability Roadmap", 2003

[4] Daniel Keely, "A security strategy for mobile e-business", IBM Security and Privacy Sevices Organization, 2001.

[5] Sastry Duri 외 6인, "Framwork for Security and Privacy in Automotive Telematics"

[6] IST, "Roadmap for Advanced Research in Privacy and Identity Management", 2003

[7] IST, "The European Commission's Road Safety Action Programme", 2003

[8] IST, "Deliverable D41: HNSP Platform Specification, 2003

[9] Pampas, "Pioneering Advanced Mobile Privacy and Security- Deliverable D03: Refined Roadmap, 2003

[10] Pampas, "Pioneering Advanced Mobile Privacy and Security- Deliverable D04: Final Roadmap, 2003

[11] 김정우 외, "Issue Paper:가정의 디지털 혁명, 홈네트워크", SERI, 2003

[12] 김재윤, 민병석I, "유비쿼터스 컴퓨팅:비즈니스 모델과 전망", SERI, 2003

[13] IST, "D1: Comprehensive Survey of Comtemporary P2P Technology", 2003

[14] IST, "Dependable Embedded Systems Raodmaps", 2003

[15] DHS, "National Strategy To Secure Cyberspace", 2003

[16] NCSP, "Awareness for Home Users and Small Business", 2004

[17] NCSP, "Corporate Governance", 2004

[18] 정보통신부, "IPv6 보급 촉진계획(안)", 2003

[19] 정보통신부, "Broadband IT Korea 건설을 위한 광대역통합망 구축 기본계획(안), 2003

[20] 황주성외, "IT의 사회문화적 영향 연구 총괄보고서", 정보통신정책연구원, 2004.

[21] Roberto, "Security And Privacy Issues of Handheld and Wearable Wireless Devices", Communications of the ACM, 2003

[22] http://europa.eu.int/comm/transport/road/roadsafety/rsap/index_en.htm

[23] http://www.epic.org/privacy/rfid

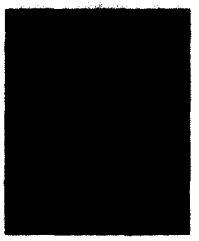
[24] http://www.cioinsight.com

[25] http://www.autoidcenter.org/privacy_hearing.aspversity of California, Berkeley

[26] Adrian Perrig 외 4인, "SPINS: Security Protocols for Sensor Networks", Uni

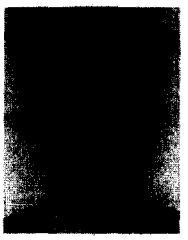
[27] David W. Carman 외 2인,"CONSTRAINTS AND APPROACHES FOR DISTRIBUTED SENSOR NETWORK SECURITY", 2000

[28] Preetida Vinayakray-Jani, "Security within Ad hoc Networks", PAMPAS Workshop, 2002



이 웅 용

1995년 : KAIST 전산학과 졸업
2003년 : KAIST 테크노경영대학원 졸업
1996년 ~ 1997년 : 데이콤
1997년 ~ 1999년 : 데이콤 ST
2000년 ~ 2002년 : 데이콤
2003년 ~ 현재 : 한국정보보호진흥원 정책기획단



박 광 진

1982년 : 동국대학교 전자계산학과 졸업
1988년 : 한양대학교대학원 산업대학원 졸업
1983년 ~ 1988년 : 한국통신
1988년 ~ 1997년 : 정보통신정책연구원
1996년 ~ 현재 : 한국정보보호진흥원 정책기획단장

참 고 문 헌

[1] L. Garber. "Denial-of-service attacks trip the Internet". Computer, pages 12, Apr. 2000.

[2] Computer Emergency Response Team, "TCP SYN flooding and IP Spoofing attackts," CERT Advisory CA-1996-21, Sept, 1996.

[3] P. Ferguson and D. Senie. "Network ingress Filtering: Defeating denial of service attacks which employ IP source address spoofing", May 2000. RFC 2827.

[4] K. Park and H. Lee. On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack. In Proc. IEEE INFOCOM '01, pages 338(347, 2001.

[5] D. X. Song, A. Perrig, "Advanced and Authenticated Marking Scheme for IP Traceback," Proc, Infocom, vol. 2, pp.878-886, 2001.

[6] Steve Bellovin, Tom Taylor, "ICMP Traceback Messages" , RFC 2026, Internet Engineering Task Force, February 2003.

[7] Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson, "Practical Network Support for IP Traceback", Technical Report UW-CSE-2000-02-01, Department of Computer Science and Engineering, University of Washington

[8] R. Stone, "CenterTrack: an IP overlay network for tracking DoS floods," Proc, 9th Usenix Security Symp., Aug., 2000.

[9] A.C. Snoeren, C. Partridge, L.A. Sanchez, W.T. Strayer, C.E. Jones, F. Tchakountio, and S.T. Kent, "Hash-Based IP Traceback", BBN Technical Memorandum No. 1284, February 7, 2001.

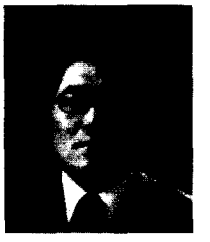
[10] H. Y. Chang et al., "Deciduous : Decentralized Source Identification for Network-based Intrusions," Proc, 6th IFIP/IEEE Int'l Symp., Integrated Net., Mmgt., 1999.

[11] Deering, S. and R. Hinden, "Internet Protocol, Version 6, (IPv6) Specification", RFC 2460, December 1998.

[12] Tatsuya Baba, Shigeyuki Matsuda, "Tracing Network Attacks to Their Sources," IEEE Internet Computing, pp.20-26, March, 2002.

[13] Andrey Belenky, Nirwan Ansari, "On IP Traceback," IEEE Communication Magazine, pp.142-153, July, 2003.

[14] W. Lee and K. Park, "On the Effectiveness of Route Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets," Proc. SIGCOMM, ACM Press, pp. 15-26., 2001.



이 형 우

1994년 2월 : 고려대학교 컴퓨터학과 졸업(이학사)

1996년 2월 : 고려대학교 컴퓨터학과 졸업(이학석사)

1999년 2월 : 고려대학교 컴퓨터학과 졸업(이학박사)

1996년 ~ 현재 : 컴퓨터과학기술연구소 연구원

1999년 ~ 2003년 : 천안대학교 정보통신학부 조교수

2003년 ~ 현재 : 한신대학교 소프트웨어학과 조교수

<관심분야> 정보보호, 네트워크 보안, 해킹·바이러스, 스테가노그래피, 침해대응/스팸대응기술, 컴퓨터 포렌식스 기술 등