휴대폰 사용자의 개인정보 보호 의식 연구

정회원 이 혜 경*

A Study of Privacy Protection Awareness of Mobile Phone Users

Hae-kyung Rhee* *Regular Member*

요 약

무선 통신 기술이 모바일 기기들에 속속 도입됨에 따라 개인의 프라이버시도 침해 당할 가능성이 높아지고 있다. 그한 예로 오스카 수상식에 참석한 패리스 힐튼의 스마트폰이 스웨덴 해커들에 의해 해킹 당하는 일이 발생했다. 본논문에서는 어떤 종류의 개인정보들이 침해 사건처럼 해커들에 의해 노출될 수 있는지 탐구하였다. 본 연구를 수행하면서, 모바일 기기의 플래시메모리에 어떤 종류의 정보가 저장되어 있는지 검사하기 위한 기술적인 분석은 기기마다 독점적인 방식으로 제조되었기 때문에 기술적으로 거의 불가능임을 알게 되었다. 저장된 내용을 검사하기 위한 범용 도구를 발견할 수 없었다. 이러한 기술적인 어려움을 인식함에 따라, 개인정보에 관련된 의식 수준을 알기 위해 설문지에 의한 조사를 실시하게 되었다. 설문조사는 가장 정평이 나있는 온라인 조사 사이트 월드 서베이에서 시행했다. 응답 결과에서 열명 중 아홉 명이 개인 주소와 같은 정보를 저장한다는 놀라운 사실을 발견하였다. 전화번호, 성명, 개인계좌번호와 같은 정보들도 저장한다는 것이 밝혀졌다.

Key Words : Mobile privacy, Personal privacy, Mobile devices

ABSTRACT

Adoption of wireless communication facilities in mobile devices leads to increased vulnerability in individual privacy. One of such cases was discovered when a smart mobile phone of Paris Hilton at Oscar Award Ceremony was hacked a Swedish group of hackers. In this study, I wondered what sort of personal information could be exposed to hackers in such cases. In the course of survey, it was recognized that technical analysis of flash memory in mobile devices to check what kinds of data are stored there is technically almost impossible, since they are usually built in a proprietary manner. No generic tools could apply to discover their contents. Having recognized technical difficulties, it was inevitable to resort to a questionnaire survey to see awareness level with regard to personal privacy. We collected response from three hundred respondents by posting the questionnaire at World Survey on-line research site. What we have discovered was quite astonishing that even personal residence registration numbers have been found from nine of every ten respondents. Other data revealed include phone numbers, names, and personal bank accounts.

Ⅰ. 배 경

개인정보의 유출 및 도용은 현재 정보화 사회가 가져다 준 대표적인 역작용이다. 하루가 멀다 하고 발생되는 개인정보 유출 사건은 더 이상 새로운 현상이 아니라 일상이 되다시피 했다. 특히 주민번호의 도용 등으로 인해 갖가지 피해가 속출하고 있으나 이를 막기 위한 방법은 그리 믿음직스럽지 못하다. 최근 정부당국은 개인정보 침해와 주민등록번호의 남용을 막기 위해 대체 수단인 아이핀(Internet

* 용인송담대학 컴퓨터게임정보과(leehk@ysc.ac.kr)
논문번호 : KICS2007-12-538, 접수일자 : 2007년 12월 4일, 최종논문접수일자 : 2008년 5월 13일

Personal Identification Number)을 도입하기도 하였다. 아이핀은 주민등록번호와는 달리 생년월일, 성별 등의 정보를 갖지 않으며 언제든지 변경할 수 있는 장점이 있으나, 대다수의 상위권 내의 포털이나 쇼핑몰, 온라인게임 사이트에서는 거의 사용하지 않는 실정이다.

Ⅱ. 동 기

악의적인 해킹에 의한 개인정보 도용도 막아야 할 일이지만, 우선 개인정보를 보호하기 위해서는 본인 스스로 개인정보가 유출되지 않도록 개인정보 보호에 대한 보다 적극적인 개인 인식이 선행되어야만 한다. 그러나 아직도 이런 인식이 미흡한 실정이다. 미국에서 몇 년 전 미국 매사추세츠 공대(MIT) 대학원생들이 중고 PC 158대를 대상으로 데이터 복구 실험을 했을 때 129대의 PC에서 개인 및 기업 정보가 발견되었다[1].

이와 비슷한 맥락으로 2005년 KAIST 데이터베이스 연구실에서 연구한 바에 의하면 중고 PC 매매로 인한 개인정보 유출이 심각한 것으로 나타났다[2]. 매년 약 100만대 이상의 PC가 중고 시장의 매물로 나오고 있는 현실에서 PC 대부분이 판매 전 포맷을 하지 않거나 포맷을 하더라도 영구삭제를 하지 않아 데이터 복구가 가능한 상황에서 거래가 이뤄지는 것이 보편적이다. KAIST 데이터베이스 연구실에서 연구한 바에 의하면 온라인 경매사이트에서 구입한 중고 PC의 HDD 30개를 분석한 결과, HDD 내에서 중요한 개인정보 및 기업정보가 지워지지 않은 채로 발견되었다. 특히, 국내 한 보험사 연수원에서 사용된 것으로 보이는 PC에서는 보험사 직원과 고객 사이의 통화내용이 담긴 음성 녹취 파일 200여 개가 남아있었으며 그 중 20여 개는 주소, 전화번호, 학력, 주민등록번호 등 상세한 개인정보 1700여건이 발견됐다. 또 국내 한 대기업 계열사에 사용하던 PC에서는 개인신상정보와 내부 보고서뿐만 아니라 제품 설계도 등 민감한 기업 정보가 담긴 파일까지 복구되었다. 이와 같이 개인의 민감한 정보를 넘어선 프라이버시까지도 마음만 먹으면 얼마든지 도용 가능하다는 것이 드러났다. KAIST 데이터베이스 연구실의 연구의 실험 과정은 하드디스크 상의 파일 시스템에서 보여 지는 모든 파일(휴지통, 웹브라우저 임시파일 등 포함)을 확인한 뒤, 시중에 판매되고 있는 전문 데이터복구 프로그램을 사용하여 포맷 또는 삭제된 파일 중 일부를 복구하는 것이었다. 기술적으로 고난도 분석은 아니었지만, 처음으로 PC 사용자의 개인정보 보호 의식 수준을 실험적으로 분석한 점에서 긍정적인 평가를 받을 만하다.

PC에 버금가게 개인정보를 많이 저장하고 있는 매체가 휴대폰이다. 보통 플래시메모리를 사용하는 휴대폰은 용량이 현재 2GB까지 시판 중이며, 우리나라 인구 중 열의 여덟이 소지하고 있다. 휴대폰의 용도는 개인정보의 저장을 넘어서 개인의 민감한 프라이버시까지도 저장할 수 있다. 그래서 일본의 대표적인 이동통신업체인 'NTT도코모'는 고객정보 보호를 위한 전략으로 새 휴대폰을 사면서 반납하는 휴대전화는 고객이 보는 앞에서 분쇄하도록 하고 있다[3]. 또한 고객정보를 취급하는 직원의 사내 휴대폰 사용을 금지하기도 하였다. 사용 중이던 휴대폰을 사용하지 않게 되었을 경우에는 이와 같이 분쇄하는 방법이 가장 이상적이나 아직 우리는 그렇게 철저히 관리를 하지 못하고 있는 실정이다. 특히 휴대폰의 새로운 모델 출시 주기가 짧아짐에 따라 중고 휴대폰의 유통이 차츰 증가하고 있으나, 중고 휴대폰의 유통과정에서 개인정보 보호 인식에 대한 연구는 전무한 형편이다.

휴대폰 역시 PC와 마찬가지로 중요한 개인정보를 플래시메모리에 저장함으로써 메모리에 저장된 정보는 사용자가 삭제를 하더라도 바로 깨끗하게 삭제가 되는 것이 아니기 때문에 완전히 파쇄하기 전에는 정보가 그대로 남아있다는데 문제가 있다. PC와 달리 아직 휴대폰에 장착된 플래시메모리를 복구하는 것은 기술적으로 매우 고난도이기 때문에 실제상황에서의 실험을 통한 개인정보 보호 의식에 대한 연구는 불가능하다. 그러므로 본 연구에서는 사용자의 개인 정보를 넘어선 프라이버시의 보고인 휴대폰 개인정보 보호에 대한 의식 수준에 대해 설문을 통해 조사, 분석함으로써 개인정보 보호의 필요성을 인식시키고자 한다.

Ⅲ. 관련 사례 연구

3.1 2005년 3월 패리스 힐튼 T-mobile폰 해킹 사건

2005년 3월 오스카 시상식 식장 주변에서 휴대폰 개인정보 침해 사건이 발생 했다[4]. 레드 카펫을 통해 휴대폰을 들고 입장한 100여명의 스타에 대한 프라이버시 침해 사건이 발생한 것이다. 미국의 4명의 대학생(University of Southern California)에 의해 2003년 설립된 Flexilis라는 회사의 주도 아래,

임의로 고용된 3명의 연구원들이 오스카 시상식장인 Kodak극장에 도착하는 스타들을 지켜보려는1000여명의 군중 속에서 스마트폰을 가진 50-100여명의 스타들의 개인정보를 탐색할 수 있었다고 한다.

Flexilis연구원들은 소프트웨어와 랩톱 컴퓨터를 스캐닝할 수 있는 강력한 성능의 안테나를 이용하였고, 탐색한 개인정보 가운데는 영화배우 Paris Hilton의 T-mobile 폰에 있는 내용들을 서비스 제공업자들의 컴퓨터로부터 입수할 수가 있었다고 한다. Paris Hilton의 전화에 들어있는 컨텐츠에는 다른 참석자들의 전화번호 등이 포함되어 있었다.

그러나 그들이 공격할 수 있는 전화의 정확한 숫자는 확신할 수 없었다. 왜냐면 어떤 전화는 한번 이상씩 검출되었기 때문이다. 스캔된 전화들에 대해서는 불법적인 행위이므로 확인 전화를 시도할 수가 없었다. 그래서 정확히 누구의 전화가 공격당할 수 있는지 확인해 볼 수는 없었다.

레드 카펫으로부터 20피트 떨어진 곳에서도 프라이버시에 침해될 위험이 발생했다. 즉, 최신형 휴대폰으로 비밀번호, SSN(Social Security Number)와 신용카드 정보를 포함한 개인 자료를 전송하는 것이 포착되었기 때문이다. 일반적으로 시상식 참석자, VIP, 정치인 들이 이런 종류의 공격에 가장 노출되기 쉽다. 왜냐면, 그런 사람들은 새로운 소비자 기술을 제일 먼저 사용하기 때문이다. 블루투스 같은 단파장 무선 데이터기술이 단거리용 케이블을 대체시키는 추세에 있다. 많은 종류의 휴대폰들은 컴퓨터와 동기화를 허용하기 위해 블루투스 기술을 내재하고 있다. 최근 블루투스는 고급자동차에 휴대폰을 쉽게 사용할 수 있게 하기 위해 사용되는 표준기술로도 자리 잡고 있다. 또한 키보드, 마우스, 프린터 등을 위한 케이블 대용으로서 개인용 PC에 사용되고 있는 추세이다. 블루투스 자체가 우려되는 것이 아니라 그 자체 내에 적당한 기밀 보안 기술이 포함되어야 한다[5,6]. 즉, 무선 세계에서의 보안 단계를 유선 세계에서와 같은 수준으로 끌어올리려는 노력이 절실히 필요하다.

모의 스마트폰 공격실험은 기술적인 측면에서 그리 어려운 작업이 아니었다. 강력한 안테나에 의한 전파송수신 정보를 스캐닝함으로써 간단히 개인정보를 포착할 수 있었다. 우리가 별 의식 없이 사용하는 스마트폰에 대한 해킹 가능성을 실험해 보임으로써 개인 프라이버시 보호의 중요성을 인식시킨 작업이었다.

3.2 BlueBag기반 해킹 사건

2006년 이탈리아에서 3명의 Secure network S.r.l의 연구원들에 의해 BlueBag이라는 기기 탐색장치를 이용한 블루투스 기술이 장착된 기기들에 대한 정보 탐색이 시행되었다[7]. 실험의 목적은 널리 보급되어 있는 불안전한 기기들에 대한 자료 수집과 공항이나 사무실 건물과 같은 보안이 필요한 지역에 대한 공격 가능성에 대해 조사하는 것이었다.

실험에서는 BlueBag을 이용하여 비밀리에 다른 기기들을 스캐닝하고 공격할 수 있도록 하였다. 동시에 발견되는 기기들을 처리하기 위하여 리눅스 기반의 시스템을 마련하였고, 보다 광범위한 지역을 담당하기 위해 전방향성의 안테나를 준비하였다. 이러한 기기들을 숨기고 또한 장 시간 동안 사용할 수 있는 배터리를 손쉽게 운반할 수 있도록 BlueBag을 제조하여 표면적으로는 일반 여행용 가방과 같으나 그 속에는 위에서와 같은 필요한 장비들을 배치하였다. 탐색 장소는 아래에서와 같이 모두 7군데를 특성 별로 선정하여 조사를 실시하였다.

- InfoSecurity 2006 가 열리는 밀라노의 Exhibition Center
- Orio 센터 쇼핑몰
- MM2 Cadorna 전철역
- Assago 밀라노 사무실 밀집지역
- 밀라노 중앙역
- 밀라노 Malpensa 공항
- Politecnico di 밀라노 공과대학

실험 대상으로 선정된 지역은 서로 다른 종류의 사람들이 밀집해 있는 곳으로서 잠재적으로 침입할 수 있는 목표들이 분포되어 있었다. 예를 들어 밀라노 중앙역은 평일 평균 270,000여명의 이용객들로 붐비는 곳이고, 토요일 Orio 센터 쇼핑몰은 많은 젊은 사람, 또는 가족들로 붐비는 곳이다. 이곳은 신기술과 관련된 위험에 대해 관심을 가지지 않는 층들이 밀집한 지역인 반면, InfoSecurity 2006 박람회장인 경우는 반대이다.

실험은 모두 7일간에 걸쳐서 총 23시간 동안에 여러 지역에서 각각 수행하였다. [표1]에서 보는 바와 같이 짧은 조사 기간 중에도 블루투스 기반의 기기들이 해킹 당하기 쉬운 상황에 노출되어 있었다. 조사된 기기 개수는 조사 기간 동안 발견된 기기들의 숫자를 의미하고, 기기 비율은 1분 동안 발견된 기기의 수를 의미한다.

표 1. 조사 결과 요약

장소	날짜	기간 (시:분)	조사된 기기갯수	기기 비율
InfoSecurity 2006	02/08-10/2006	4:42	147	0.53
Orio 센터 쇼핑몰	03/01-11/2006	6:45	377	0.93
MM2 Cadorna 전철역	03/09 /2006	0:39	56	1.44
Assago 밀라노 사무실 밀집지역	03/09 /2006	2:27	236	1.60
밀라노 중앙역	03/09 /2006	1:12	185	2.57
밀라노 Malpensa 공항	03/13 /2006	4:25	321	1.21
Politecnico di 밀라노 공과대학	03/14 /2006	2:48	81	0.48
합계		22:58	1405	

실험결과를 분석해 보면, 짧은 기간 동안에 많은 숫자의 침입 당하기 쉬운 기기들이 발견됨으로써 블루투스 기술이 일상생활에 분포되어 있음을 알 수 있었다. 아주 전문적인 분야에서부터 개인적인 부분에까지 개개인의 일상생활에 마치 모세관 현상처럼 확산되고 있었다. 중앙역, 공항, 그리고 사무실 밀집지역 간에는 많은 차이가 있었다. InfoSecurity 2006 박람회장과 대학교에서는 사용자들이 의식적으로 기기 사용의 중요성을 인지하고 있었다.

검색된 1405개의 기기들에 대한 종류별 분석을 해 본 결과, 휴대폰, 스마트폰은 1,312개, PC또는 노트북은 39개, 휴대용 나침반은 21개, GPS 내비게이터는 15개, 프린터는 5개, 기타 기기들이 13개를 나타냈다. 이번 실험으로 알 수 있는 중요한 점은 시장에 나와 있는 휴대폰 모델들 중 블루투스 기술이 사용되었다면 기본적으로 탐색이 될 수 있음을 알 수 있었다. 탐색을 피하려면 사용자는 반드시 수동으로 휴대폰을 안전모드 상태로 바꾸어 놓아야만 한다.

이번 실험 역시 모의 스마트폰 공격 실험과 마찬가지로 기술적인 측면에서 그리 어려운 실험은 아니었다. 여행용 가방 안에 마더보드, 충전기, 강력한 안테나 등으로 구성한 다음 여러 종류의 인식된 기기들을 스캐닝 하는 것이었다. 블루투스 기술의 보안 문제가 분명하게 증명되는 실험이었다.

3.3 중고 PC, 중고 휴대폰 매매로 인한 개인 정보 유출

2004년, 2005년 두 차례에 걸쳐 KAIST데이터베이스 연구실에서 우리나라 개인 정보 유출 실태를 조사하였다[2]. 한 해 동안 버려지거나 중고 PC 매매로 재활용되는 중고 PC는 수백만 대에 달한다. 첫 번째 실험에서 연구팀은 중고 하드디스크 41개를 인터넷 경매 등을 통해 구입하여 하드디스크의 데이터를 복구해 보았다. 그 결과 조사 대상의 30%에 해당하는 12대에서 모두 1,349명에 대한 개인정보를 쉽게 복구할 수 있었다. 본 연구에서는 국내 최초로 폐기되는 PC에 대한 개인정보 노출의 위험성을 실험을 통해 확인할 수 있었다. 2005년 실험에서는 온라인 경매사이트에서 구입한 중고 PC의 HDD 30개를 분석한 결과, HDD 내에 중요한 개인정보 및 기업정보가 발견됐다. 국내 한 보험사 연수원에서 사용된 것으로 보이는 PC에서는 보험사 직원과 고객 사이의 통화내용이 담긴 음성녹취 파일 200여 개가 남아있었으며 그 중 20여 개는 주소, 전화번호, 학력, 주민등록번호 등 상세한 개인정보 1700여건이 발견됐다. 또 국내 유수 대기업 계열사에 사용하던 PC에서는 개인신상정보와 내부 보고서뿐만 아니라 제품 설계도 등 민감한 기업 정보가 담긴 파일까지 복구됐다. 이 같은 현상은 국내에 국한된 것이 아니라 2003년 미국 메사추세츠 공대(MIT)대학원생들이 중고 PC 158대를 대상으로 데이터 복구 실험을 했을 때 129대의 PC에서 개인 및 기업 정보가 발견되었다[1].

Ⅳ. 휴대폰 개인정보 보호 의식 조사

아직까지 전 세계적으로 휴대폰 프라이버시에 관련된 실험이나 연구는 발표된 바 없으나, 일반적인 침해 가능성에 대해서는 계속적으로 경고하고 있는 실정이다. 2007년 5월 현재 우리나라 전체 인구의 약 79%가 휴대폰을 이용하고 있는 실정이어서 PC와 개인정보보호의 중요성은 이루 말할 수 없을 정도이다.

본 연구에서는 휴대폰에 저장하는 개인정보를 비롯하여 개인의 프라이버시에 대한 의식을 조사하고자 한다. 실제 중고휴대폰에 있는 메모리 분석 실험을 통해 구체적인 프라이버시 침해 실태를 파악해야 하나, 아직까지 기술적 분석을 하는데 시간이 많이 소모되기 때문에 설문조사를 바탕으로 의식 조사를 하고자 한다.

설문조사 방법은 온라인을 통한 방법 이외에 오프라인으로 하는 방법이 있을 수 있으나, 본 연구에서는 우선 온라인을 통한 방법을 선택하였다. 왜냐하면 면대면 설문지 조사 방법은 좀 더 다양한 조사대상을 설정하여 보다 구체적이고 사실적인 결과를 얻을 수는 있으나, 시간이 많이 소요되며, 조사대상자들 선택에 있어서도 연구자의 주변 환경에 의지할 수밖에 없기 때문이다. 이와 같이 오프라인을 통한 조사 방법도 다양한 표본을 대상으로 설문조사를 실시하기에는 한계가 있을 수밖에 없기 때문에 부득이하게 온라인 설문을 이용하였다.

전체 설문지는 휴대폰 매매 등 교체주기 관련된 통계학적 문항 2개와 휴대폰 사용 실태에 대한 문항 4개와 정보보호 의식 수준 관련 문항 1개로 모두 7개의 문항으로 구성되었다. 2007년 10월 4일부터 10월 5일 이틀간 조사를 하였으며, 설문 대상자는 온라인 설문 사이트 '월드 서베이'의 온라인 회원들이었으며 총 응답자는 300명이었다.

온라인 설문 조사 결과 휴대폰을 중고 상에 판적이 있다고 응답한 비율이 약 20%를 차지하였다. 보통 일반인들인 경우 휴대폰은 중고품 매매가 이루어지는지 조차 모를 수도 있으나 5명 중 1명이 이미 휴대폰 중고 매매 경험이 있다는 것은 주목할 만한 사항이다. 특히 휴대폰 제조업체들의 새로운 모델의 출시가 빈번함에 따라 교체 주기와 맞물려서 더욱 증가될 추세로 보인다.

휴대폰 교체주기는 2년 이상이 42%로 제일 많았고, 다시 말하면 58%의 휴대폰 이용자들이 2년 이내에 새로운 휴대폰으로 교체한다는 결과이다. 휴대폰 사용실태 조사에서 휴대폰으로 인터넷뱅킹을 한 적이 있는 가를 묻는 설문에 26%가 한 적이 있다라고 응답하였다. 인터넷뱅킹을 하기 위해서는 개인의 인증 비밀번호와 주민등록번호도 입력해야 한다. 즉 휴대폰 메모리에 주민등록번호와 함께 인증 비밀번호도 저장되어 있는 것이다. 만일 이러한 정보를 완전히 삭제하지 않고 중고로 유출할 경우 매우 심각한 개인 정보 침해가 일어날 수 있다.

전체 설문 응답자의 약 33%가 이메일을 한 적이 있다고 응답하였다. 더욱이 약 61%의 응답자가 사적인 연정을 문자 메시지로 전해본 적이 있다고 하였다. 이는 이메일과 더불어 반드시 보호되어야 할 개인의 프라이버시이다. 이메일과 문자메시지는 삭제하지 않고 계속 저장할 수도 있으며, 삭제했더라도 완전히 메모리에서 지워진 것은 아닌 상태이므로 매우 중요하고 민감한 정보들이다.

휴대폰에 저장하는 정보는 전화번호가 23.59%로 제일 많았고, 이름은 21.73%였다. 다음으로 사진이 16.48%, 문자 수신내역이 15.51%, 통화내역이 13.41%였고 주소가 6.54%였다. 특기할 만한 결과로 휴대폰에 저장할 필요가 없을 것 같은 주민번호도 1.53%를 차지하였다. 자신의 정보 이외에 지인의 전화번호, 이름, 사진 등 프라이버시까지도 휴대폰에 저장되기 때문에 휴대폰의 정보 보안이 매우 심각한 상황임을 알 수 있었다.

휴대폰을 바꿀 때 구 휴대폰에 저장되어 있는 정보를 삭제 하는가 라는 설문에는 약 63%가 자신이 직접 삭제한다고 응답하였고, 약 34.7%가 삭제하지 않고 교체한다고 하였다. 휴대폰에는 간단하게나마 삭제하는 기능이 있는데 이 기능이 있는지 조차 모르는 응답자도 약 3%가량 되었다. 자신의 정보 보호에 대한 의식 수준이 그리 높지는 않은 것으로 생각되었다.

종합적으로 정리 해보면, 신 모델의 출시가 빈번해 짐에 따라 휴대폰 교체 주기가 빨라지며, 중고품 매매가 빈번히 발생될 것으로 전망할 수 있다. 인터넷뱅킹과 이메일 경험을 한 사람이 PC에서처럼 많은 숫자는 아니지만 모바일의 편리성 때문에 차츰 증가하리라 생각되며 점차 개인 정보를 휴대폰에 저장하는 이용자들이 많아질 것으로 예상된다. 사적인 연정과 같은 개인의 프라이버시도 휴대폰을 통해 전달됨에 따라 프라이버시 보호에 보다 적극적인 보호 의식이 필요하다. 또한 휴대폰 교체 시 개인의 정보를 약 1/3가량의 응답자가 그냥 방치하는 것은 문제가 있다고 파악된다.

4.1 휴대폰 교체 주기 관점에서 본 의식 수준

새로운 기능과 모양을 갖춘 새로운 모델의 휴대폰이 앞 다투어 출시됨에 따라 현재 중고 휴대폰 매매 시장은 호황이다. 2005년 KOTRA에서 발표한 자료에 의하면 중고 휴대폰 판매량이 6000만대를 넘어섰다고 한다.

[그림 1]과 같이 설문 응답자의 절반 이상인 58%가 2년 내에 휴대폰을 새 모델로 교체한다고 한다는 것은 2007년 5월 현재 전체 휴대폰 사용자 3800만 명 가운데 2204만 명이 2년 내에 휴대폰을 교체한다는 것을 의미한다. 특히 12.66%의 응답자가 1년 이내에 교체한다는 통계자료는, 유행에 민감하여 계속적으로 새로운 모델을 구입하는 사용자들로서 1년 이내의 거의 신형에 가까운 481만대의 중고 휴대폰이 시장에 나올 수 있다고 볼 수 있다.

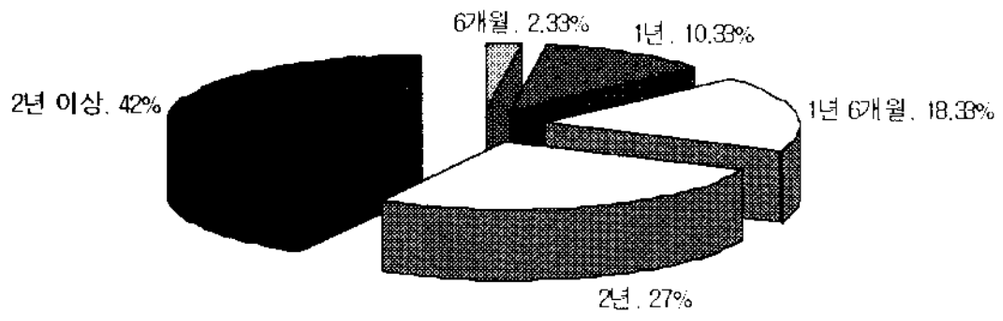

그림 1. 휴대폰 교체 주기 의식 조사

이러한 통계적 자료를 근거로 중고 휴대폰 시장은 매년 더 비대해 질 것으로 예측 할 수 있다.

4.2 휴대폰 개인정보 안전 관리 관점에서 본 의식 수준

자신이 사용하던 휴대폰을 중고로 매매가 하더라도 자신의 휴대폰에 저장되어 있던 정보를 깨끗이 삭제하는가 하는 설문에 [그림 2]와 같이 62.67%만이 자신이 직접 삭제한다고 응답하였고 약 35%가 삭제하지 않는다고 하였다. 이는 1년 이내에 휴대폰을 교체하는 경우, 약481만대 중 178만대의 중고 휴대폰이 개인정보 유출 위기에 놓여 있다고 할 수 있다. 즉, 1년에 178만대의 중고 휴대폰 개인정보가 고스란히 유출될 위기에 놓여 있는 것이다. 악의적인 타인의 정보이용자가 아무런 작업 없이도 손쉽게 타인의 정보를 유용할 수 있는 위기에 접하게 된다고 할 수 있다.

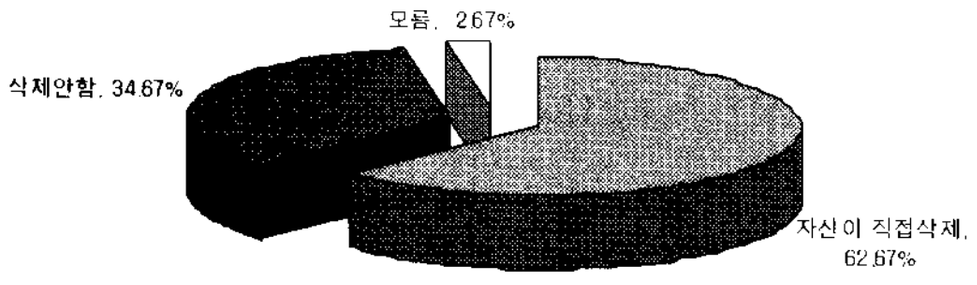

그림 2. 휴대폰 개인정보 안전관리 의식 조사

4.3 프라이버시 관점에서 본 의식 수준

전체의 61.33%가 [그림 3]에서 보는 바와 같이 개인의 프라이버시인 사적인 내용을 휴대폰을 통해 전달하는 것으로 응답했다. 3장에서 살펴본 모바일 폰 공격 모의실험에서와 같이 개인의 휴대폰에 내장된 컨텐츠까지도 도청이 가능한 현실로 미루어 보면 개인의 사생활도 안전하지 못하다는 것으로 분석할 수 있다. 즉, 전체 휴대폰 이용자 중 2330만 명이 사적인 내용을 휴대폰을 통해 쉽게 전달하는 현실이다. 하지만 이메일은 32.67%가 이용한 적이 있다는 것은 인터넷은 접속 등으로 인한 비용 부담, 또는 조작 상의 불편함으로 인해 문자 메시지보다는 이용률이 낮았다.

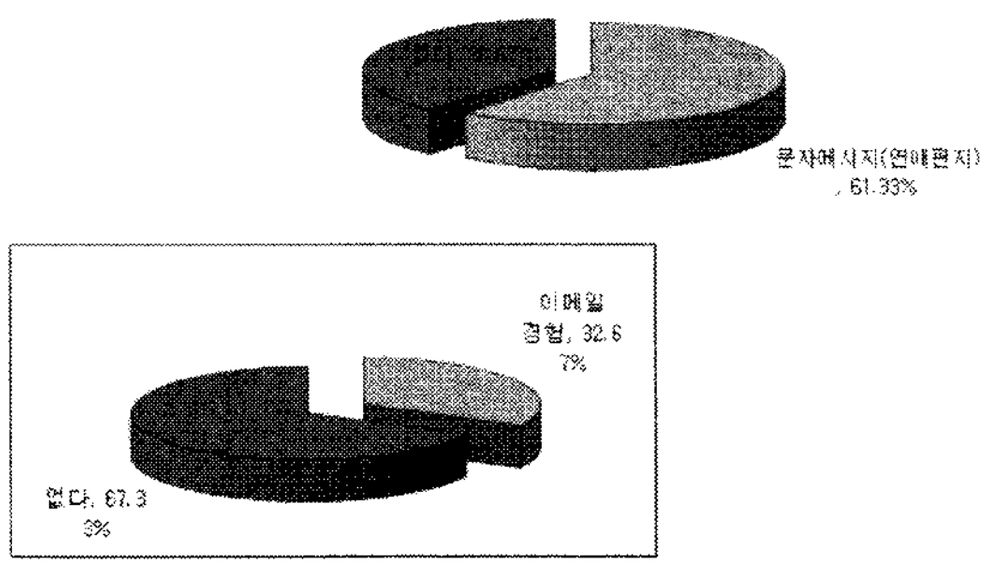

그림 3. 휴대폰과 프라이버시 의식 조사

4.4 휴대폰을 이용한 금융업무 수행 관점에서 본 의식 수준

PC를 통한 은행업무인 인터넷뱅킹은 이미 보편화된 지 오래이나, 대금결재 및 예금이체 등 휴대폰을 이용한 인터넷뱅킹은 [그림 4]에서 보는 바와 같이 전체 응답자의 26%인 98명이 경험한 적이 있다고 응답하였다. 인터넷뱅킹을 하기 위해서는 공인인증번호 및 주민번호와 같은 아주 중요한 개인정보가 필요하기 때문에 PC상에서도 매우 주의를 요하는 일이다.

휴대폰의 특성 상 본인이 인터넷뱅킹을 하기 위해 입력한 정보 들이 고스란히 저장되기 때문에 사용 후 신경을 써서 일일이 삭제해야 한다. 또한 인터넷뱅킹의 편리를 위해 공인인증번호는 휴대폰 안에 항상 저장시켜 놓을 수도 있기 때문에 만일 타인이 이를 악의적으로 휴대폰 정보에 대해 오용한다면 경제적 손실 등의 위험에 처할 가능성도 배제할 수 없다.

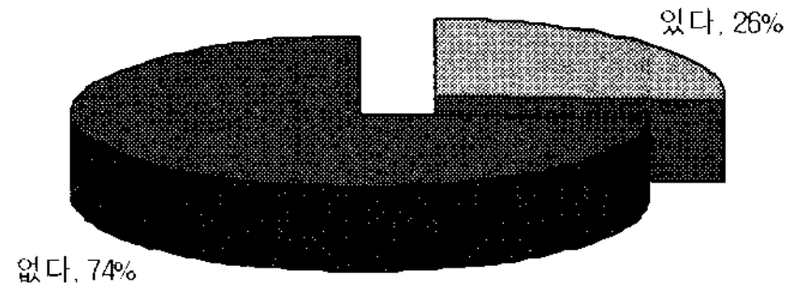

그림 4. 인터넷뱅킹 사용 유무 의식 조사

4.5 휴대폰에 저장하는 주요 정보 관점에서 본 의식 수준

휴대폰에 주로 저장하는 정보들을 8가지 중에서 다수의 선택을 허용하였더니 모두 1238건이 조사되었다. 이는 총 응답자 300명이 한 명 당 평균 4가지 이상의 정보들을 저장하고 있었다. [그림 5]에서 보는 바와 같이 전화번호는 총 응답자의 97%, 이름은 90%가 저장하고 있었고 이는 통계적으로 거의

대부분의 사용자가 저장한다고 볼 수 있다. 사진과 문자수신 내역은 각각 68%, 64%로 저장 비율이 비슷하였고, 통화내역도 55%가 저장하였다. 주민번호도 6%가 저장한다고 응답하였다.

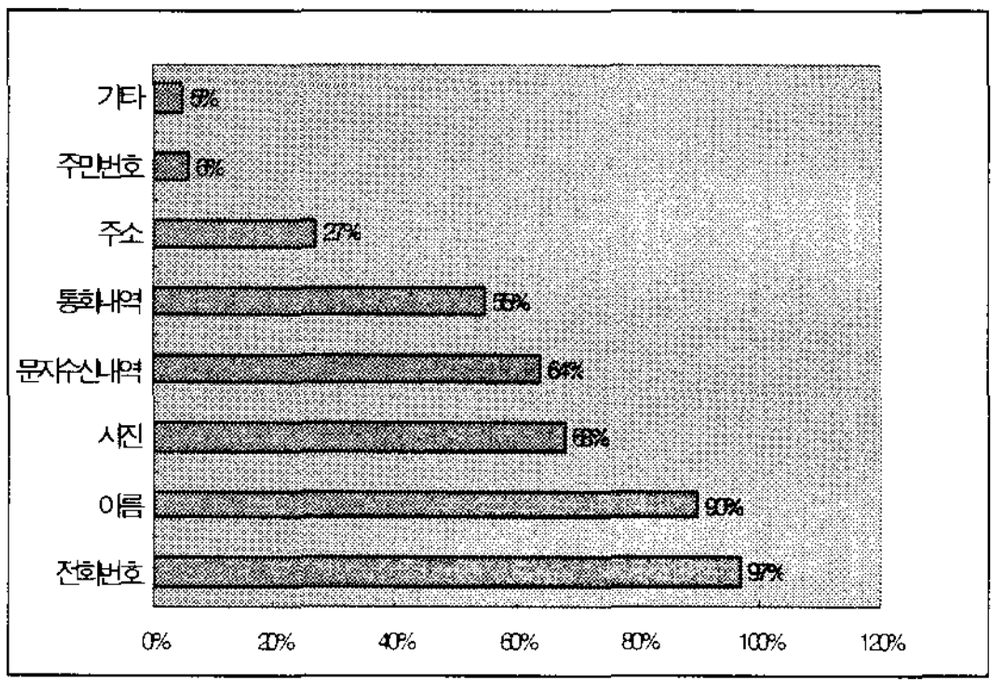

그림 5. 휴대폰에 저장하는 정보의 종류 분석

4.6 설문조사 결과

조사 기간: 2007년 10월 4일 - 10월 5일

설문 주제: 휴대폰 개인정보 보호 의식 조사

문 항 1 휴대전화를 중고상에 판 적이 있습니까?

예

└> 58 명 (19.33%)

아니오

└> 242 명 (80.67%)

문 항 2 보통 어느 주기로 휴대전화를 교체합니까?

6개월 이내

└> 7 명 (2.33%)

1년 이내

└> 31 명 (10.33%)

1년 6개월 이내

└> 55 명 (18.33%)

2년 이내

└> 81 명 (27.00%)

2년 이상

└> 126 명 (42.00%)

문 항 3 휴대전화로 인터넷뱅킹을 한 적이 있습니까?

예

└> 78 명 (26.00%)

아니오

└> 222 명 (74.00%)

문 항 4 휴대전화에 저장하는 정보는?(다수의 응답도 무방함)

전화번호

└> 292 건 (23.59%)

이름

└> 269 건 (21.73%)

주소

└> 81 건 (6.54%)

주민번호

└> 19 건 (1.53%)

문자수신 내역

└> 192 건 (15.51%)

통화 내역

└> 166 건 (13.41%)

사진

└> 204 건 (16.48%)

기타

└> 15 건 (1.21%)

문 항 5 휴대전화로 이메일을 한 적이 있습니까?

있다

└> 98 명 (32.67%)

거의 없다

└> 202 명 (67.33%)

문 항 6 '신정아게이트'가 연인간의 메시지로 밝혀지게 되었는데 사적인 연정을 문자 메시지로 전해 본 적이 있습니까?

있다

└> 184 명 (61.33%)

거의 없다

└> 116 명 (38.67%)

문 항 7 휴대전화를 바꿀 때 구 휴대전화에 저장되어 있는 정보를 삭제합니까?

자신이 직접 삭제한다

↳ 188 명 (62.67%)

삭제하지 않고 교체한다

↳ 104 명 (34.67%)

삭제하는 기능이 있는지 모르겠다

↳ 8 명 (2.67%)

V. 의식조사 결과의 시사점

5.1 개인정보 보호를 위한 정보 삭제

설문을 통한 휴대폰 정보보호 의식 조사 결과를 분석해 보면, 신형 휴대폰으로 교체하는 주기가 점점 빨라짐에 따라 중고 휴대폰 매매 시장이 확장되는 추세이므로 중고 휴대폰에 대한 정보보호 문제가 발생될 수 있음을 알 수 있다. 휴대폰은 개인의 수첩 기능을 할 정도로 각종 개인적인 자료를 보관하고 있었고, 특히 다수는 아니지만 금융 업무를 할 정도로 그 기능이 확대되고 있음을 알 수 있었다.

이와 같이 중요한 정보들을 휴대폰에 저장하는 반면에 더 이상 사용하지 않는 휴대폰에 대한 개인정보 안전관리 면에서는 그리 안심할 만한 수준이 아니었다. 휴대폰에 정보를 삭제하는 기능을 이용하면 간단히 삭제할 수 있는 데도 이를 모르거나 무관심한 사용자가 40%가 되었기 때문이다.

휴대폰에는 개인 정보뿐만 아니라 자신의 휴대폰에 저장된 지인의 정보까지도 보호되어야 한다. 그러나 설문조사 결과에 따르면 아직까지 개인정보 보호에 대한 의식이 그리 높지는 않은 편이다. 사용하던 휴대폰을 더 이상 사용하지 않게 되었을 땐 자신이 저장한 정보는 깨끗하게 처리하여야 하는 것이 원칙이지만, 그렇지 않을 경우 중고 휴대폰의 매매가 유지되고 있는 한 개인정보는 고스란히 유출될 위기에 처할 수 있게 된다.

5.2 중고 플래시 메모리 분석 시 예측 가능한 심각성

본 논문의 조사 연구 결과는 설문조사에 의하여 개인정보보호에 관한 의식수준을 알아보고자 하였다. 그러나 실제 중고 휴대폰에 내장된 플래시 메모리를 분석해 본다면 개인정보 보호에 대한 실질적인 의식 수준을 알 수 있으리라 생각된다. 아마 그 심각성은 쉽게 예측할 수 있으리라 본다. 머지않아 국내외 유수 연구실에서 발표할 가능성이 있는 휴대폰 중고 플래시 메모리 관련 프라이버시 내용 분석 결과와 본 설문결과에 따른 분석 결과가 어느 정도 상응되는지 상호 교차 점검하는데 본 연구가 활용할 수 있을 것으로 기대된다.

5.3 향후 연구를 위한 의식 조사 방향

본 연구에서는 연구의 기반이 되는 설문조사가 온라인을 통해서만 이루어져 연구 결과의 신뢰도에 있어서 다소 현장감이 떨어질 수도 있다. 온라인 설문조사방법은 시간이 적게 걸리는 장점이 있기는 하지만, 인터넷을 주로 많이 이용하는 연령층과 비례하여 자칫하면 젊은 연령층들과 같은 특정한 대상들이 다수 참여할 가능성이 높기 때문이다. 이러한 점을 보완하기 위해서 본 연구의 설문항목에 성별, 연령, 직업 등을 포함시켰다면 보다 다양한 각도에서의 의식조사를 할 수 있었을 것 같다. 앞으로 좀더 현실적인 연구결과를 얻기 위해서는 조사방법을 다양화하는 것이 바람직할 것 같다. 조사방법에 있어서는, 시간은 많이 소요되지만 조사대상자를 다양하게 선별할 수 있는 면 대 면을 통한 설문조사가 동시에 이루어져야 하며, 또한 설문항목을 개발하여 다양한 각도에서의 의식조사를 할 필요가 있다고 본다.

VI. 결 론

중고 PC 메모리 복구 작업에 의한 개인 정보 유출 사례는 이미 발표되어 그 심각성은 널리 알려졌으나, 휴대폰에 대한 연구는 없는 실정이다. 중고 휴대폰 안에 내장된 플래시 메모리를 복구하여 개인 정보를 포함한 프라이버시에 대해 분석한 연구는 현재 국내 외 유수 연구실에서 연구 중이나 기술적으로 대단히 고난도의 작업이어서 아직 발표되지 않았다. 그러므로 본 연구에서는 휴대폰 정보보호 의식 수준을 우선 설문을 통해 조사해 봄으로써 개인 정보 보호의 중요성을 파악하고자 하였다.

설문 결과에 대한 분석에서는 휴대폰 교체 주기 관점에서 본 의식 수준 등 모두 5가지 관점에서 의식 수준을 조사하였다. 조사 결과 현재는 약 80%가 휴대폰을 매매한 적이 없다고 하였으나, 매년 중고 휴대폰 시장이 성장할 것으로 예상되므로 중고로 매매되는 휴대폰에 대해서는 더욱 세심한 정보 삭제가 요구된다. 휴대폰의 안전관리 측면에서는 아직

개인 정보의 중요성을 인식하지 못하는 사용자들이 전체의 약 1/3을 넘고 있다. 개인적인 메시지 등의 전달 매개 수단으로써 휴대폰의 역할이 큰 편이고, 특히 이메일 대신 문자 메시지를 이용하여 개인의 감정을 손쉽게 전달하는 것으로 나타났다. 휴대폰을 이용한 금융업무 수행 관점에서 본 의식 수준에서는 26%가 이용함으로써 그리 보편화되어 있지 않은 형편이었다. 휴대폰에 저장하는 주요 정보 관점에서 본 의식 수준에서는 전화번호, 이름을 가장 보편적으로 저장하고 있었고, 그 다음으로 사진과 문자수신내역 순이었다. 소수이긴 하지만 주민번호와 같은 중요한 개인정보를 저장하는 응답도 전체 응답자의 6%나 되었다.

참 고 문 헌

〔1〕 S. Garfinkel and A. Shelat, "Remembrance of Data Passed: A Study of Disk Sanitization Practices," *IEEE Security & Privacy*, pp.17-27, 2003.

〔2〕 문송천, 권 영철, "우리나라 개인정보 국내정보 국내 유출 실태 심각", *한국정보과학회지*, 제22권 제5호, pp.42-43, 2004.

〔3〕 개인정보보호 전문교육 - 개인정보보호 법률 및 사례, *한국정보보호진흥원*, http://www.kisa.or.kr, 2007.

〔4〕 John, M. and Laura. M. H, "Oscar surprise: Unsafe cellphones," *Printed Version of The New York Times*, 3rd March, 2005.

〔5〕 M. Jacobsson, S. Wetzel, "Security Weaknesses in Bluetooth,"*Proc. 2001 Conf. Topics Cryptology(CT-RSA01)*, Springer-verlag, pp.176-191, 2001.

〔6〕 S. F. Hager and C. T. Midkiff, "Demonstrating Vulnerabilities in Bluetooth Security," *Proc. IEEE Global Telecommunications Conf. (GLOBECOM03)*, Vol.3, IEEE CS Press, pp.1420-1424, 2003.

〔7〕 Luca, C. Claudio, M. and Stefano, Z., "Studying Bluetooth Malware Propagation: The BlueBag Project," *IEEE Security & Privacy*, pp.17-25, 2007.

이 혜 경 (Hae-kyung Rhee) 정회원

1979년 2월 숭실대학교 전자계산학과 졸업

1985년 4월 University of Illinois (Urbana-Champaign) 전산학과 석사

2000년 2월 성균관대학교 정보공학과 박사

1988년 3월~1989년 2월 국립천안공업전문대학 전자계산과 전임강사

1992년 3월~2001년 8월 경인여자대학 멀티미디어정보전산학부 조교수

2001년 9월~현재 용인송담대학 컴퓨터게임정보과 부교수

<관심분야> 데이터베이스, 데이터 모델링, 정보보호