情 報 保 護 學 會 誌
第17卷 第4號, 2007. 8

모바일 환경에서의 개인정보 위협 분석 연구

박현아*, 최재탁*, 임종인*, 이동훈*

요 약

2002년 11월 대한민국 전자정부의 공식출범을 비롯하여 최근 IT 839 전략 등에 힘입어 차세대 IT 분야의 급속한 발전은 바야흐로 유비쿼터스 컴퓨팅 시대로의 진입을 가속화 하고 있다. 최근에는 이것을 뒷받침 하는 기술 분야의 하나인 BcN(Broadband Convergence Network) 역시 그 연구에 박차를 가하고 있으며, 이것의 단말기 역할을 하는 이동성 있는 모바일 폰 기술 역시 급속도로 발전하고 있다. 하지만, 이런 기술 발전과는 달리 그 이면에는 개인정보보호의 침해라는 문제가 있다. 기술의 발전에 비례해서 개인정보 침해 역시 고도화, 전문화되어 급속도로 증가하고 있는 것이다.

본 고에서는 개인정보의 개념부터 먼저 살펴본 후, 모바일 폰의 표준화 현황 및 기반 기술과 응용 서비스 기술을 분석하여 문제점을 도출하고 그 대응 방안을 모색한다. 현재 서비스들이 하나의 소형화된 기기로 집적화되어 가고 있는 추세에서 휴대형 정보기기에서의 개인정보보호를 위한 대안이 절대 한 가지 메카니즘 만으로는 부족하며, 종합적인 보안 기술의 집합체를 이루어야 한다는 사실을 알 수 있게 된다.

Ⅰ. 서 론

2000년 이래 세계의 주요 학술대회나 보고서의 주요 이슈는 개인 정보보호에 대한 것이었다. 이러한 개인정보보호문제에 대해서 관심이 높은 이유는 우리의 일상생활에서 정보통신 기술의 급속한 발전에 기인한 것이다. 2002년 11월 대한민국 전자정부의 공식출범을 비롯하여 최근 홈네트워킹, 유비쿼터스 컴퓨팅, 전자태그(RFID) 등 차세대 IT 분야에 '붐'이라 해도 과언이 아닐 만큼의 많은 관심이 쏠리면서 기업 및 정부, 학계에서 많은 연구가 추진되고 있으며 인터넷 및 이동전화의 이용자가 전체 국민의 70% 이상을 점하게 됨에 따라, 이에 따른 개인정보 침해 사건 역시 급속하게 증가하게 된 것이 사실이다.

특히 근래에는 휴대폰, 스마트폰 등의 이동통신 단말기 이외에도 PDA와 휴대용 게임기, PMP(Portable Media Player) 등의 사용이 점점 늘어나고 있는 추세로 이와 더불어 향후 유비쿼터스 컴퓨팅 시대에는 많은 정보 기술이 서로 융합되어 이른바 디지털 컨버전스(Convergence)화하고, 언제 어디서나 어떠한 멀티미디어 서비스를 이용할 수 있게 되었다. 이것은 편의성 측면에서 사용자에게 더 없이 좋은 일이나 한편으로는 나의 모든 행동과 일상이 모두 관찰, 기록, 저장되어짐을 의미하며, 이것은 현대인의 개인주의적인 성향과는 정반대적인 성격을 지니는 것이다.

그런데 개인정보 침해 및 오남용 문제가 날로 늘어나고 심각해지고 있는 반면 IT 강국이라고 자부하는 우리나라에서는 IT분야의 외면적 발전과는 달리 이에 대한 적절한 대비책 마련은 소홀히 하고 있는 것이 사실이다. 이에 본 고에서는 개인정보의 개념에 대해 먼저 알아보고, 휴대형 정보기기 중 우리나라가 기술적 선진국의 위치라고 자부하고 있는 모바일 폰에서의 개인정보보호의 문제점을 분석하여 그 대응책을 마련하고자 한다.

Ⅱ. 개인정보

이 장에서는 개인정보의 법적 관점에서의 개념과 의미적 관점에서의 개념에 대해 알아본다.

* 고려대학교 정보보호대학원(kokokzi@cist.korea.ac.kr, algedi@cist.korea. ac.kr donghlee@korea.ac.kr, jilim@korea.ac.kr)
이 논문은 2006년도 한국전자통신연구원의 지원(06MW2220)에 의하여 연구 되었습니다.

2.1. 법적 정의

2.1.1. 95 EU 개인정보보호 지침(Directive 95/46/EC) 제2조 제a항:

식별된 또는 식별가능한 자연인(정보주체)에 관한 정보, 단 식별가능한 사람은 특히 신원증명번호 또는 육체적, 심리적, 정신적, 경제적, 문화적 또는 사회적 신원 중 한 가지 이상의 요인을 참고하여 직접적 또는 간접적으로 식별될 수 있는 사람을 말한다.

2.1.2. 국내법

① 공공기관의 개인정보보호에 관한 법률 제2조 2항 및 정보통신망 이용촉진 및 정보보호에 관한 법률 제2조 6항(2001.7.1 시행)

개인정보란 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명 · 주민등록번호 등의 사항에 대하여 당해 개인을 식별할 수 있는 부호 · 문자 · 음성 · 음향 및 영상 등의 정보(당해 정보만으로도 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합되어 식별할 수 있는 것을 포함한다)를 말한다.

2.2. 개인정보의 의미적 정의

개인정보와 관련해서 반드시 고려되어야 할 개념은 프라이버시이다. 개인정보와 프라이버시는 흔히 동일한 의미로 사용되고 있다. 일상적인 수준에서 그러한 혼용이 큰 문제를 낳는 것은 아니지만, 개인정보 침해에 대한 사회적 혹은 개인적 대응의 여러 가지 측면을 고려할 때 개인정보 혹은 개인정보보호의 개념만으로는 충분하지 않다.

어떤 사람의 개인정보에 대한 부적절한 접근, 수집, 저장, 분석, 이용은 그 사람에 대한 타인의 인식과 행동에 영향을 주며, 그 사람의 사회적 지위나 평가, 재산, 그리고 안전에 부정적인 결과를 초래할 수도 있다. 따라서 개인정보는 부적절한 접근, 수집, 저장, 분석, 이용으로부터 보호되어야 한다. 이 맥락에서 개인정보는 객체적 존재로서 보호의 대상이다.

그러나 보호해야 할 대상을 개인정보 자체라기보다 개인정보에 관한 권리라고 이해한다면 그것은 프라이버시 개념으로 접근할 수 있다. 프라이버시는 개인정보에 관해 정보주체가 쟁취하고 지켜야 할 권리라는 측면을 강조한 것이다.

프라이버시는 크게 다섯가지 차원을 갖는다.

(1) 프라이버시는 원하지 않은 접근으로부터 자유로울 권리를 말한다. 이 차원은 '홀로 남아 있을 권리'라는 고전적 의미의 연장이다. 이는 개인의 신체나 공간에 대한 물리적 접근을 의미할 뿐 아니라 전자우편, 메시징 등과 같은 가상적 접근(virtual access)도 포함한다. 다시 말해 주민이나 소비자가 온라인이나 오프라인을 통한 타인의 접근을 거부할 수 있는 권한을 갖는 것이다.

(2) 프라이버시는 자신에 관한 정보가 자신이 원하지 않은 방식으로 이용되지 않을 권리를 의미한다. 이는 본인의 동의 없이 개인정보가 매매, 이전, 노출, 매칭 등이 되지 않을 권리를 말한다. 이에 따르면 정부나 기업은 수집된 개인정보를 주민이나 고객이 동의하지 않은 용도로 이용할 수 없다.

(3) 프라이버시는 자신도 모르는 사이에 자신에 관한 정보가 남에게 수집되지 않을 권리를 의미한다. CCTV에 의한 모니터링, 쿠키나 로그파일에 의한 기록 등이 여기에 해당된다. 이는 정부나 기업이 주민이나 고객의 개인정보를 수집하는데 고지의 의무를 갖는다는 것을 의미한다.

(4) 프라이버시는 자신이 정확하고 올바르게 표현될 권리를 의미한다. 지식정보사회에서는 데이터베이스에 들어있는 개인정보가 한 사람의 정체성을 구성하기 때문에 개인정보의 무결성을 유지하는 것은 대단히 중요한 일이다. 여기서 파생되는 권리가 자기정보에 대한 접근과 결정이다. 정보주체가 데이터베이스에 들어있는 자신의 정보를 열람하거나 수정할 수 없다면 정보의 무결성은 유지되기 어려울 것이다.

(5) 프라이버시는 자신의 정보가 지닌 가치에 대해 보상받을 권리를 의미하기도 한다. 지식정보 사회에서 많은 경우 개인정보는 재산적 혹은 상품적 가치를 지니고 있다. 이는 개인정보의 수집과 활용에 있어 각 정보주체에게 어떤 형태로든 적절한 보상이 주어져야 함을 의미한다.

Ⅲ. 모바일폰 표준화 현황

모바일폰의 기술 발전은 크게 다섯 가지 부분으로 나눌 수 있다. 먼저 우리나라에서 CDMA (Code Division Multiple Access, 코드분할다중접속)로 대표되는 무선 이동 통신 방식, 단말기 및 칩 구성, 플랫폼, 응용 프로그램, 관련 서비스가 그것이다. 여기서는 표준화 활동이 활발한 네 가지 부면 즉 통신방식 및 전송기술, 플랫폼, 단말기, 응용 및 서비스에 관련된 표준화 현황을 살펴본다.

3.1. 통신방식 및 전송기술의 표준화 현황

이동 전화 서비스를 위한 통신방식과 전송기술은 1980년대부터 2000년대 중반인 오늘날까지 꾸준히 발전해 왔으며 이를 뚜렷한 기술과 서비스의 진보에 따라 세대별로 구분하고 있다.

3.1.1. 1세대~3세대

먼저, 첫번째 이동 전화 기술은 1980년대 아날로그인 AMPS(Advanced Mobile Phone System) 방식으로 첫 발을 내디뎠다. 하지만 이러한 1세대 아날로그 방식은 사용자가 많아질수록 주파수 대역을 할당하기가 어려워져 서비스의 양적 확대가 어렵다는 단점이 있었다. 또한 AMPS가 사용한 주파수는 음성전송과 신호 전송에 각각 아날로그 주파수 변조 (FM: Frequency Modulation)와 주파수변이변조 (FSK: Frequency shift keying)를 사용했기 때문에 오로지 음성 통화만 가능할 뿐 데이터 서비스는 불가능했다. 결국 이러한 한계를 지닌 AMPS를 이용한 이동 전화 서비스는 1999년 12월에 사라지고 말았다.

이어 1990년대 중반 획기적인 기술의 진전이 있었는데, 우리나라를 중심으로 상용화된 CDMA방식과 전세계의 대부분의 시장을 차지하는 시분할 다중접속 방식인 TDMA(time division multiple access)를 근간으로 한 GSM(Global System for Mobile communication) 방식의 2세대 통신 방식의 출현이 그것이다. 특히 우리나라는 코드분할 다중접속 방식인 동기식 CDMA 서비스를 세계최초로 상용화하여 괄목할 만한 성과를 거두었다. 이후 1800~1900 MHz의 주파수 대역을 사용하는 PCS (Personal Communication Service)가 2세대 후반에 등장해 CDMA 셀룰러 폰에 비하여 저렴한 단말기 제공과 멀티미디어 서비스 등 보다 차별화된 서비스를 선보였다.

3.1.2. 3세대 이후 표준화 동향

2세대 이후 급격한 팽창을 보인 모바일 폰 시장은 IMT2000으로 대변되는 3세대 기술로 다시 한번 도약한다. 특히 우리나라는 2000년 10월 CDMA2000 1X가 상용화하여 2세대 CDMA에 비해 동일 주파수 대역을 사용하면서도 약 2-10배 정도 빠른 144kbps의 속도를 지원하게 된다. 또한 음성 통화 외에 고속 데이터 서비스가 가능하고 동영상 및 이미지 전송 등의 부가서비스도 지원한다. 이어 2002년에는 국내 업체들인 SK텔레콤과 KTF등이 CDMA200 1X를 업그레이드한 CDMA 2000 1X EV-DO(Evolution Data Only)를 소개하였다. EV-DO는 다양한 데이터 서비스를 2.5Mbps로 지원한다. 하지만 우리나라에서 이러한 동기식 CDMA계열의 발전과 달리 세계적으로는 2.5세대 비동기식 방식인 GPRS(General Packet Radio Service)가 주목을 받으면서, 우리나라 역시 이후 시장 주도를 위해 W-CDMA (Wideband CDMA) 나 HSDPA (High Speed Downlink Packet Access)와 같은 비동기식 서비스를 내세우고 있다. 3세대 WCDMA가 약 2Mbps의 속도로 EV-DO 기반의 서비스에 비해서 3배 정도 빠르다면 HSDPA는 14.4Mbps의 속도로 WCDMA에 비해 7배 이상 빠르다. HSDPA 단말기는 화상통신이 지원되며 화상통화 중에 문자 메시지 전송이 가능하다. 또한, 음악을 들으면서 콘텐츠를 다운로드할 수 있을 만큼 멀티태스킹이 유연하다. 하지만, 아직 이들 서비스는 전국망 구축이 되지 않았음은 물론 단말기의 기술력 부족으로 속도 또한 2Mbps가 채 되지 않는다.

3세대에서 4세대로 넘어가기 전 단계인 3.5 세대 기술 가운데 하나인 와이브로(Wibro) 기술은 우리나라에서 표준화하고 상용화한 순수국내기술이다. 이동 중에도 수십 Mbps의 전송속도를 갖고 있으며 IP 기반의 기술이기 때문에 기존 인터넷 서비스를 모두 활용할 수 있다는 장점을 갖고 있다.

4세대 통신은 속도의 차별화로 3세대와 구분된다. 3세대 통신의 경우 대용량 멀티미디어 서비스가 가능하기는 하지만 HDTV와 같은 고품질의 화상서비스는 어려운게 사실이었다. 하지만 이동 중 100Mbps, 정지 중 1Gbps대의 4세대 통신이 제공하는 속도는 유선과 무선

의 결합, 통신과 방송의 결합을 예고하며 차세대 통방융합 시장을 통신이 주도해 나갈 것을 예고하고 있다. 속도 못지않게 끊김없는(seamless) 서비스 역시 4세대 기술이 지향하는 바이다. 4세대 표준은 아직 확정되지 않았으며 2007년 11월 4세대 대역에 사용할 주파수가 먼저 결정된 뒤 표준이 논의되고 2010년 이후 본격적으로 상용화될 것으로 예상된다.

3.2. 모바일 플랫폼 표준화 현황

지난 수 년간 모바일 컨텐츠를 개발하는 컨텐츠 제공업체들은 통신사마다 서로 다른 플랫폼을 사용하는 바람에 동일한 컨텐츠에 대해 각각의 특성에 맞도록 별도 개발해야 하는 불편을 감수해야만 했다. 이러한 비효율성을 줄이기 위해 표준 플랫폼에 대한 필요성이 제기되었으며 마침내 이통3사, 한국무선인터넷표준화포럼, 전파연구소, ETRI, TTA를 중심으로 2003년에 WIPI (Wireless Internet Platform for Interoperability)라는 이름으로 현실화 되었다.

3.2.1. 국내 표준화 현황

원래 WIPI는 한국 무선인터넷 표준화 포럼내의 모바일 플랫폼 특별분과 위원회에서 표준화를 수행하였다. 이를 위하여 SKT, KTF, LGT 등 이동통신 3사의 모바일 플랫폼에 대한 요구사항을 수렴하였고 그러한 요구사항을 반영하여 플랫폼을 개발할 업체로 복수의 업체를 선정하여 수행 하도록 하였다. 이때 각 업체들이 제안한 표준 규격(안)들은 플랫폼 표준 규격 작성에 참고자료로 활용되었다. 한편, 2002년 2월에 있었던 중간평가에서 복수의 플랫폼 개발 업체들 중 아로마소프트㈜가 최종 수행 업체로 선정 되었다. 이 업체는 포럼의 플랫폼 특별분과 위원회에서 제정하는 모바일 플랫폼 표준 규격의 지원 및 참조 구현(Reference Implementation)을 통한 규격의 검증 작업을 수행하게 되었다.

한국 무선인터넷 표준화 포럼은 모바일 표준 플랫폼의 표준 범위를 Basic 및 Extended API와 HAL API로 한정하였다. 이어 2002년 2월 C 및 Java API를 포함한 모바일 표준 플랫폼의 규격 초안을 작성하였는데, 이는 표준 플랫폼을 도입하여 단말기용 어플리케이션 개발자에게는 플랫폼간 컨텐츠 호환성을 보장하고, 단말기 개발자에게는 단말기 이식성을 제공하기 위한 최소한의 필요 조건이라 할 수 있다. 공모에 의하여 WIPI로 명명된 모바일 표준 플랫폼의 규격은 이후 표준화 일정을 거친 후 TTA의 단체 표준으로 확정되었다.

3.2.2. 국제 표준화 추진 현황

2002년 5월 12일부터 5월 17일에 개최되었던 3GPP TSG-T Working Group 2에 퀄컴의 BREW와 함께 모바일 플랫폼의 표준으로 발표 되었으며, 향후 모바일 실행 환경의 새로운 클래스마크(Classmark)로의 채택을 목표로 지속적인 활동이 이루어 질 전망이다. 또한 한.중 무선인터넷 포럼 간의 협력, 노키아의 무선인터넷 플랫폼인 OMA(Open Mobile Alliance)와의 협력 등을 통하여 국제적인 인지도를 증대시키려는 노력도 함께 이루어지고 있다.

일단 WIPI를 위시한 국내 모바일 플랫폼의 개발 환경은 갖추어 진 셈이다. 우리나라가 2, 3 세대 모바일 기술에서 세계를 선도해 왔음에도 막대한 기술 로열티 유출 문제를 해결하지 못한 선례를 교훈삼아 3.5~4세대에 더욱 확장되는 모바일 통신 시장에서는 기반 기술과 응용 기술의 시장 확보를 위해 플랫폼 원천 기술의 내재화 등의 다각적인 노력을 기울여 나아가야 할 것이다.

3.3. 단말기 보안 관련 기술 표준

모바일 폰이 디지털 만능기기(All in One)로 변신하면서 분실 혹은 도난 시 데이터에 대한 정당하지 않은 접근으로부터 보호받을 수 있는 방안이 필요하게 되었다. 특히 모바일 뱅킹이나 모바일 주식 거래가 보편화되면서 각종 개인 정보가 모바일 폰에 고스란히 담기기도 하고 송수신 되면서 이러한 필요는 더하게 되었다. 이동통신 사업자 그룹은 모바일 폰용 하드웨어 기반 보안 표준을 발표했다.

표준단체인 TCG(Trusted Computing Group)는 모바일 폰 작업반 TCG (https : // www. trusted compputting group. org/groups/mobile)을 산하에 두고 모바일 폰용 하드웨어 기반 보안 표준의 초안인Mobile Trusted Module Specification, Version 0.9를 2006년 9월 1일 공식 발표했다. TCG는 Nokia, Motorola, Intel, 삼성, Verisign, Vodafone 등 대기업이 후원하는 컨소시엄으로서 PC와 서버에 대해서도 이미 유사한 스펙을 개발 완료한 적이 있으며 "Trusted Computing Group Mo-

bile Specification: Securing Mobile Devices on Converged Networks"라는 화이트 페이퍼를 공개한 표준화 단체이다.

TCG가 제안한 표준은 사용자의 개인적인 데이터만 보호하는 것이 아니다. 엔터테인먼트 업계의 요청에 따라 저작권 보호 기능도 추가됐다. DRM(Digital Rights Management) 기술을 이용해 모바일 폰으로 이용할 수 있는 콘텐츠로의 접속은 다양하게 할 수 있도록 하면서도 해당 콘텐츠가 모바일 폰에서 운영되는 것은 제한하는 것이다.

이 기술을 이용하면 모바일 폰 서비스 업체들이 자사 단말기를 더욱 철저히 통제할 수도 있다. 이는 서비스 업체들이 모바일 폰 단말기를 이용해 자사 네트워크에 접속할 수 있는 방법을 통제하고, 어떤 서비스와 소프트웨어가 모바일 폰에서 운영될 수 있는지에 대해서도 더욱 강력하게 제어할 수 있게 된다는 것을 의미한다. 그러나 이러한 수단이 오히려 사용자의 선택과 자유를 제한하는데 악용될 수도 있다.

아직 모든 면에서 표준화가 진척되지는 않았지만 일단 'Mobile Trusted Module Specification, Version 0.9'에 따르면 모바일 폰 하드웨어는 TPM(Trusted Platform Module)과 유사한 기능을 지원해야 한다. TPM은 PC와 서버에서 인증, 스토리지 보안, 이메일 보안 등 다양한 보안 기능을 추가할 수 있도록 설계된 보안 칩으로 PC 사용자수에 비해 모바일 폰 사용자수가 적기 때문에 TPM 기술이 적용될 필요가 있다. TCG는 모바일 폰 제조업체들의 원가를 줄여주고, 부품 공급업체들이 표준화될 수 있도록 하나의 표준을 제공하는 것을 목표로 하고 있다.

Ⅳ. 모바일 폰 응용 서비스 분석

이 장에서는 모바일 폰 관련 응용 서비스 기술을 분석한다.

4.1. 모바일 위치기반서비스

위치기반서비스(Location Based Service, LBS) 란, "이동통신망을 기반으로 사람이나 사물의 위치를 정확하게 파악하고 이를 활용하는 응용시스템 및 서비스를 통칭"한다.

LBS S/W는 크게 LBS 플랫폼, 위치응용 S/W, 단말기 S/W 등 3가지 요소로 구성된다.

첫번째로, 기존의 무선망 플랫폼을 위치 응용 S/W와 위치 서비스 클라이언트를 통합하여 지원하는 LBS 플랫폼이 있다. LBS 플랫폼은 망과의 인터페이스, 특히 위치를 측위하는 시스템과의 인터페이스 기능, 위치정보 저장 및 처리 기능, 유무선 게이트웨이 기능, 응용 프로그램 지원 API 기능, 컨텐츠 전송 및 변환 기능, 보안 및 인증 기능, 프로파일 관리 기능, 고급 위치기반 서비스 지원 기능 등을 제공한다.

두번째로, 위치 컨텐츠를 처리하고 고객에게 부가 서비스를 제공하는 위치 응용 S/W가 있다. 항법, 경로안내, 위치추적, 주변정보 검색 등 다양한 위치기반 서비스를 위한 응용 S/W가 여기에 해당된다.

세번째로, 단말기에서 위치응용 서비스를 제공하기 위한 단말기 클라이언트 S/W가 있다. 단말기 S/W는 다양한 Kjava, WAP 등 다양한 무선 단말플랫폼 위에서 위치 응용서비스를 제공해주기 위한 S/W 이다.

위치기반서비스는 크게 공공 안전 서비스, 위치기반 과금, 추적 서비스, 확장 통화 라우팅, 위치 기반 정보 서비스, 네트워크 확장 서비스 등으로 나눌 수 있으며 세부 서비스는 다음과 같다.

4.1.1. 공공 안전 서비스(Public Safety Services)

① 응급 서비스 (Emergency Services): 119와 같은 응급 구조 시스템.
② 응급 경계 서비스 (Emergency Alert Services): 지진, 해일, 산사태 등이 발생한 지역에 대한 정보와 사용자의 위치를 대조하여 긴급 경계를 발하여 안전을 보장하고 실시간 정보 제공

4.1.2. 위치 기반 과금 (Location Based Charging)

4.1.3. 추적 서비스 (Tracking Services)

직원의 위치와 상태를 파악해야 할 배달 서비스의 감독자, 아이들이 어디 있는지 알아야 할 부모, 동물 추적, 그리고 자산의 추적 등이 있다.

① 차량 및 재산 관리 서비스 (Fleet and Asset Management Services)
② 교통 감시 (Traffic Monitoring)

4.1.4. 확장 통화 라우팅(Enhanced Call Routing)

이것은 가입자들이나 사용자 통화들이 원래 위치를 근거로 가장 가까운 서비스 클라이언트로 통화가 분배되도록 한다. 사용자는 서비스를 이용하기 위해 형상이나 서비스 코드를 통하여 전화를 걸 수 있다.(예를 들어 가장 가까운 주유소에 대해서는 *GAS등).

4.1.5. 위치 기반 정보 서비스 (Location Based Information Services)

서비스 요청은 가입자에 의한 주문으로 이루어질 수도 있고 조건이 만족되면 자동으로 이루어질 수도 있으며, 하나의 요청이나 주기적인 응답으로 결과가 나올 수도 있다.

① 항법(Navigation)- 핸드 셋 사용자에게 목적지를 안내해 준다.

② 도시 관광 (City Sightseeing)-관광객에게 현 위치와 관련된 특정한 정보를 전달한다.

③ 위치 의존 컨텐츠 중계(Location Dependent Content Broadcast)- 네트워크가 주어진 영역 내에서 모든 단말기로 중계되거나, 특정한 구성원들(아마도 특정한 단체의 일원들)에게만 중계될 수 있다. 사용자는 단말기로부터 이 기능을 제한할 수도 있고, 사용자가 관심 있는 정보 범주만 선택할 수도 있다.

④ 모바일 옐로우 페이지(Mobile Yellow Pages)-전화번호부를 넘기거나 114에 전화하는 대신 간단히 온라인에 들어가 번호를 찾으면 된다. 무선 옐로우페이지 서비스는 사용자에게 이탈리아 식당과 같은 가장 가까운 서비스 지점의 위치를 제공한다. 질의 결과는 범주(3km 내에 있는 이탈리아 식당)를 만족하는 서비스 포인트로 열거될 수 있다.

4.2. 모바일 RFID

지금까지 RFID는 유통, 재고관리 등 주로 기업의 비즈니스 목적에 대한 응용만 고려되어 왔다. 하지만, 고객들이 쓸 수 있는 모바일 폰에 태그나 리더기를 부착하여 RFID 서비스를 이용한다면 무궁무진한 편리한 활용이 가능해진다. 이에 발 맞추어 모바일 기기에 장착할 수 있을 만큼 작은 크기의 RFID 리더기가 개발되었고 이에 따른 모바일 RFID활용 방안도 활발히 전개될 수 있었다.

다음은 모바일 RFID 서비스의 예이다.

① 와인 정보 제공 서비스-와인병에 부착된 RFID 태그를 인식하여 상세정보를 확인하는 서비스.

② 양주 진품 제공 서비스-양주에 부착된 태그를 인식하여 진위 여부를 확인하는 서비스.

③ 관람 영화 정보 서비스- 고객이 소지한 태그를 영화관에 설치된 리더기가 인식하여 상영 영화 정보, 이벤트 및 프로모션 정보를 제공하는 서비스

④ 버스 정보 제공 서비스-버스 정류장에 부착된 태그를 인식하여 버스 도착 예정정보 및 정류장 위치기반의 다양한 생활정보서비스를 제공

⑤ 택시 안심 정보 서비스-택시에 부착된 태그를 인식하여 택시정보를 쉽게 조회하고 지인에게 택시정보를 전달할 수 있는 안심 귀가 택시 서비스(서울시 전차량에 부착 예정)

⑥ 관광 정보 제공 서비스-관광지의 주요 시설물, 문화재, 안내소 등에 부착된 태그를 인식하여 관광객 및 관리자가 해당 정보를 제공받는 서비스

⑦ 식품 안전 정보 제공 서비스-식품에 부착된 태그를 인식하여 제조/유통 이력을 확인하는 서비스

⑧ 강원 한우 정보 제공 서비스-한우 팩에 부착된 태그를 인식하여 사육정보(농장, 사료, 품종, 도축, 유통 등)를 제공받는 서비스

4.3. 모바일 헬스케어

유비쿼터스 혹은 퍼베시브(pervasive), 착용하는 모바일 컴퓨터(Mobile Wearable Computer) 연구의 일환으로 구현된 모바일 헬스(m-health) 솔루션은 착용하는 컴퓨터, 이동통신 단말기 기술의 활용을 위하여 다양한 응용 플랫폼을 제시하고 있다.

모바일 당뇨폰의 기본 서비스로는 모바일 폰을 기본 플랫폼으로 하여 혈당계, 만보계 등을 모바일 폰 시스템에 반영해 유선 및 무선네트워크로 개인별 서비스가 가능하게 되는 것이 있다. 특히 혈당측정기와 만보계를 배터리 팩에 내장해 언제 어디서나 편리하게 자신의 혈액을 채취하고 이를 배터리 팩에 꽂아 혈당을 측정하여 무선 DB를 이용한 효과적인 혈당 데이터 분석 및 관리가 가능한 것이 특징이다. 서비스 세부 항목으로는 일반과 프리

미엄이 있는데 일반 서비스의 경우 월 6,000원의 요금 정도로 지속적인 식이요법, 운동요법 처방 등 개인별 '주치의 서비스'와 같은 맞춤 서비스를 제공받을 수 있다.

당뇨폰이 실질적인 모바일 헬스케어 서비스의 출발점으로 각광받는 이유는 무엇보다 환자는 혈당체크에서 식단·투약·운동 등 종합적 관리가 가능하고 의사는 진단과 처방 및 진료 등 환자관리를, 병원은 비용절감, 환자 유치 및 홍보에 이르기까지 효율적인 업무관리가 가능해지기 때문이다. 이처럼 모바일 헬스케어는 환자-의사-병원간 모두에게 이익을 안겨주는 서비스 모델이다.

삼성전자의 체지방 모바일 폰은 모바일 폰 본체와 측정기로 분류돼 있으며, 측정기에 양 손가락을 대면 체지방 수치가 자동으로 측정돼 LCD화면에 나타난다. LG전자의 당뇨폰 역시 자신의 혈액을 채취해 배터리팩에 꽂으면 간편하게 혈당을 측정할 수 있는 것으로 무선으로 혈당 데이터 분석까지 가능하다. 팬택은 음악과 영상을 통해 심리를 치유하는 '힐링 윈도'(Healing Window)를 장착한 심리치유폰(S2M)를 출시했다. 국내 업체는 특히 스트레스 지수를 산출, 건강한 정신을 유지하는 스트레스폰 등의 시제품을 국제의료기기전시회에 선보이고 비만도 및 칼로리를 측정하고 다이어트 콘텐츠를 제공하는 다이어트폰을 차기 제품으로 준비하고 있으며 심전도·혈압·맥박 등의 생체 신호를 측정할 수 있는 바이오폰도 선보였다.

한편 대전광역시는 2005년 국내 최초로 모바일 헬스케어 시범도시를 구축하여 시민의 건강증진을 도모하고자 하였다. 2005년 11월부터 3개월간 대전시를 주축으로 7개 시내 종합병원과, 개발업체, 연구소 등과 협력하여 당뇨환자 1,000여 명을 대상으로 혈당 측정기(Gluco Plus)와 혈당 측정칩(스트립) 등을 무상으로 제공하였다.

분당 서울대병원은 이른바 '유비쿼터스 건강관리 시험서비스'를 통해 환자가 집에서 혈당과 심전도를 측정하면 그 정보가 무선망을 통해 병원으로 전달하는 서비스를 운영하고 있다. 삼성 서울병원은 Mobile Hospital 시스템을 확대, 원내는 물론 원외, 전국 어디에서든 환자정보를 조회해 신속하세 처치하고 모바일 스마트폰을 통해 PACS 영상 이미지까지 조회할 수 있도록 할 계획이다. 유럽에서는 모바일 헬스케어 서비스의 일환으로 GPRS와 UMTS를 이용한 MobilHealth BAN 프로젝트를 추진하고 있다.

또, 모바일 RFID를 이용하여 다양한 서비스들과 연계될 수 있는데, 홈 네트워크도 그 중 하나이다.

홈 네트워크 가입자는 자신의 집에서 정보가전과 냉난방, 가스, 전기 등을 조절하고 TV나 인터넷을 통해 디지털 콘텐츠를 제공받는다. 또한 가정내 설치된 의료기기 등을 통해 실시간 의료 서비스를 제공받을 수도 있다. 뿐만 아니라 모바일 폰이나 PDA, 기타 휴대형 정보기기를 집 외부로 가지고 나가더라도 이동 통신 망을 통해 홈 네트워크 헬스케어 서비스를 제공받을 수 있다. 환자가 가정 내 의료기기에서 투약을 지시받은 의약품을 소지하고 외출하면 모바일 폰으로 투약 시점과 투여량을 알람으로 알려 줄 수 있다. 더욱이 IBM이 추진한 착용하는 컴퓨터와 연계하면 환자는 맥박계, 혈당계 등이 부착된 컴퓨터를 입은 채 일상 생활을 하면서 실시간으로 건강 체크를 받을 수 있다.

4.4. 모바일 TV

모바일 TV는 말 그대로 모바일 기기로 TV를 시청함으로써 장소와 시간의 제약을 뛰어 넘을 수 있는 서비스를 지칭한다. 서비스 초기 콘텐츠의 부족과 지상파 방송사 간의 수익 분배 등 협상 문제로 부진한 면이 있었다. 하지만 최근에 모바일TV의 열기는 다시 달아오르고 있다. 미국의 예를 들면 시장 조사 기관 인스탯(In-Stat)은 미국에서 지난해 110만 명 정도가 모바일 비디오 콘텐츠를 구입한 것으로 추정하고 있지만 이 수는 2010년에는 3,000 만에 이를 것으로 전망하고 있다. 위성 DMB (Digital Multimedia Broadcasting), 지상파 DMB, 이동통신망을 이용한 스트리밍방송 등 이른바 모바일TV 시장 선점을 위해 전 세계 통신방송업체들이 치열한 경쟁을 벌이고 있다.

4.5. 모바일 웹

모바일 폰이 보편화되고 성능이 크게 향상됨에 따라 모바일 폰으로 웹 서비스를 이용하려는 요구가 일었다. 하지만, PC나 랩톱에 비해 모바일 폰은 화면의 크기가 매우 작고 기기 환경도 차이가 나기 때문에 모바일 폰에 알맞는 웹 서비스가 필요하였다. 이에 개발자들과 포털 업체들은 자사의 홈페이지를 PC및 유사 환경과 모바일 폰에서 따로 동작할 수 있게 디자인하기로 의견을 모았다. 이것이 바로 모바일 웹의 등장 배경인데, 이른바 모바일 폰의 환경에 맞게 최적화된 웹서비스를 제공하자는데 그 의의가 있으며 그러자면 브라우저나 화면

구성, 기술적 부문 등 관련 요소들의 표준화가 선행되어야 할 것이다. 모바일 웹 표준화가 바로 다양한 이동 단말기에서 기존 인터넷과 포털 등에서 제공되고 있는 각종 콘텐츠와 서비스를 이용할 수 있도록 웹 사이트 설계와 브라우저 규격 등을 표준화하는 것이다.

V. 개인정보의 위협 분석 및 대응 방안

휴대형 정보기기로서 가질 수 있는 개인정보 보호에 있어서의 문제점과 모바일 폰 기기의 특수한 서비스로 인해 나타날 수 있는 위협으로 나누어 생각해 본다.

5.1. 휴대형 정보기기로서 가지는 공통된 문제점

5.1.1. 단말기 자체의 보안 취약점으로 인한 문제점

1) 불법복제 단말

기존 이동통신의 경우, 핸드폰 고유 식별자인 ESN (Electronic Serial Number) : 무선 전화기의 마이크로칩 속에 생산자가 삽입해 넣은 32비트의 전세계 고유번호로, 가입자가 통화를 시도하면 자동으로 ESN과 전화기 사업자의 MIN(Mobile Identification Number)이 송출되며 기지국을 통해 이 번호가 인증이 되면 통화를 연결한다. 번호를 복사하여 복제폰을 만드는 것이 가능하였으며, 지금도 불법복제에 의한 피해가 계속 발생하고 있다.

이런 불법복제 단말에 대한 대응책으로는 복제가 불가능한 스마트카드를 활용한 인증방식을 도입하는 것과 단말의 도난/분실 시 바로 신고하여 대응할 수 있는 절차를 마련하는 것이다.

2) 단말기 내에 저장되어 있는 개인정보보호의 문제점

서비스 정보 단말기에 개인 식별정보를 입력하고 관리할 경우 단말기에 저장된 정보가 다른 사용자에 의해 노출될 우려가 있다. 원칙적으로 단말기 내의 개인 정보의 저장을 금해야 하고, 단말기 내에 가입자의 개인 정보를 저장하여 관리할 경우에는 이용목적 및 사용 용도를 알리고 명시적인 동의를 받아야 한다. 그리고 단말기별로 사용자를 명시하고 접근권한을 부여하여 지정된 자 외의 사람이 단말기에 접근할 수 없도록 한다.

또, 분실 시에는 사용자가 서비스에게 신고하도록 하여 서버측에서 사용자의 메모리에 저장된 내용을 사용자의 패스워드로 암호화되게끔 하는 메카니즘을 구축해 놓는 방법도 생각해 볼 수 있다.

공공기관의 개인정보보호에 관한법률시행규칙에서는 단말기 내에 개인정보를 저장하는 경우에 대한 처리 및 관리 규정을 제시하고 있다- 공공기관의개인정보보호에 관한법률시행규칙 제6조 (단말기의 설치·관리).

3) 단말기 인증

불법 단말기의 사용을 방지하기 위해서는 단말기 자체에 대한 인증 과정이 필요하다. 현재까지 단말기 자체에 대한 인증은 미들웨어 레벨에서 제공되고 있다. 하지만 단말기 유효성 확인을 위한 시리얼 넘버나 인증서 등은 개별 제조업체 등에서 자체적으로 발행하고 있다. 그리고 각 단말기들의 성능이 다르므로 그에 따른 보안 기술이 각각 다르다.

디바이스가 서비스의 주체가 되어 서비스 도메인간의 인증기능 로밍이 가능한 멀티도메인 인증기술을 사용하여야 한다.

또, 하드웨어 기반의 인증을 위해 TPM(trusted platform module) 칩을 기기에 탑재하는 것도 하나의 대안이 될 수 있다.

5.1.2. 무선 인터페이스에 관련된 위협들

휴대형 정보기기의 전송 구간은 단말과 기지국 간의 무선 인터페이스 구간과 기지국과 제어국 및 각종 서버 간의 유선 인터페이스로 구성된다. 이런 유/무선 상에서의 개인정보의 위협은 각기 다를 것이므로 본 과제는 유/무선 인터페이스 구간을 구분하여 분석하도록 한다.

1) 인증 및 권한

현재 사용자 인증 기술은 생체인식, 패스워드, 인증서, 스마트카드 등 다양한 기술이 사용된다. 하지만 유비쿼터스 컴퓨팅 환경으로의 진화를 고려할 때 정보단말기기는 낮은 성능을 고려한 사용자 인증기술을 사용할 것이며, 또한 사용자의 편의성을 고려하여 더욱 편리한 생체중심의 사용자 인증수단이 많이 사용되어질 것이다.

무선 인터페이스와 관련하여 사용자 및 서버의 서비스 인증이 제대로 이루어지지 않았을 경우 시스템 상에서 발생할 수 있는 문제는 다음과 같다.

- 데이터로의 인가되지 않은 접근

- 도청
- 무결성 위협
- 서비스 거부(DoS)
- 시스템으로의 인가되지 않은 접근
- 또 다른 시스템으로 가장 : 침입자는 네트워크 상에서 또 다른 사용자로 가장할 수도 있다. 침입자는 사용자를 향해 기지국인척 가장할 수도 있으며 그때 인증을 수행한 후에 연결을 하이젝킹할 수도 있다.

WPKI 등은 모바일 환경에 적합한 인증 체계가 있다. 따라서 스마트 카드 칩이 탑재된 모바일폰 등 보다 강화된 보안 모델이 필요하다. 특히, 단방향 인증방식을 사용할 경우, 기지국을 위장한 공격이 발생할 수 있다. PKMv1의 경우, 단말은 X.509 인증서를 기지국에 보내어 기지국은 단말을 인증할 수 있지만, 단말은 기지국을 인증하는 메커니즘이 적용되어 있지 않다. 이때 공격자는 기지국으로 위장하여 정상 단말의 접속을 유도한 후, 단말을 무조건 인증하고, 임의로 생성한 인증키를 단말에 분배한다. 이후 단말이 송수신하는 모든 트래픽은 공격자가 엿볼 수 있으며, 불법접근이 가능해진다.

이를 해결하기 위한 방안으로는 PKI 기반의 안전한 인증 및 키 관리 프로토콜을 사용하는 것이다. 이때 인증은 클라이언트 단 뿐만 아니라 서버단의 인증까지 같이 고려되는 양방향 인증이어야 하며, 서비스 거부 공격과 단말 및 기지국을 위장하는 공격에도 안전한 프로토콜이어야 한다.

2) 전파 간섭(Frequency Jamming)

주파수 간섭 공격은 강한 주파수 간섭을 발생시켜, 서비스거부공격을 유도하는 보안위협이다. 공격에 대응하기 위해서는 강한 시그널을 사용하여 주파수 간섭 공격에 의한 간섭을 최소화하거나, 주파수 모니터링 장비를 통해 사전에 공격을 탐지하고 대응한다.

이에 대한 대책으로 우선 전파간섭 사실을 중앙전파관리 연구소에 신고 하는 것이 있을 수 있으며, 공격자를 추적하거나 비정상적인 동작을 하는 단말을 모니터링 하는 것을 들 수 있다.

3) 부인

무선상에서 일어날 수 있는 부인은 다음의 세 가지 경우로 나누어 볼 수 있다.

(1) 과금의 부인 사용자는 시스템에 접근한 사실 자체를 부인하거나 서비스를 사용한 사실을 부인함으로써 과금할 의무를 거부할 수가 있다.
(2) 사용자가 트래픽을 전송한 사실을 부인
(3) 사용자가 트래픽은 수신한 사실을 부인.

(2)번과 (3)번의 경우는 MAC을 이용해서 메시지 및 리소스 인증을 동시에 함으로써 해결 가능하다. (1)번의 경우는 서비스 이용시 개인의 고유 비밀값을 이용한 단말 및 사용자 인증 후 서비스를 이용하도록 하는 것이 바람직하다.

4) 해킹/ 악성코드

현재 모바일 폰에서는 폰 바이러스가 창궐하고 있는 추세로 이는 점차 고도화 되어 다른 정보기기(PC, PDA 등)로 전이된 사례도 있다. 또 수능부정 사건에서 알 수 있는 것처럼 통신사에는 일반 사용자들의 정보 등이 실시간으로 쌓이게 된다. 폰 바이러스나 폰 웜(Worm)은 모바일 폰의 개인정보를 파괴하거나 다른 폰으로 무차별 전송할 수 있기 때문에 이에 대한 철저한 보안적 관리가 요구된다. 문자 메시지 등은 관리적 보안뿐 아니라 기술적 보안도 함께 이루어져야 한다. 검색 가능한 암호화 DB 스킴 등을 사용하다면, 기한이 지난 메시지를 지우지 않더라도 자신이 주고 받은 메시지의 검색과 함께 자신의 프라이버시도 보호할 수 있을 것이다.

5.1.3. 유선 인터페이스에 관련된 위협들

1) 주요 시스템 접속기능 제한

시스템을 구성하는 장비들에 대해 비인가된 부서, 사

[표 1] 통합 보안관리시스템의주요기능

구 분	주요내용
관제기능	- 각종 네트워크 장비의 로그 수집 - 보안 관련한 이벤트 필터링 - 추적기능을 통해 패킷이 지나간 통로 역추적 - 해킹시도 및 접근경로를 실시간으로 파악하여 대응
운영관리 기능	- 로그분석, 보안감사, 자산관리, 구성관리, 성능관리 - 장애관리, 이력관리, 무결성 관리, 다중계정관리

람들의 접속을 통제할 수 있어야 한다. 특히 핵심 구성 요소들은 반드시 사전승인을 받은 부서, 사람들만 접근할 수 있도록 통제해야 한다. 사용자별로 허용된 위치(IP주소, 단말, 통신 등)에 의해서만 접근이 이루어져야 하며 사용하지 않는 서비스는 차단해야 한다. 이를 위해 주요 시스템에 대한 접근을 제한하기 위한 체계적인 관리절차의 마련도 필요하다.

2) 주요 시스템에 대한 통합 보안관리

(1) 패치관리시스템 사용-운영체제에 대한 최신 패치 및 업그레이드.

(2) 비정상트래픽 모니터링 및 대응

통합 보안 관리시스템은 침입차단시스템, 침입탐지시스템, 가상사설망, 바이러스월등 각종 네트워크 보안 제품의 통합관리와 각 요소 제품 간에 인터페이스 및 교환되는 메시지포맷 표준화를 통해 모니터링과 원격지 중앙관리까지 가능하여 해킹, 바이러스 등에 대한 종합적인 판단과 효율적인 대응능력을 제공한다.

다음은 통합 보안관리시스템이 제공하는 주요 기능을 나타낸다.

5.1.4. 서비스 환경과 관련한 개인정보보호의 위협

1) 서비스 가입 및 해지시

개인 정보가 포함된 가입 및 해지 관련 서류는 어떤 서비스 분야에서도 중요하게 관리되어야 한다. 가입 관련 서류는 사본이 생성되어서는 안되고 필요에 의해 사본이 만들어질 경우는 원본과 사본이 구별 되어져야 한다. 가입 서류 등은 잠금장치가 되어 있는 보관소에 저장되어야 하며, 정기적으로 사업본부로 이관되어져야 한다. 만일 서비스 사업자가 보관중인 서류는 가입자가 해지를 원할 경우 즉시 폐지되어야 하고, 주기적인 감사를 통해 이를 이행하고 있는지 판단하여야 할 것이다.

2) 타 서비스와 연계시

타 서비스와 연계시의 문제점은 우선 각 서비스 제공자들마다 가입자들에 대한 정보를 공유하고, 인증한다는 것이다. 여기서 각 개인의 정보들은 서비스 제공자에 따라 필요한 것과 필요하지 않는 것이 있을 수 있는데, 어떤 서비스를 위해 필요하지도 않은 정보를 공유함으로써 관리의 소홀을 야기하여 개인정보의 유출 및 침해를 일으킬 수도 있다. 따라서 여기서 중요한 것은 각 서비스 업체들은 반드시 자신의 서비스에 필요한 정보들만을 공유하여야 하며(정보 최소 수집의 원칙), 서비스 이동시 상호 인증후 서비스를 이용하게끔 하는 것이 바람직하다.

연계된 복잡한 서비스를 제공하는 환경에서는 통합 보안 관리(integrated security management, ISM) 툴은 다양한 보안 기술을 정책 준수나 서비스 및 지원, 손쉬운 구축과 통합을 가능하게 해주는 포괄적인 보안 시스템을 제공한다. 다양한 보안 기능을 결합한 ISM은 네트워크 공격에 대한 영향을 최소화하기 위해 각 계층에서의 다양한 위협에 효과적으로 대응할 수 있다.

3) 기지국 및 제어국에서의 개인정보보호 요구사항

(1) 기지국/제어국에 접근하여 사용하는 내부자에 대한 관리감독이 필요하다. 기지국/제어국을 사용하는 경우 id/password와 같은 인증과정을 거친 후 사용하도록 한다.

(2) 외부에서 네트워크를 통해 접근하여 기지국/제어국을 이용 할 수 없도록 하거나, 기지국에 접근할 수 있는 IP 주소 및 사용자를 제한해야 한다.

(3) 기지국에 설정된 기본적인 id/password를 삭제하거나, 기본적인 id/password를 통해 기지국의 중요정보에 접근 하지 못하도록 접근제한을 둔다. 또한 각 사용자별로 접근할 수 있는 데이터 항목을 구분하여 설정 할 수 있도록 하는 기술을 적용한다.

(4) 기지국/제어국과 장치 및 서버사이에 전송되는 데이터를 생성한 주체를 검증하는 과정이 필요하다. 또한, 전송된 데이터가 변조 되었는지를 판단할 수 있는 검증 과정이 있어야 한다.

(5) 기지국/제어국과 장치 및 서버와 전송되는 데이터에 대해 암호화 기능을 적용하여, 데이터가 유출되지 않도록 해야 한다.

(6) 기지국(사용자 단말)에서 사용자 단말(기지국)과의 접속을 종료하는 경우, 접속 종료를 요청하는 메시지 및 메시지를 보낸 주체에 대한 검증과정이 필요하다.

(7) 기지국은 일정시간이 지나면 재인증을 요청한다. 일정시간이 지나지 않은 상황에서 공격자가 정상적인 사용자 단말로 위장하여 재인증 메시지를 전송할때, 전송되는 메시지를 보낸 주체 및 메시

지 변조여부를 검증해야 한다.

(8) 사용자 단말이 다른 지역으로 이동하는 경우, 기존 기지국과의 연결을 종료하기 위해 핸드오프 메시지를 전송한다. 기지국에 전송되는 메시지를 보낸 주체 및 메시지 변조 여부를 검증해야 한다.

4) 서비스 사업자의 대응

정보보호담당자는 설치한 보안 장비가 정확하게 설정되어 있는지 주기적으로 확인하여 침해사고를 예방하여야 하고, 서버관리자는 운영 중인 네트워크 장비가 해킹, 웜·바이러스 공격 등의 피해를 입지 않도록 주의해야 한다. 다음은 서버 보안 취약으로 인한 개인정보 누출 잠재성에 대해 이야기 한다.

(1) 서버 보안 취약으로 인한 개인정보 누출

휴대형 정보기기를 통하여 전송되는 정보들은 최종엔 서버의 데이터베이스에 저장된다. 서버단계에서 가장 중요한 이슈는 불법적인 침입자로부터 서버 자원이 보호되어야 하는 것이다. 이를 위해 모든 서버에서는 식별 및 인증, 접근 권한 정책 등을 실시할 수 있으며, 이를 의무화할 필요성도 있다.

이를 위한 방어책으로는 다음과 같은 것이 있다.

① 데이터베이스 보안 기술 적용

② 접근 권한 및 통제 기술 적용

③ 접속 기록의 유지- 보안사고가 발생했을 때 서버의 접속 기록을 통해 사고의 원인을 파악하게 된다. 즉, 불법적인 패킷 혹은 불법적인 서버로의 접근 기록, IP 주소 등을 파악하여 IP 역추적을 수행한다. 이를 가능하게 하기 위해서는 접속 기록의 유지 및 보관은 반드시 필요하다. 정기적인 백업과 안전한 관리도 뒤따라야 할 것이다. 이와 더불어, 수집한 기록의 누설, 멸실, 훼손으로부터의 적절한 보호도 필요하다. 또한 저장된 자료를 가지고 시스템 접근에 대한 정기적인 분석 작업을 통하여 적절한 통계 값을 산출하여 보안사고 예방에 활용할 수 도 있을 것이다.

5.2. 모바일폰의 특수성으로 인해 야기되는 개인정보 위협

앞서 살펴본 바와 같이 현재 많은 다양한 서비스가 모바일 폰을 통해서 제공되고 있으며, 향후 더 많은 서비스가 BcN 기술의 발달과 더불어 모바일 폰을 이용하여 제공 되어질 전망이다. 우리는 이 모바일 폰 서비스 중 일반 휴대형 정보기기와는 차별화 되었다고 보여지는 모바일 RFID와 모바일 헬스케어, 위치기반 모바일 등에서 야기되어질 수 있는 개인정보보호의 문제를 가상 시나리오를 설정하여 그 과정 과정에서 개인정보보호의 잠재적 위협을 분석해 본다.

5.2.1. 모바일 RFID

모바일 폰에 RFID가 심겨진 이 기술의 서비스는 기존 RFID의 보안 이슈를 그대로 안고 온다. 여기에 모바일 폰의 특성, 이를테면 수동적 RFID에 비해 기지국이나 통신사와의 양방향 통신이 가능하다는 점으로 인해 추가적인 보안 문제점이 야기되어진다. 인증정보의 송신이 대표적인 예라 할 수 있으며, 또한 위치추적성은 여전히 골칫거리이다.

프라이버시 보호를 위해서 안전한 익명 프로토콜이 제공되어져야 한다. 이는 익명성 뿐만 아니라 추적 역시 가능해야 한다. 그리고 암호화 기법이 필요한데, RFID의 저전력, 소용량의 특성을 감안하여 초경량의 안전한 암호 모듈의 개발이 절실하다.

모바일 RFID는 크게 두 가지로 나누어 볼수 있다. 하나는 모바일 폰에 RFID 태그가 부착되어 신분증의 용도 또는 현관 열쇠, 지불 및 결제 등의 용도로 이용하는 방식이며, 또 다른 하나는 모바일 폰이 RFID 리더기 역할을 하여 영화 포스터에 부착된 RFID 태그를 읽어 정보 서비스를 이용하는 방식처럼 다른 RFID 태그를 읽어들이는 것이다. 향후는 이 두 가지 경우가 복합된 형태 즉, 모바일 폰이 RFID의 태그가 부착됨과 동시에 리더기의 역할도 같이 하는 방향으로 움직일 전망이다.

이에 따라, 모바일 RFID 리더기의 이동성으로 인한 개인정보보호 침해와 이동통신 및 무선인터넷 환경으로 인한 정보 노출의 위협이 예상되며, 모바일 RFID 서비스의 불법적 이용 및 RFID 태그 정보의 위변조가 가능하므로, 개인정보 침해 및 노출의 위협을 최소화하기 위해 모바일 RFID 태그 및 단말기, 응용 서버간 안전한 서비스를 제공하기 위한 새로운 보안 기술이 필요하다.

위 두 가지 경우를 나누어 살펴보도록 하자.

1) 모바일 폰 + RFID Tag

모바일 폰에 RFID 태그가 내장된 형태로서, 이경우

내장된 RFID 태그는 보통 일반적인 RFID와 같은 기능을 한다. 따라서, 이에 대한 개인 정보의 위협도 일반 RFID와 유사하다.

① 위치기반 위협 (location threat)
특정 장소에 숨겨진 리더는 두가지 유형의 프라이버시 위협이 발생한다. 첫번째는, RFID 태그를 부착한 물건을 들고 가는 개인에 대해 추적이 가능하고, 두번째는 태그가 부착된 물건의 위치정보가 알려질 수 있다.

② 고유정보에 관한위협 (Preference threat)
태그에는 개인 정보나 고유의 ID와 같은 정보가 기록되어 있다. 이러한 정보를 이용하여 개인 정보를 알 수 있다.

③ 거래에 관한 위협 (Transaction threat)
모바일 RFID를 가지고 있는 사용자가 어떤 물건에 대해 구매를 할 때, 태그안의 정보뿐만아니라 계좌번호나 신용카드정보 같은 추가적인 정보가 전달된다. 이러한 정보가 누출되면 개인정보 및 금전적인 문제가 발생할 수 있다..

④ 해결 방법

- Sleeping; 프라이버시 침해를 해결하기 위한 가장 확실한 방법은 RFID 태그를 물리적으로 제거하거나, RFID 태그 기능을 kill 명령을 이용하여 정지시키는 것이다. 언뜻 보기에는 태그를 정지시키는 것이 매우 유용한 것처럼 보인다. 하지만 많은 RFID 응용 서비스에서는 개인이 RFID 태그 부착 물품을 소유한 이후에도 계속 서비스가 이루어져야 하기 때문에, RFID 태그 기능 정지만이 최상의 프라이버시 보호 방법은 아니다. Sleeping 태그는 killing 태그와 비슷하다. 하지만 활성화되지 않는 태그는 "wake" 명령을 통해 활성화 시킬 수 있다. Sleeping 태그 방법은 어떤 리더가 활성화 시킬 수 있는지를 관리해야 하기 때문에 현실에서는 사용하기가 쉽지않다.
- 태그 패스워드; 기본적인 RFID 태그는 PINs 이나 패스워드를 확인하기 위한 저장 공간이 충분하다. 태그는 정당한 패스워드를 받을 때만 중요한 정보를 전송한다. 그러나 리더가 태그의 ID를 알고있지 않으면 태그에게 전송할 패스워드를 알지 못한다는 모순이 발생한다. 즉, 모든 리더기가 사전에 모든 태그의 ID를 알고 있어야 한다는 것이다.
- 익명태그(Tag pseudonyms); 모든 태그는 익명들의 집합을 소유하고, 그 익명을 매번 리더의 쿼리에 대해서 다른 값을 선택하여 태그의 ID로 사용한다. 정당한 리더는 태그와의 모든 익명들을 공유하고 있기 때문에 태그를 인증할 수 있다.
- 암호화 태그의 ID를 암호화하는 방법은 프라이버시를 보호하여 좋은 방법으로 보이지만, 암호화된 ID가 새로운 다른 ID가 되기 때문에 프라이버시를 해결하는 방법으로는 적당하지 않는다. 또한 암호화 키를 관리해야하는 문제도 발생한다. 무엇보다도 비용문제 때문에 값싼 태그에는 적용하기가 어렵다.
- 해쉬 기반 접근 제어(Hash-Lock Access Control)
해쉬 기반 접근 제어는 태그에 대한 접근 제어 기술이다. 접근 제어는 허가된 사용자만이 태그를 접근할 수 있도록 하기 위한 방법을 말한다. 태그를 잠그기 위하여, 리더는 난수 형태의 키를 해쉬하여 데이터베이스에 저장하고 이를 태그의 메타 아이디로 사용한다. 그리고 리더는 태그에게 메타 아이디를 보내고 태그는 이를 저장하고 잠김 상태가 된다. 태그의 잠김 상태를 풀기 위하여, 리더는 태그에게 잠김을 풀려고 한다는 메시지를 보낸다. 태그는 자신이 저장했던 메타 ID를 리더에게 보내고 리더는 데이터베이스에서 메타 ID에 해당하는 ID와 자신이 생성했던 키를 가져온다. 리더는 태그에게 키를 보내고 태그는 이 키를 해쉬해서 나온 값이 자신의 메타 ID와 동일하다면 태그는 잠김 상태에서 빠져나와 주위의 리더에게 반응하게 된다.

2) 모바일 폰 + RFID 리더기

이 경우는 크게 두 가지 경우로 나누어 생각할 수 있다. 리더기 기능을 가진 사용자가 공격자가 되어 RFID 태그를 가진 사람의 프라이버시를 침해하는 경우와 반대로 리더기 기능을 가진 사용자가 다른 태그를 읽어들이고 서버와 통신하면서 자신의 프라이버시를 침해당하는 경우를 생각할 수 있겠다.

① 다른 사람의 프라이버시를 침해하는 경우
모바일 RFID를 가지고 다니는 사람은 정보의 무

한적인 수집이 가능하다. 왜냐하면, 리더를 가지고 있는 사람은 모바일 RFID를 가지고 태그를 읽을 수 있는 어떠한 장소로 이동하고, 리더를 가지고 있는 사람이 원하면 언제나 태그를 읽어들여 태그의 정보를 수집할 수 있기 때문이다. 이에 대한 대응방안으로는 상점에서 물건에 대한 태그에 리더가 읽을 수 있는 범위를 제한한다. 그러면 상점에 있는 물건에 대한 정보는 상점 안에서만 읽을 수 있고, 멀리 있거나 모르는 곳에서 상품에 대한 정보를 알 수 없게 한다.

② 자신의 프라이버시를 침해 당하는 경우
모바일 RFID를 가지고 다니는 사람의 위치 추적이 가능하거나 지속적인 관측이 가능하다. 모바일 RFID를 가지고 있는 사람이 무선통신을 사용하여 모바일 RFID 서비스를 사용하게 되면, 모바일 RFID 서비스 제공자가 모바일 RFID를 가지고 있는 사람의 위치를 알 수 있다. 이에 대한 대응방안으로 태그를 읽을때마다 리더의 ID를 한번만 사용한다. 즉, 위에서 설명한 해쉬기반 접근 제어와 같은 방식을 사용하여 매번 랜덤한 ID를 사용한다.

모바일 RFID 서비스 사용시 추가적인 정보의 이동에 대한 보안이 필요하다. 예를들어, 어떤 물건에 대한 구매시 그 물건에 대한 태그정보와 함께 추가적으로 계좌정보나 신용카드번호 같은 정보가 그대로 전달되면 문제가 발생할 수 있다. 특히 리더를 가지고 다니는 사람이 공격자로서 시스템의 정보를 읽을 수 있으면 심각한 문제가 된다. 이에 대한 대응방안으로 태그 정보 이외의 전송되는 정보에 대해서 암호화를 하여 중간에 도청이 발생하여도 원래의 값을 알지 못하게 한다.

5.2.2. 모바일 헬스케어

모바일 헬스케어 서비스 분야는 현재 뿐만 아니라 향후에 있어서도 프라이버시적 관점에서 상당히 중요한 부분으로 자리 메김 할 것으로 보여진다. 그 이유는 예를 들어, 당뇨병 환자의 경우와 같이 응급한 경우가 아닌 만성 질환의 경우에는 입원하지는 않아도 하루에 몇번씩 혈당 체크며 투약 등을 본인이 직접 시행해야 하고, 그 결과 및 추이 상황을 자신의 주치의가 알고 있어야 한다. 뿐만 아니라, 이런 환자는 언제 응급 상황에 처해질 지 모르는 일이므로 항시 주위의 관심 속에 살고 있다. 이 경우, 모바일 헬스케어 서비스를 이용하면 더 없이 편리하고 환자에게 있어서는 안전할 것이다. 검사 결과가 위험한 상황이면 그 결과가 바로 주치의에게 알려져 바로 치료책을 받을 수 있기 때문이다. 정말 응급한 경우에는 119 응급 구조대와도 바로 연계되는 서비스 역시 가능할 것이다.

이런 환자의 편의와 안전 측면에서 향후에는 필히 대중적인 인기를 끌 서비스 분야라는 것은 자명한 일이다. 하지만, 이와 관련하여 역시 우려되는 측면은 프라이버시 문제이다. 의료 정보는 개인의 아주 민감한 정보임과 동시에 의학적 연구 및 공공의 의료 안전을 위해 공개 역시 되어야 하는 정보이기 때문이다. 어떤 질환으로 치료 받고 있는 환자들의 임상 자료들은 차후 약품이나 의료 시술 개발에 중요한 통계 및 분석 자료가 될 수 있으며, 전염병 환자의 경우 보건소나 당국에 신고되어 일반인들과 격리되어지고 더 이상 질환이 전파되는 것을 막아야 하기 때문이다. 하지만, 이 과정에서 개인의 프라이버시가 노출되는 경우가 허다하며, 이런 의료 정보 시스템을 모바일 헬스케어 서비스를 이용한다면 프라이버시 침해의 위협은 더 커질 것이다.

우선 이런 위협은 어떤 것이 있을 수 있는지 가상 시나리오를 통해서 분석해 보도록 한다.

<가상 시나리오- 50세 OOO환자씨는 분당 OO병원에서 당뇨를 모바일 헬스케어로 통해 원격진료를 받는다. 모바일을 통하여 매일 측정해서 의료 자료가 병원으로 전송되어 지는데, 그 자료는 자신의 모바일 폰에 저장되었다가 병원에 보내진다. 검사 수치가 정상이면 하루에 한번 정해진 시간에 전송 되고, 비정상 수치 즉, 응급을 요하는 수치면 바로 전송되어 의사에게 바로 알려지게 되어 있다. OO월 OO일 이환자씨는 당뇨 측정을 한 결과, 비정상치로 측정되어 바로 병원으로 자료가 보내어졌다.>

1) 모바일 헬스케어의 프라이버시 위협

① 시스템 상에서의 오류
모바일를 이용하여 잘못된 업데이트, 공격자에 의한 바이러스 등을 통해 시스템 오류를 일으켜 저장된 정보가 누출되는 사고가 발생하는 등, 프라이버시가 위협 받을 수 있다. 데이터의 무결성에 대한 문제가 생길 수 있으며, 이것은 환자의 생명에 치명적인 위해를 가할 수도 있다.

② 서버에 자신의 정보 저장

모바일에서 의료자료가 병원으로 전송되어 병원 측 서버에 계속 저장되어 진다. 이 자료가 유출되어 진다면 프라이버시가 위협 받을 수 있다.

③ Public DB
의료 연구 및 통계학적 자료를 위해 의료 DB가 공개 되어질 수 있는데, 이때 불필요한 정보까지 유출 가능하여 프라이버시가 위협 받을 수 있다.

④ 전송상의 문제점
의료 자료가 모바일에서 병원의 담당의사에게 전해질 때까지 전송 상에서 공격자가 침입하여 데이터를 삽입, 변조, 삭제 등을 일으킬 수 있다. 의사와 환자의 인증 문제가 있을 수 있다. 이는 프라이버시 측면 뿐만 아니라 환자의 생명과도 관련된 중요한 문제이다.

⑤ 서버 스푸핑 공격
병원이 아닌 곳 예를 들어 의약 제품을 파는 회사가 서버인척 하여 접근을 하여, 이메일이나 각종 수단으로 자 회사의 제품을 광고할 수 있게 되어 프라이버시침해를 받을 수 있다.

2) 모바일 헬스케어의 프라이버시 침해 해결 방법

① TPM(Trusted Platform Module) chip 탑재
Trusted hardware module은 강도 높은 사용자 인증과 기기 인증을 제공하는 것이다. 따라서, TPM chip은 키 암호 및 디지털 인증을 위한 안전한 저장 공간을 제공한다. 즉, 서비스의 보안과 무결성은 소프트웨어 만으로는 충분치 않기 때문에 하드웨어 기반의 인증을 위해 작은 칩을 기기에 탑재하는데, 이것은 강도 높은 플랫폼 인증을 수행할 수 있다. 시스템이 잦은 공격을 받으면 플랫폼 구성상에 허가되지 않은 변화가 발생하여 디바이스나 그것의 컨텐츠가 오용되고, 또는 불법적인 네트워크 접근이 이루어질 수 있다. 이러한 상황에서도 TPM 칩이 탑재된 디바이스는 플랫폼 무결성을 보장할 수 있게 하는 것이다.
하드웨어에 저장되기 때문에 외부 소프트웨어 공격이나 물리적인 도난에 대해 더 안전하다.

② DB 보안 - 접근 제어와 암호화
DB 보안은 접근 제어를 통한 시스템적 측면의 보안과 DB에 담긴 정보 자체의 암호화를 통한 보안, 이 두가지가 동시에 이루어져야 할 것으로 보인다. 의료 자료는 민감한 자료이므로 내부 관리자에 의한 정보의 유출을 막기 위해서 자료의 암호화가 반드시 필요하다. 의무 기록은 담당 의사와 간호사만이, 원무 기록은 원무과 직원만이 복호화가 가능하게 되면 개인정보의 노출에 대해 안전하게 될 수 있다.

③ PPDM(Privacy Preserving in Data Mining)
데이터 마이닝은 사용자와 연관된 데이터들의 상관관계를 인공지능 기법을 이용하여 명확히 밝혀서 이를 사용자에게 제공해주는 기술이다. PPDM (데이터 마이닝에서의 프라이버시 보호 기술)이라는 것은 데이터 마이닝의 최종 목표인 또 다른 정보 추출에 중점을 둠과 동시에 참여자들의 프라이버시 보호를 위해 데이터를 가공 처리한 후에도 데이터를 변화시키지 않고 데이터 마이닝을 수행한 결과와 동일한 결과를 도출하게끔 하는 기법이다.

④ 메시지 인증 코드(Message Authentication Code : MAC)
데이터 인증을 위한 메시지 인증 코드(Message Authentication Code : MAC)를 이용하여 데이터가 삽입, 변조, 삭제 등을 막을 수 있고, 사전에 키를 공유하고 있는 송·수신자간에 인증이 확인될 수 있다. 이로써 환자는 안심하고 의사의 처방을 따를 것이며, 의사 역시 환자의 상황을 정확히 판단하여 적절한 처방을 내릴 것이다.

⑤ 양방향 인증
서버의 스푸핑 공격 및 가장 공격을 막기 위한 필수적인 사항이다. 위에서 제시한 인증에 관련한 서버 스푸핑과 같은 문제들은 현재 인증 시스템이 양방향이 아닌 단방향 시스템이기 때문이다. 즉, 단말에 대한 인증은 있지만 서버에 대한 인증 과정은 없다. 따라서 가장 공격 및 DoS 공격, 서버 스푸핑과 같은 인증과 관련한 대안책으로 양방향 인증은 현재 필수적이면서 시급한 과제라고 할 수 있겠다.

5.2.3. 위치기반 모바일

안전한 상호인증이 제공되지 않는다면, 능동적인 공격자가 임의로 가상의 더미(dummy) 개체를 형성하여 자신이 정당한 서비스 제공자임을 혹은 LBS 시스템임을 가장하는 중간공격이 가능하게 된다.

위치기반 서비스 시스템에서 요구되는 인증은 크게

세 곳에서 발생한다. 사용자와 서비스 제공자 간의 인증 절차, LBS 시스템과 서비스 제공자간의 인증 절차 그리고 LBS 시스템과 위치 획득 장비간의 인증 절차가 그것이다. 하지만 현재의 LBS 시스템에서는 단말기와 위치정보 서비스 제공자 사이의 신뢰관계를 보증하기가 어렵다. 즉, 현재의 LBS 시스템에서는 단말기가 자신의 ID와 인증서를 포함한 메시지를 위치정보 서비스 제공자에게 전송하면, 위치정보 서비스 제공자는 전송받은 메시지를 검증하지 못하며 단말기는 바로 자신의 위치정보를 위치정보 서비스 제공자로 전송하여 서비스를 시작하는 방식으로 개인정보 및 프라이버시를 보호할 수가 없다. 이러한 문제는 PKI 기반의 전자서명 기술을 통해서 극복할 수 있다. 전자서명은 메시지(위치정보)에 대한 인증과 사용자에 대한 인증을 제공해 준다. 메시지(위치정보)에 대한 인증은 서명된 전자서명을 검증함으로써 확인될 수 있고, 사용자 인증은 전자서명 기반 키 교환 프로토콜에서 형성된 키를 확인하는 과정에서 달성될 수 있다.

한 때 삼성의 계열사와 직간접적으로 관련을 맺고 있는 사람끼리 자신도 모르는 사이에 휴대전화 '친구찾기(위치추적)' 서비스에 가입이 되고 그것을 통해 누군가로부터 감시를 받은 피해사례가 있었다. 이 뿐만 아니라 GPS칩 내장 휴대폰으로는 도감정의 위험도 있다. 복제폰과 복제 대상이 된 휴대전화가 같은 기지국의 한 중계기 범위 내에 있으면 도감청이 가능하여 사생활침해 및 인권침해의 우려가 있다.

다음은 모바일 위치기반 서비스에서의 가상 시나리오를 설정하여 개인정보 위협을 분석해 보았다.

1) 자신의 위치를 요청할 경우

000씨는 그 전날 폭음을 하여 깨어보니 자신도 모르는 외딴 곳에 쓰러져 있었다. 인근에 돌아다니는 사람도 없었고, 택시 및 건물도 보이지 않았다. 000씨는 집에 가기 위해 단말기로 위치기반 서비스를 이용하여 자신의 위치를 요청했다.

① 서버에 저장된 자신의 위치 노출

위치정보 서비스 제공자의 서버에서는 서비스를 요청한 사람의 위치 정보가 저장되어 있다. 따라서 서버단에서의 보안상 취약함으로 인해 해킹을 당하거나 내부자의 관리 소홀 및 내부자 공격으로 개인의 위치 정보가 노출 되어질 수 있다. 이를 위해서는 앞 1절에서 언급한 서버단의 DB 보안 대책을 적용하면 해결 가능할 것이다.

② 가장 공격

서버가 공격자가 되는 상황이나 혹은 공격자가 서버를 가장하는 공격을 예로 들수 있다. 이때 공격자는 사용자에게 틀린 위치 정보를 줄 수 있다. 그리고 서버에서는 제 3자가 위치를 알고 싶은 사용자인 척 행동을 할 수 있으므로, 사용자의 인증이 필요하다. 이것은 양방향 인증 시스템으로 방어 가능하다.

2) 본인의 위치를 제 3자에게 제공하는 경우

xx씨는 남편 yy 씨가 회사에서 밤늦도록 돌아오지 않아 위치기반 서비스를 이용하여 위치를 파악할 수 있었다.

① 정당한 사람 내에서 사생활 침해 문제

위치 추적이 꼭 필요할 때도 있지만, 시시때때 계속해온다면 사생활 침해가 될 것이다. 한 때 일본에서 유행한 엔젤폰 처럼 아이들이 유괴되는 것을 두려워한 부모들이 이런 서비스를 이용할 수는 있으나, 이 때에도 아이들의 프라이버시는 보장할 수 없다는 문제점을 갖고 있었다.

② Replay / 가장 공격

사용자를 가장한 공격자에 의해 범죄에 악용될 수 있다. 이때 공격자는 집에 누가 있는지 또는빈집인지 아닌지를 확인하여 범죄를 저지를 수 있으며, 유괴 또한가능하다. 따라서, 여기서는 상호 인증이 상당히 중요하며, 상호 인증 뿐만이 아니라 제 3자와 본인의 상호 동의하에 서비스가 이뤄져야 할 것이며, 현행적으로 위치 정보를 알려달라는 질의가 왔을 때에도 한번의 인증으로 서비스 이용이 가능한 적절한 횟수 또는 기간을 정하여 질의에 대한 재인증 및 응답이 이루어져야 한다. 만약 위치정보 요청 프로토콜이 허술하다면 replay 공격이 가능하여 사용자를 가장하기가 보다 쉬워진다. 이때에는 타임스탬프를 메시지에 첨가하면 방어 가능하다.

5.2.4. 모바일 지급결제

모바일 결제 서비스는 개인 휴대전화나 PDA등 이동통신기기를 사용하여 자금이체나 상거래 대금결제 등에 이용하는 서비스를 뜻한다. 이 서비스는 휴대 단말기를

통해 거래대금을 지불하는 휴대폰 소액 결제에서 휴대폰에 스마트 칩을 장착한 모델로까지 다양하게 변화하고 있다.

1) 휴대폰 소액 결제 서비스에서 취약점 분석

휴대폰 소액 결제 서비스는 실질적인 서비스 주체가 모바일 결제 전문 업체이지만 이동통신업체의 지불 시스템에 의존도가 매우 높은 것이 특징이다.

그러나 휴대폰 소액 결제 방식은 보안이 취약하다는 단점이 있다. 예를 들어 온라인 쇼핑몰에서 상품을 구매할 때, 구매에 따른 인증번호가 이동통신업체의 SMS를 통해 전달되는 것 이외 별도의 보안 인증 절차가 이루어지지 않는다. 따라서 휴대폰을 공유할 수 있거나 주위에서 쉽게 접할 수 있는 가족 구성원들일 경우, 충분히 악용될 소지가 많다. 인터넷 쇼핑 후 지급 결제 수단으로 딸들이 엄마의 휴대폰을 이용할 수도 있는 것이다. 때문에 소액 결제 서비스는 이러한 간순한 보안 인증 절차를 이유로 하여 소액 결제만을 치중하고 있다.

이런 모바일 폰을 이용한 지급 결제 수단은 일반 전자 상거래에 비해서 또 다른 프라이버시 침해를 받을 수 있다. 모바일 스팸 메일이 바로 그것이다. SMS를 통한 인증 정보의 전달을 위해 사용자들은 본인의 핸드폰 번호를 입력해야 하고, 이것은 서비스 제공자의 서버에 남게 된다. 이런 서비스 제공 업자들의 서버 보안 취약은 사용자들의 개인 정보를 노출시켜 모바일 폰 스팸 메일에 사용자들을 시달리게 하는 것이다.

2) 금융기관 호스팅을 통한 모바일 결제 서비스에서 취약점 분석

금융기관 호스팅을 통한 모바일 결제 서비스는 이동통신업체와 금융기관이 제휴한 형태로써 금융기관은 이동통신업체의 컨텐츠 제공자 역할을 하고 있다. 이 서비스를 통해서 계좌 조회나 자금 이체와 같은 금융 서비스가 제공되고 금융기관은 자체의 온라인 뱅킹 서비스에 모바일 접속을 가능하게 한 형태이다. 금융기관 호스팅을 통한 모바일 결제 서비스도 이동통신사에 따라 수행 방법이 다르다. 어떤 서비스는 결제수단으로써 단순히 휴대폰을 이용하여 인증하는 방식을 택하고 있는데 이는 보안상의 문제를 해결 하는 데에 어려움이 있다. 왜냐하면 위에서 언급했듯이 인증을 위해서 계좌번호, 계좌비밀번호와 주민등록번호를 입력하는 식이기 때문에 개인정보 누출 시 쉽게 타인 또한 접속이 가능하기 때문이다. 대신에 스마트카드를 도입하면 보안상의 문제를 해결 할 수 있고 온라인 뿐 아니라 오프라인 상에서도 결제가 가능해 진다.

3) 스마트카드를 도입한 모바일 결제 서비스에서 취약점 분석

스마트카드를 도입한 모바일 결제 서비스는 기존의 마그네틱 띠에 저장된 사용자 정보에 의존하는 플라스틱 카드와는 달리, 내부에 정보 저장 및 수정이 가능한 IC칩을 탑재한 카드를 이용하여 카드 하나에 여러 가지 필요한 지급 결제기능들을 모아 만든 스마트카드와 모바일 금융 서비스의 결합된 형태이고 이동통신사와 금융기관이 서로 대등관계로 발전한 형태이다. 또한 스마트카드를 도입함으로써 보안이 우수해지고 다양한 금융 서비스를 제공할 수 있다.

하지만, 스마트 카드를 도입한 모바일 폰은 스마트 카드의 프라이버시 위협을 그대로 가질 수 있다. 스마트 카드는 tamper-resistant한 성질 때문에 보안의 우수성이 인정되고 있긴 하나, 외국의 프라이버시 침해 사례를 보더라도 완벽할 수는 없는 것이다. 스마트 카드 자체의 문제만으로 야기되어지는 문제는 거의 없으나, 스마트 카드 리더기를 가장하여 생기는 문제는 심각하다. 공격자는 가짜 리더기를 설치하여 스마트 카드 칩 내에 있는 개인 신상에 관한 정보를 모두 볼 수 있다. 이에 대한 대응책으로는 사용자 인증 뿐만 아니라 서버 인증, 즉 양방향 인증을 통하여 서버를 인증한 후에야 칩내의 정보를 서버가 볼수 있도록 하는 것이다. 이를 위해서 칩내의 정보를 서버의 키로 암호화 시켜 놓는 방법도 생각해 볼 수 있다.

Ⅵ. 결 론

우리나라는 정보 통신 인프라를 기반으로 개인의 인터넷 생활화, 디지털 경제로의 전환, 전자정부 구축이 가속화되고 있다. 또, 2004년부터 BcN(Broadband convergence Network, 광대역 통합망)이라는, 통신, 방송, 인터넷이 융합된 품질보장형 광대역 멀티미디어 서비스를 언제, 어디서나, 끊김없이(seamless) 안전하게 광대역으로 이용할 수 있는 차세대 통합 네트워크를 추진해 오고 있는데, 이는 개방형 플랫폼(Open API) 기반의 통신망과 네트워크 단말에 구애받지 않고 유비쿼터스 서비스 환경을 지원하는 통신망이다. 이런 맥락에서

모바일 폰과 같은 이동성 휴대형정보기기가 우리의 일상에서 차지하는 비중이 나날이 커져가고 있다.

이런 기술적인 진보로 유비쿼터스 시대가 점점 가까워져 보다 편리하고 효율적인 생활을 영위할 수 있는 것과는 반대로 한 가지 크게 문제시 되는 점은 프라이버시 침해도 그와 비례하여 증가한다는 것이다. 즉, 프라이버시에 관한 주요한 권리인 자기정보결정권, 자기정보통제권을 보장하지 못하는 기술 환경이 확장 되어 가고 있다. 언제 어디서나 네트워크에 연결 가능하다는 것은 24시간 자신의 일거수 일투족이 감시되고 기록되어 질 수 있다는 것을 의미한다. 자신이 원하지도 않은 정보들이 감시되고 저장 되어져 이렇게 다른 사람에 의해 오/남용 되어질 수 있는 것이다.

이런 프라이버시의 침해도 BcN과 같은 기술 환경의 발전과 더불어 나날이 지능화 되고 복잡해 졌다. 하나의 기기로 여러 서비스를 연계하여 이용하면, 다른 것은 보안상 전혀 문제가 없다 하더라도 하나가 헛점이 뚫리면 전혀 문제가 되지 않았던 다른 부분도 역시 문제를 일으킬 소지가 많다. 따라서, 이에 대한 방어책으로서 '통합관리시스템'은 필수 요건이라 할 수 있다.

본 고에서 연구한 모바일 폰은 단순히 이동성만을 의미하는 전화기가 아니다. 각종 서비스를 제공할 수 있는 최첨단 기술이 집적된 하나의 종합 예술이다. 이런 예술품의 진가는 '통합관리시스템'을 주축으로 하여 프라이버시가 침해 당하지 않는 안전한 환경 하에서 제대로 발휘될 수 있다. 앞으로 유비쿼터스 시대의 현실화와 그로 인해 프라이버시가 중요한 이슈가 되고 있는 상황에서, 기술과 경쟁력의 우위는 그 기기에 얼마나 우수한 프라이버시 보호기술이 탑재되어 있느냐에 달려 있을 것이다.

참고문헌

[1] 개인정보보호를 위한 기술개발 및 기술정책에 관한 연구, 한국전산원, 수탁기관: 고려대학교, 2004. 9

[2] 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 개정안, 정보통신부, 03, 31, 2006

[3] KBS뉴스 2005.1.7[뉴스타임] [유비쿼터스 ⑤차세대 성장동력'2만 불 시대

[4] WS-I, http://ws-i.org

[5] Ray Wagner, "Act Now to Help Shape Web Services Security Scenarios,"Gartner, Mar. 2004

[6] "Handbook of Privacy-Enhancing Technologies", by J. Huizenga, 2003

[7] General overview of standards for privacy of indivisuallyidentifiable health information [45 CFR Part 160 andSubparts A and E of Part 164

[8] HIPAA(Health Insurance Portability and AccountabilityAct)-[기반보호 동향], 2003.2.27/기반보호팀

[9] 개인정보분쟁조정위원회, "APT개인정보가이드라인제정방안", 2003

[10] 미국의 전자정보공개법 제정과정의 교훈, 명승환 (한국전산원 정보화연구실 위촉 선임연구원)

[11] 한국사이버범죄백서 - 한국사이버감시단, 2001

[12] 오돈성외, '차세대 이동통신 기술 및 표준화 동향', ETRI 전자통신동향분석 제21권 제3호, 2006년 6월

[13] 박석지외, '이동통신산업 동향분석 및 발전전망', ETRI 전자통신동향분석 제19권 제3호, 2004년 6월

[14] 윤성임외, '차세대 이동통신 서비스 연구', ETRI 전자통신동향분석 제21권 제3호, 2006년 6월

[15] 안재영외, '차세대 이동통신 표준화 및 기술개발 동향' ,ETRI 전자통신동향분석 제19권 제3호, 2004년 6월

[16] 아이뉴스24, '[4G포럼]삼성전자의 4G는 번개... 3G보다 20배 이상 빨라' 2006년 08월 31일

[17] 한국표준협회 http://www.it-standards.or.kr/

[18] 한은영외, '모바일 위치기반 서비스 표준화에 관한 연구', 한국GIS학회 춘추계학술대회 pp. 256~260

[19] 디지털타임스, '이통3사, 위치기반 서비스 두고 「제 2라운드」 위치정보보호법 시행 앞두고 서비스 확대 `총력전'', 2005.07.19

[20] 안병익, '위치기반 서비스 (LBS) 기술', 정보통신연구진흥원

[21] 김용운외, '모바일 RFID 서비스 네트워크 구조 및 표준화 현황', TTA Journal No. 102, 2005

[22] 김형준, '모바일 RFID 기술 국제 표준화 현황', http://www.krnet.or.kr

[23] 정병주, 'u-Healthcare 서비스 현황과 과제', 한국전산원, 2005.12.16

[24] 박래웅, 'Ubiquitous Health Care 발전방향', 대한병원협회지, 5,6월호, 2005

〔25〕 전자신문, '바이오폰 선점경쟁 시동', 2004.03.18
〔26〕 디지털타임스, '모바일TV머잖아 황금시장 세계기업 잰걸음음성매출 한계 극복 대안오렌지 · 보다폰 · SKT 두각', 2005.10.19
〔27〕 디지털타임스, 'ETRI, 모바일 웹 표준화 추진', 2006.06.22
〔28〕 이원석, 전종홍, 'W3C(World Wide Web Consortium), 모바일 웹 표준화를 의한 모바일 웹 이니셔티브(Mobile Web Initiative) 동향'
〔29〕 모바일 디바이스를 위한 종합 보안 방역, www.trendmicro.co.kr/product/prditm_pds_download.asp?filename=mobile_security_kr.pdf
〔30〕 Microsoft, 'Bluetooth 휴대폰을 통한 무선 공격 예방'
〔31〕 한국정보보호진흥원, 와이브로 보안기술 해설서, 2006. 8
〔32〕 이경철, 무선인터넷 서비스 시대, ㈜인프라벨리 기고문, 2006. 2
〔33〕 이경철, 이동통신서비스의 진화, ㈜인프라벨리 기고문, 2006. 3
〔34〕 홍대영외, 2.3GHz 휴대인터넷 기술의 국내 표준화, TTA Journal No. 92, 2004
〔35〕 김현곤외, 3GPP와 3GPP2의 Core Network 표준화 동향과 전망, LG전자㈜, 2003
〔36〕 이명수외, 무선 브로드밴드 산업동향, 전자부품연구원, 2006. 2

〈著者紹介〉

박 현 아 (Park Hyun-A)
학생회원
2003년 2월 : 고려대학교 수학과 졸업
2005년 2월 : 고려대학교 정보보호대학원 석사
2005년 3월~현재 : 고려대학교 정보경영공학전문대학원 박사과정
관심분야 : 암호프로토콜, PET 기술(익명성 연구, DB 프라이버시), IDM

최 재 탁 (Choi Jae Tark)
학생회원
2002년 2월 : 충북대학교 수학과 졸업
2004년 8월 : 한국과학기술원 수학과 석사
2005년 3월~현재 : 고려대학교 정보경영공학전문대학원 박사과정
관심분야 : 암호프로토콜, 암호 이론

이 동 훈 (Lee Dong Hoon)
정회원
1983년 8월 : 고려대학교 경제학사
1987년 12월 : Oklahoma University 전산학 석사
1992년 5월 : Oklahoma University 전산학 박사
1992년 8월 : 단국대학교 전자계산학과 전임강사
1993년 3월 ~ 1997년 2월 : 고려대학교 전산학과 조교수
1997년 3월 ~ 2001년 2월 : 고려대학교 전산학과 부교수
2001년 2월~현재 : 고려대학교 정보경영공학전문대학원 교수
관심분야 : 암호프로토콜, 암호이론, USN 이론, 키 교환, 익명성 연구, PET 기술

임 종 인(Lim Jong In)
정회원
1980년 2월 : 고려대학교 수학과 졸업
1982년 2월 : 고려대학교 수학과 석사
1986년 2월 :고려대학교 수학과 박사
1986년 9월 ~2001년 1월 :고려대학교 자연과학대학 정교수
2001년 2월 ~ 현재 : 고려대학교 정보경영공학전문대학원 원장, 고려대학교 정보보호기술연구센터 센터장
관심분야 : 암호 이론, 암호 정책, PET 기술