유비쿼터스 컴퓨팅 보안기술에 관한 연구

A Study of Ubiquitous Computing Security Technology

강희조*

목 차

Ⅰ. 서론
Ⅱ. 유비쿼터스 컴퓨팅 환경에서 개인정보보호
1. 개인정보의 유형과 종류
2. 해외의 개인정보 동향
3. 유비쿼터스 환경에서 개인정보 침해 유형
Ⅲ. 유비쿼터스 환경에서 개인정보보호 방법
1. 개인정보 침해 기술
2. 개인정보 보호 기술
Ⅳ. 정보 보호 구현 방안
Ⅴ. 결론

Key Words : Ubiquitous Computing, Security, Platform for Privacy Policy, Mix-network

Abstract

유비쿼터스 컴퓨팅 사회의 보안기술에 대한 적절한 정의가 필요하고 유비쿼터스 컴퓨터 환경을 신뢰하고 안전하게 사용할 수 있고 활성화하기 위한 환경을 만드는 것이 매우 중요하다. 본 논문에서는 유비쿼터스 컴퓨팅 환경 내 개인정보의 중요성 및 특징, 피해현황, 해외 개인정보 동향, 개인정보의 침해 기술, 개인정보 보호 기술에 대하여 검토하고 정보보호 구현방안을 검토한다.

* 목원대학교 컴퓨터공학부 부교수, hjkang@mokwon.ac.kr, 011-9620-3205

Ⅰ. 서론

유비쿼터스 컴퓨팅은 인간생활을 편리하게 할 것으로 예상되고 있다.마크 와이저의 연구에 따르면 미래의 각 가정에는 지각할 수 없는 컴퓨터가 100여대 이상 설치될 것이라 한다[1],[2]. 이런 사실을 두고 각 개인의 프라이버시와 개인정보보호가 잘 될 것인지 걱정하게 하는 연구 사례가 많이 발견되고 있다. 개인정보의 부적절한 사용으로 인한 개인정보 침해문제는 유비쿼터스 컴퓨팅이 가져다 줄 긍정적인 효과를 반감시키는데 결정적인 요인이 될 수 있기에 개인정보의 보호는 중요하다. 유비쿼터스 컴퓨팅 환경에서는 모든 정보가 공유될 수 있고 악의 적으로 누구나 쉽게 접근할 수 있는 가능성이 있다. 이러한 측면에서 개인의 정보가 다른 사람에게 쉽게 유출되어 개인적인 사생활의 보장이 유실되는 세계가 될 가능성이 있다. 그 외 크래커에 의한 정보유출, 바이러스, 컴퓨터 범죄, 프라이버시 침해 등 현재 가상 세계에서 벌어지고 있는 각종 부작용들의 증가로 이어질 수 도 있다. 예를 들어 개인정보나 구매내역이 기업들 사이에서 상업적인 목적으로 공유되고, 통행인의 얼굴을 인식해서 범죄 혐의자와 대조하는 무인 감시카메라에 이르기까지 많은 문제의 소지를 가지고 있다[3]. 따라서 본 논문에서는 유비쿼터스 컴퓨팅 환경에서 발생될 수 있는 개인정보 침해유형을 살펴보고 이를 보호할 수 있는 방안과 방법을 제안하고자 한다.

Ⅱ. 유비쿼터스 컴퓨팅 환경에서 개인정보보호

1. 개인정보의 유형과 종류

우리나라는 1995년 1월 8일 법률 4734호에 제정된 개인정보보호법에 개인 사생활의 비밀을 보호하고 사적 권익의 침해를 방지하고 있다. 또한 국가인권위원회법을 통해여 모든 개인이 가지는 불가침의 기본적 인권을 보호하고 인권의 보호와 향상을 위한 업무를 수행하기 위해 국가인권위원회를 두었다. 하지만 현실을 보면 주민등록번호의 노출 및 기타 개인정보의 노출로 인권침해 및 범죄의 활용 가능성이 더욱 증가하고 있다. 이는 각종 정보매체나 인터넷을 통한

유형구분	개인정보의 종류
일반정보	이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 성별
가족정보	가족구성원들의 이름, 출생지, 생년월일, 직업, 전화번호
교육정보	학적사항, 기술자격증 및 전문면허, 상벌사항
병역정보	군번 및 계급, 제대유형, 주특기, 근무부대
부동산정보	소유주택, 토지, 자동차, 기타 소유차량, 상점 및 건물 등
동산정보	보유현금, 저축현황, 현금카드, 주식, 채권, 예술품, 보석
소득정보	현재 봉급, 봉급경력, 보너스 및 수수료, 이자소득, 사업소득
기타수익정보	보험(건강, 생명 등), 가입현황, 회사의 판공비, 퇴직프로그램
신용정보	대부 잔액 및 지불상황, 저당, 신용카드, 압류통보기록
법적정보	전과기록, 자동차교통위반기록, 구속기록, 이혼기록, 납세
의료정보	가족병력기록, 과거의료기록, 정신질환기록, 각종 의료정보
신체정보	지문, 홍채, DNA 신장, 가슴둘레 등

<그림 1> 일반적 개인정보의 유형과 종류

정보노출이 쉽기 때문인데 유비쿼터스 환경에서는 이러한 현상이 더욱 심해질 것이라고 예측할 수 있다. 개인정보보호 법제를 가진 대부분의 국가에서도 이러한 개인정보 침해에 대하여 적극 보호하려 하고 있다. 현행 개인정보는 그림 1에서와 같이 주로 개인의 신상 및 개인의 관계성에 기반한 정보가 대부분이다. 유비쿼터스 컴퓨터 환경에서도 이러한 개인정보의 분류가 적용될 것으로 예상된다.

2. 해외의 개인정보 동향

개인정보의 국제법적 제도적 측면에서 중요한 연구 방향 중 한가지는 OECD에서 제시하는 프라이버시 보호 및 국제적 유통에 관한 가이드라인 부분이다. OECD 기준은 주로 정보주체의 동의 절차에 대한 명시가 중요한 내용으로 포함되어 있다. OECD의 개인정보보호 8대 원칙은 그림 2에 나타낸다.

원칙	내용
수집 제한의 원칙	개인 데이터의 수집에는 제한을 두어야 한다. 어떠한 개인 데이터도 합법적이고 공정한 절차에 의하고, 가능한 경우에는 데이터 주체에게 알리거나 동의를 얻은 연후에 수집하여야 한다.
정확성 확보의 원칙	개인 데이터는 그 이용 목적에 부합되는 것이어야 하며 이용 목적에 필요한 범위 안에서 정확하고 완전하며 최신의 것이어야 한다.
목적 명시의 원칙	개인정보는 수집 시 그 목적이 명확히 제시되어야 하며, 그 후의 이용은 수집 목적의 실현 또는 수집 목적과 양립되어야 하고 목적이 변경될 때마다 명확화될 수 있는 것으로 제한되어야 한다.
이용제한의 원칙	개인정보는 목적 명확화의 원칙에 의하여 확인된 목적 이외의 다른 목적을 위해 개시, 이용, 그 밖의 사용에 제공되어서는 안 된다. 다만 정보 주체의 동의가 있거나 법률의 규정에 의한 경우에는 예외로 한다.
안전성 확보의 원칙	개인 데이터는 분실 또는 불법적인 액세스, 파괴, 사용, 수정, 개시 등의 위험에 대하여 합리적인 안전 조치를 함으로써 보호하여야 한다.
공개의 원칙	개인 데이터와 관련된 개발, 실시, 정책에 대하여는 일반적인 공개 정책을 취해야 한다. 개인 데이터의 존재, 성질 및 주요 이용 목적과 함께 데이터 관리자의 식별, 주소를 명확하게 하기 위한 수단은 용이하게 이용할 수 있어야 한다.
개인 참여의 원칙	개인은 자기에 관한 정보의 소재를 확인할 권리를 가지며, 필요한 경우에는 자신에 관한 정보를 합리적인 기간 내에 합리적인 비용과 방법에 의해 알기 쉬운 형태로 통지 받을 권리를 갖는다. 이러한 권리가 거부된 경우에 개인은 그 이유를 구하고 거부에 대하여 이의를 제기하거나 데이터의 폐기, 정정 및 보완을 청구할 권리를 갖는다.
책임의 원칙	데이터 관리자는 위의 제 원칙을 실시하기 위한 조치에 따를 책임이 있다.

<그림 2> OECD의 개인정보 보호 원칙

3. 유비쿼터스 환경에서 개인정보 침해유형

현재 개인정보는 인터넷, 각종 마케팅 행사, 다양한 커뮤니티에 저장된 개인정보, 설문조사 등의 방법으로 각 개인이 원하지 않음에도 불구하고 각종 저장매체에 기록되고 유통되고 있다. 개인정보의 침해되고 있는 유형을 분류해보면 그림 3과 같이 분류할 수 있다[4].

개인정보 침해유형	현행	유비쿼터스 컴퓨팅 환경
부적절한 접근과 수집	정보주체의 동의없는 개인정보의 수집	정보주체가 인식할 수 없는 상황에서 정보주체가 완전한 자기정보 통제권을 상실할 가능성이 큼
부적절한 분석	부적절하게 수집된 정보의 분석, 동의없는 사적 정보의 분석	부적절하게 수집된 정보의 분석을 통해 개인 지배 또는 개인에 대한 통제행위가 심화될 가능성 큼
부적절한 모니터링	동의없는 개인의 인터넷 활동을 ha니터링	부적절한 모니터링을 통한 개인의 라이프스타일 등 개인의 생활 전반이 노출될 가능성이 큼
부적절한 개인정보유형	개인정보를 제 3 자에게 양도하는 등 불법적 거래	개인정보를 제 3 자에게 양도하는 등 다양한 유형의 개인정보가 불법적으로 거래되거나 유통될 가능성
원하지 않는 영업행위	동의없는 상품광고, 광고성 정보전송행위	개개인의 특성에 정확하게 조응하는 광고성 구체적 상품광고가 동의 없이 무차별적으로 유통될 수 있음
부적절한 저장	정보수집 목적 달성 후 개인정보를 파기 하지 않는 행위	한번 수집된 정보는 파기되지 않고 수차례의 분석을 통해 다양한 용도로 재활용될 가능성 큼

<그림 3> 유비쿼터스 환경에서의 개인정보 침해 유형[4]

Ⅲ. 유비쿼터스 환경에서 개인정보보호 방법

1. 개인정보 침해 기술

개인정보 침해 기술은 컴퓨터 환경 내 개인정보 관련 오남용 또는 악의의 피해가 발생할 수 있는 분야에 대하여 기술적 관점에서 체계적으로 분석하고 대응할 수 있는 기술적 체계 구성을 말한다. 이는 표 1 과 같다.

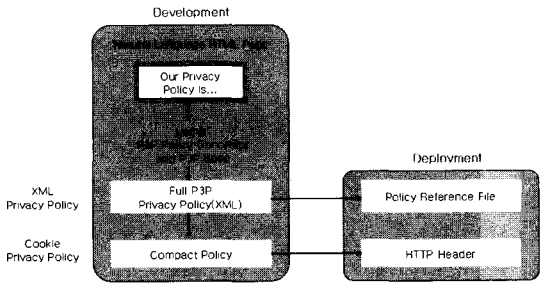
2. 개인정보 보호 기술

개인정보 보호 기술은 크게 웹 기반의 익명성을 제공해 주는 기술, 에이전트 환경 내 개인정보를 관리하는 기술, 그리고 네트워크나 인터넷 환경 내에서 신뢰할 수 있는 개인정보 전송을 보장해 주는 기술의 세 가지 범주로 나눌 수 있으며, 개인정보 보호 기술은 표 2 와 같다[5].

1) P3P를 활용한 개인정보보호 방법

P3P는 각 웹사이트의 개인정보를 자동으로 검색 파악한 후 사용자의 공개수준과 비교 판단할 수 있도록 하는 표준이다[6]. 이 기술은 쿠키제어를 통해 사용자가 직접 통제가능한 개인정보 보호 기술로 평가된다. 동작원리는 각 개인의 클라이언트 PC에 설정된 개인정보 공개수준을 설정하고 웹 사이트 방문 시 해당 사이트의 개인정보보호

정책 수준을 취득하여 이를 비교한 후 수준이 일치하는 경우는 자동 접속하지만 일치하지 않으면 경고 메시지를 출력하며 접속하지 않는다. 자세한 내용을 그림 4 에 나타내었다.



<그림 4> 개인정보 보호정책 생성 구조도

유비쿼터스 환경에서도 이를 활용 할 수 있다. 개인이 소지한 PostPC나 스카트 핸드폰, RFID가 첨부된 개인 ID에서 자신의 개인정보를 공개할 수준을 미리 설정해 놓는다. 주변의 유비쿼터스 컴퓨팅 환경에서도 개인정보를 취득할 수준을 설정해 놓고 이를 비교해서 일치하면 개인정보를 취득하고 개인이 이를 낮게 설정하여 취득 할 수 없는 경우는 취득하지 않는다. 궁극적으로 개인정보 노출 정도를 각 개인이 설정할 수 있는 것이다.

2) 홈 게이트웨이를 활용한 개인정보 보호 방법

홈 게이트웨이는 홈 네트워킹 시스템에서 가정과 외부 네트워크를 연결하는 부분이다. 또한 가정내 여러 가지 기기들을 제어하는 주요 구심점이 도리 것이다. 또한 가정내의 유비쿼터스 컴퓨팅 환경에서 발생하는 정보들을 외부로 전달하게 되는 관문이 된다. 가정내에서 발생하는 모든 개인정보는 홈 게이트웨이에서 제어하는 것이 타당하다. 이를 홈 네트워킹 시스템을 이해하는 것으로부터 자세하게 살펴본다.

홈 네트워킹은 유·무선을 통합하는 네트워킹 기술을 기반으로 가정의 기기들을 제어하고 관리하는 하드웨어나 기반 소프트웨어 그리고 정보가전기기들을 통합하여 외부의 인터넷 망에 연결하는 것을 총칭한다.

홈 네트워킹에서는 유선 홈 네트워크와 무선 홈 네트워크 기술이 사용된다. 유선 홈 네트워크 기술에는 Home PNA, PLC, 이더넷, USB, IEEE1394 등이 있고, 무선 홈 네트워킹 기술에는 무선 LAN, Home RF, Bluetooth, IrDA(Infrared Data Association), UWB 등이 있다. 이 때 홈 네트워킹에서 사용되는 네트워크를 가정의 맨 앞에서 제어할 수 있는 것이 홈 게이트웨이이다[7].

가정 내에서 사용되는 지능형 가전기기나 유비쿼터스 컴퓨팅에서 자동으로 개인정보를 취득하여 개인에게 편리한 서비스를 제공할 수 있다. 개인의 취향 및 개인이 주로 사용하는 기기 등의 정보가 개인정보로 분류될 수 있다. 하지만 외부에서 이것을 알게 되면 개인 사생활 침해가 될 것이다. 그렇기 때문에 이러한 정보를 외부로 전달되지 않도록 홈 게이트웨이에서 통제하며, 외부의 불법 접근도 차단할 수 있도록 기능을 부여한다.

3) 웹 기반의 익명성 제공 기술 방법

정보의 노출 자체와는 무관하게 정보와 소유자 간의 관계나 송수신자 간의 관계를 비밀로 하여 사용자의 개인정보보호를 제공하는 기술로 사용자 간의 비연결성을 통하여 익명성을 제공하는 Mix-network 기술 방법이다.

4) 에이전트 기술 방법[8]

개인정보보호를 위한 에이전트는 사용자가 파악하기 쉽지 않은 인터넷 상에서의 정보 유출에 대해 사용자를 대신하여 통제해 주는 역할을 한다. 쿠키 매니저, 에드 브로

커, 스파이웨어 필터 등의 기술 방법이 있다.

5) 네트워크 기반 기술 방법

네트워크 환경에서 정보를 전달할 때 중간에 가로채거나 수정하거나 또는 단순히 그 데이터를 보기만 하는 행동들에 의해 발생된다. 가장 널리 이용되고 있는 PET (Privacy Enhancing Technology)[9] 기술은 프록시, 방화벽, IDS 등이 기술 방법이 있다.

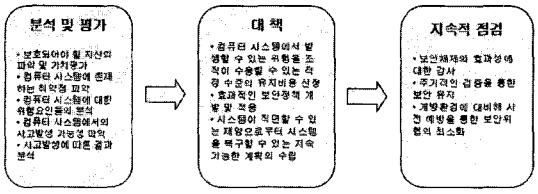
6) 법제도를 통한 개인정보보호 방법

법과 제도를 제정하여 유비쿼터스 컴퓨팅 환경에서의 개인정보 취득과 이용을 제한해야 개인정보가 보호된다. 개인정보를 보호하기 위한 많은 기술과 시스템이 있다고 하여도 법과 제도가 이를 보호하도록 하지 않으면 개인정보보호 시스템은 시간이 지나면 또 다른 시스템에 의해 해킹되거나 취득될 것이다.

하지만 단순하게 개인정보 취득을 못하도록 하는 것은 유비쿼터스 컴퓨팅 환경에 맞지 않는다. 개인에게 다양한 서비스를 제공하기 위해서는 개인정보 취득이 필수이기 때문이다. 결국 개인의 의사에 반하여 개인정보 취득을 못하도록 해야 하는데 이를 위하여 옵트 인(Opt-in)과 옵트 아웃(Opt-out)을 활용하는 방법있다.

Ⅳ. 정보보호 구현 방안

정보 자산에 대한 보호는 위에서 언급한 정보 보호의 모든 영역에 걸쳐 균형 있게 이루어져야 하며, 그림 5 과 같은 절차로 구현되어야 한다.



<그림 5> 정보보호 구현 방안

안전한 정보보호 시스템 아키텍처를 구성하기 위한 방법은 첫째로 컴퓨터 시스템이 보유하고 있는 데이터의 완결성, 비밀성, 인증성 및 가용성과 시스템 자원의 보호 및 인원 보안 등 시스템의 보안 요인들과 함께 컴퓨터 시스템에 대한 안전을 보장하기 위한 전략적인 대책을 선정한다[10],[11]. 이때 구현하고자 하는 또는 컨설팅이 필요로 하는 자산에 대한 정확한 현황을 파악하고자 하는 분석 및 평가의 작업이 이루어진다. 둘째로 정보보호의 대상이 되는 컴퓨터 시스템은 일반적으로 인적· 관리적 보안, 물리적· 환경적 보안, 기술적 보안으로 나눌 수 있으며, 이는 다시 시스템, 통신망, 데이터베이스, 소프트웨어, 설비, 인원 및 조직, 절차 등으로 세분화되어 종합적인 대책을 수립한다. 마지막으로 수립된 대책을 기반으로 순차적으로 정보보호 아키텍처를 구현한다. 잘 구현된 정보보호 시스템 아키텍처는 향후 어느 정도의 보안성을 유지하기 위한 지속적인 유지 보수 및 주기적인 모니터링 체계가 필수적이다.

Ⅴ. 결론

유비쿼터스 컴퓨팅 환경은 차세대 정보기술로서 미래에 많은 편리함을 가져다 줄 것으로 많은 사람들이 기대하고 있다. 실생활에 많은 편리함을 가져주는 만큼 악의적인 공격자로 인해서 개인의 정보 유출과 같은 큰 희생을 강요받을 가능성이 존재하는 것이 현실이다. 본 논문에서는 유비쿼터스 컴

퓨팅 환경 내 개인정보의 중요성 및 특징, 피해현황, 해외 개인정보 동향, 개인정보의 침해 기술, 개인정보 보호 기술에 대하여 검토하고 정보보호 구현방안을 제안했다.

참 고 문 헌

1. M. Weiser, "Ubiquitous Computing," Http://www. ubiq.com/Hypertext/weiser /UbiHome.h tml.
2. Mark Weiser, "Hot Topics : Ubiquitous Computing" IEEE Computer October 1993.
3. F. Stajano, Security for Ubiquitous Computing, John Wiley & Sons, LTD., 2002.
4. 윤용근, 정병주, "유비쿼터스 컴퓨팅 환경하의 개인정보 침해 유형분석," 한국전산원 정보화정책 이슈, 2004.
5. Misa Aoki, "IT 시스템에 의한 프라이버시 대책," PROVISION No.42 Summer 2004.
6. 윤재석, "P3P의 논의 현황과 문제점 및 국내정책 방향," 전자신문, 2005.
7. D.Liu and P.Ning, Efficient distribution of key chain commitments for broadcast authentic cation in distributed sensor networks, NDSS' 03, 2003.
8. www.pet-pisa.nl, "Privacy Incorporated Software Agent System Architecture(PSA)".
9. Handbook of Privacy and PET(Privacy Enhancing Technology), PISA Project.
10. R. Zimmer, " Structured Analysis of Security in Ubiquitous Computing," UBICOMP 2002, Oct. 2002.
11. A.Perrig, R.Canetti, D.Song and .D.Tygar, Efficient and secure authe-ntication for multicast, NDSS'01, Feb. 2001.

<표 1> 개인정보 침해 기술 분석표

침해기술	방법
TCP/IP 주소	TCP/IP 주소의 분배 및 관리 체계 특성 때문에 인터넷 이용시 TCP/IP 주소를 추적하여 이용자 신원을 확인하는 것이 용이하다.
도메인 네임	E-mail의 출처를 확인하는 것은 매우 간단하며, 누구나 ISP 정보와 e-mail 이용자의 ID를 알 수 있다. ISP는 이용자의 ID를 이용하여 이용자의 계정을 확인할 수 있다.
Processor Serial Number(PSN)	Intel사는 자사가 개발하는 Pentium III 칩에 고유의 프로세서 일련 번호(serial number)를 부여하여 인터넷에 접속하는 특정 컴퓨터의 이용자의 신원 정보와 연결시켜 전자상거래에 있어서 인증 목적으로 이용한다.
IPv6	IPv6의 계획은 인터넷 상의 모든 장치에 고정된 주소를 할당하는 것으로, IPv6의 새로운 주소는 하드웨어 속에 내장될 것이고, 추적 가능한 정보를 포함하게 된다. 이것은 마치 영구적인 쿠키를 심는 것과 동일한 개념이다.
쿠키(cookie)	쿠키 파일을 이용하여 인터넷 이용자의 신원을 쉽게 파악할 수 있다. 두 가지 방식으로, 첫째, 쿠키는 로그인 정보(예컨대 이름, 주소, 비밀번호 등)를 불러내는 데에 사용도리 수 있다. 둘째, 쿠키에 담긴 정보와 마케팅 데이터베이스에 있는 이용자의 이름, 주소, 이전의 소비경보 등을 상호 비교함으로써 이용자의 신원 확인이 가능하다.
웹 버그(web bug)	웹 버그는 온라인 이용자가 모르는 사이에 이용자에 관한 정보를 유출해 가거나 심지어 이용자의 시스템을 파괴할 수도 있는 기술이다. 웹 버그는 web page에 심어 놓은 매우 작은 그래픽이미지 파일로, 통상 해당 web page의 바탕화면과 같은 색을 지니기 때문에 육안으로는 거의 보이지 않는다.
스파이웨어(spyware)	무료 또는 유료로 배포되는 소프트웨어에 들어 있는 일종의 프로그램 모듈을 통칭하는 것으로, 해당 소프트웨어를 설치한 컴퓨터 이용자가 인터넷을 서핑할 때 이용자의 개인 정보나 온라인 활동 정보를 스파이웨어를 설치한 회사의 서버에 지속적으로 전송하는 것이 주된 기능이다.
고성능 스파이웨어 기술	스파이웨어 기법이 한 단계 진보한 기법으로, 스파이웨어를 탐지하기 위해 사용되는 백신이나 안티 스파이웨어 솔루션 등을 우회하기 위해, 스파이웨어를 통해 수집된 정보를 작은 크기로 나누어 컴퓨터의 파일 시스템 상에 보이지 않는 틈새공간(slack space)에 임시 정장한 다음, 특정 시간대에 내외부의 특정인에게 전송하는 방법을 이용한다. 이러한 기법은 정부의 수사기관에서 범죄자의 감시 및 경쟁사에 대한 정보 수집, 간첩정보 수집에 이용된 사례가 있다.
WLAN 환경	WLAN 사용자가 액세스 포인트에 접속할 때, 해커가 가상의 액세스 포인트를 이용하여 사용자의 중요한 개인정보를 모니터링하게 된다.
웹 메일의 첨부 파일 유출	웹 메일 첨부 파일 유출기법은 기존 e-mail이나 웹 메일을 모니터링하여 데이터를 유출하는 방식에서 한 단계 진화하여, 웹 메일에 첨부된 파일을 encoding하는 방식으로 주로 기업이 운용하는 메일 모니터링 프로그램을 우회하여 기밀정보를 유출하는데 사용된다.
Stegenography	이미지 및 오디오 파일에 중요한 파일이나 메시지를 첨부할 수 있는 스테가노그래피 기법이 확산될 전망이다. 이 기법은 오사마 빈 라덴이 알카에다 조직원과의 연락을 위해 사용된 것으로 보고되면서 널리 알려졌다.
접속 세탁 (connection laundering)	접속 세탁 기법은 해커들이나 해커 집단간 공간 창조를 통해, 해커 역추적 경로 파악을 어렵게 만드는 것으로, 해커가 여러국가를 경유하여 해킹을 할 경우, 중간 단계에 해커 그룹이 운용하는 기명경로(ancoymizer)를 거쳐 해커에 대한 역추적이 불가능하게 하는 방법이다.
위치측정 경보 침해	GPS 또는 휴대전화기의 위치측정 내용을 인터넷을 통해 확인할 수 있게 되어, 개인의 위치 정보가 유출되어 개인의 신변에 위협이 도리 수 있다.

<표 2> 개인정보 보호 기술 요약표

보호 기술	방 법
P3P (Platform for Privacy Preference)	P3P는 W3C(World Wide Consortium)에서 개발한 개인정보보호 표준 기술 플랫폼으로서 웹 사이트에서 이루어지는 데이터 처리에 관한 표준을 제시한다. P3P의 목표는 웹 사이트 운영자에게 이용자 자신의 정보를 관리할 수 있는 권한을 넘겨주는 것이며, 이용자 정보가 잘못된 방법으로 사용되지 않도록 보호하기 위해 만들어졌다.
프라이버시 정책 생성 (Privacy Policy Stabements Generactor)	OECD가 1980년에 발표한 '프라이버시 보호 및 개인 정보의 국가간 유통에 관한 지침'에 따라 개발되었고, 프라이버시 정책 문구를 자동적으로 생성하는 기능을 가지고 있다. 특히 정보보호 생성 소프트웨어가 요구하는 절차에 따라 실제 운영 중인 개인정보 보호방침을 입력하면, 해당 기업이나 조직의 개인정보 보호 방침 문구를 HTML문서로 자동 작성하여 출력하는 기능을 갖고 있다.
쿠키 관리(통제)	이용자로 하여금 언제 쿠키가 자신의 컴퓨터에 저장되는 지를 결정하게 함으로써 쿠키의 수용 여부를 결정하고 관리하도록 하며, 개별적인 쿠키에 저장된 정보가 무엇인지를 판단할 수 있는 방법으로, 개인에게 자신의 컴퓨터에 저장된 쿠키에 대해 통제권을 주는 방법이다.
암호화 소프트웨어 (Encryption Software)	암호화 소프트웨어는 암호화를 통해 자신의 e-mail 메시지, 저장된 파일, 그리고 온라인에서의 커뮤니케이션을 보호할 수 있게 하는 기능을 제공한다. 한 번 암호화가 이루어지면 오직 그 당사자만 암호화된 정보에 대한 디지털 키를 가지고 그 정보를 열람하며, 디지털 키는 브라우저, 생체 인증, 스마트카드 등과 결합하여 생성된다.
익명화 기술 (Anonymizers)	익명화는 클라이언트와 웹 사이트 간에 중개자 역할을 수행함으로써 이용자가 익명으로 웹을 서핑하도록 하는 서비스를 제공한다. 일반적으로 익명화 서비스는 웹 사이트가 방문객의 IP 주소를 식별하거나 쿠키를 개인의 컴퓨터에 저장하는 것을 막아줌으로, 소비자가 웹을 브라우징하거나 보내는 이가 누구인지 알 수 없도록 익명화된 메일을 보낼 때 유용하다. 그러나 이러한 기능은 반대로 개인화된 서비스나 온라인 계정관리, 과거의 구매기록 보관 또는 열람 등에 대한 특정한 기능을 사용할 수 없게 한다.