情 報 保 護 學 會 誌
第 14 券 第 1 號, 2004. 2

유비쿼터스 컴퓨팅과 보안요구사항 분석

조 영 섭*, 조 상 래*, 유 인 태**, 진 승 헌*, 정 교 일***

요 약

언제, 어디서나 사용자가 접속하여 원하는 정보와 서비스를 제공 받을 수 있도록 컴퓨터를 실생활 환경에 편재시키는 유비쿼터스 컴퓨팅(Ubiquitous Computing)은 차세대 컴퓨팅을 주도할 개념으로 급부상하며 많은 연구 개발이 진행되고 있다. 본 고에서는 유비쿼터스 컴퓨팅의 개요와 연구 동향 및 기술 발전 방향에 대하여 살펴본다. 또한, 유비쿼터스 컴퓨팅의 보안 요구사항을 고찰한다. 유비쿼터스 컴퓨팅의 보안 요구사항은 유비쿼터스 네트워크 환경에서의 보안요구 사항과 유비쿼터스 응용 환경에서의 보안요구 사항으로 분류하여 분석한다.

Ⅰ. 서 론

유비쿼터스 컴퓨팅의 개념은 1998년 XEROX Palo Alto 연구소의 Mark Weiser가 차세대 컴퓨팅의 비전으로 제시한 쉬운 컴퓨터에서 출발하여 일상생활에 컴퓨터를 심어 모든 사물 및 공간이 지능화되고 언제 어디서나 제한 없는 접속을 통해 서비스를 제공하는 것으로 발전해왔다.

10년 전 Mark Weiser의 비전이 제시되었을 때는 당시의 기술로는 불가능한 것으로 많은 사람들이 생각하고 있었다. 그러나 마이크로프로세서의 지속적인 가격 하락과 소형화에 따라 더욱 많은 사물에 칩을 내장시킬 수 있게 되었으며, 센서의 기능 향상으로 사물의 식별과 위치 확인이 용이해졌으며 통신기술의 진보에 따라 사물간의 통신이 훨씬 쉬워짐에 따라 유비쿼터스 컴퓨팅 개념의 실현이 가능해 지고 있다. 유비쿼터스 컴퓨팅은 도시혁명, 산업혁명, 정보혁명에 이어 인류 역사상 네 번째의 혁명을 불러일으킬 정도로 그 파급효과가 클 것으로 예상되며 현재 많은 국가에서 전략적으로 연구가 진행되고 있다. 유비쿼터스 컴퓨팅은 웨어러블 컴퓨팅(Wearable Computing), 노매딕 컴퓨팅(Nomadic Computing), 퍼베이시브 컴퓨팅(Pervasive Computing) 등 다양한 방향으로 연구가 진행되고 있다. 유비쿼터스 컴퓨팅이 현실화 되면 사용자는 의식하지 않고 인비저블(Invisible) 형태의 편재된 컴퓨팅 서비스를 제공받을 수 있을 것이다. 이러한 서비스를 제공하기 위해 유비쿼터스 컴퓨팅에서는 기존의 컴퓨팅 환경에 비해 더욱 더 많은 사용자 정보를 수집하게 된다. 또한 유비쿼터스 컴퓨팅은 사용자의 위치를 추적하면서 사용자를 인지하여 서비스를 제공하기 때문에 사용자의 위치 정보를 수집한다.

그러나 이러한 유비쿼터스 컴퓨팅의 특성은 데이터의 보안이 취약할 경우 기존 컴퓨팅 환경보다 더 큰 문제를 발생시킬 수 있다. 또한 수집된 데이터가 오·남용될 경우 사용자에 대한 감시 시스템(Surveillance System)으로 동작할 수도 있다. 이러한 문제는 실제 유비쿼터스 컴퓨팅이 현실화되는데 있어 때 가장 큰 걸림돌로 작용할 수 있다.

본 고에서는 유비쿼터스 컴퓨팅을 실현하기 위해 필수적으로 해결해야 하는 보안 요구사항을 분석한다. 이를 위해 무선통신을 중심으로 유비쿼터스 네트워크 상에서의 보안위협을 분석하고 이를 해결하기 위한 보안요구사항을 도출한다. 또한 유비쿼터스 컴퓨팅의 응용 환경에서의 보안 요구사항을 분석한다. 유비쿼터스 응용 보안 요구사항을 분석하기 위해 하나의 실현가능한(Feasible) 유비쿼터스 컴퓨팅 사용 시나리오를 도출하고 이를 지원하는 유비쿼터스 컴퓨팅 환경인 Smart Space를 정의하고 이를 통해 정의된 Smart Space

* 한국전자통신연구원 정보보호연구단 정보보호기반연구그룹 인증기반연구팀 ({yscho,sangrae,jinsh}@etri.re.kr)
** 경희대학교 전자정보대학 부교수 (itryoo@khu.ac.kr)
*** 한국전자통신연구원 정보보호연구단 정보보호기반연구그룹장 (kyoil@etri.re.kr)

에서 발생하는 보안 요구사항을 분석한다.

본 고의 구성은 다음과 같다. 2장에서 유비쿼터스 컴퓨팅의 개요와 연구동향 및 기술 발전 방향에 대하여 기술한다. 3장에서는 무선 네트워크를 기반으로 한 유비쿼터스 네트워크 환경에서의 보안 위협 및 보안 요구사항에 대하여 기술한다. 4장에서는 실현가능한 유비쿼터스 컴퓨팅 사용 시나리오를 도출하고 이를 지원하는 유비쿼터스 컴퓨팅 환경인 Smart Space를 정의하여 유비쿼터스 응용 환경에서의 보안 요구사항을 분석한다. 마지막으로 5장에서 결론을 맺는다.

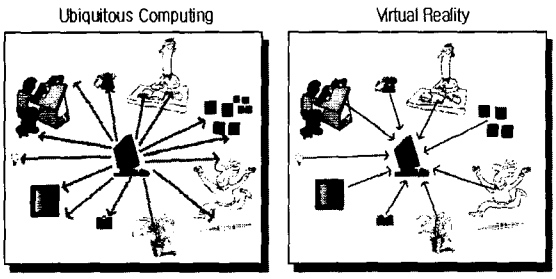
Ⅱ. 유비쿼터스 컴퓨팅

1. 유비쿼터스 컴퓨팅 개요

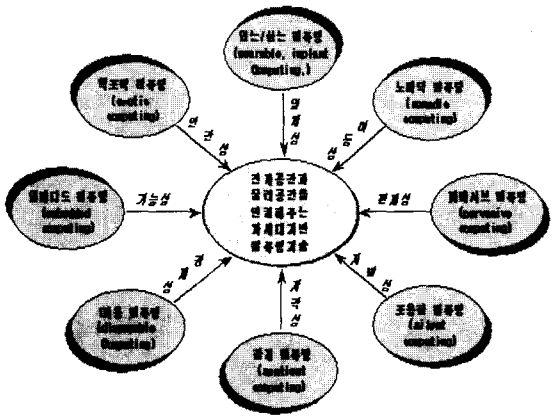
Mark Weiser에 의해 제시된 유비쿼터스 컴퓨팅은 일상 환경과 사물들에 컴퓨터가 보이지 않게 심어져 있어 서로간의 정보 교환이 가능하며, 사용자는 컴퓨터라는 거부감을 느끼지 않고 언제, 어디서나, 도처에 존재하는 즉 편재되어 있는 컴퓨터를 편리하게 사용할 수 있는 컴퓨팅 환경이다. 기존 가상현실이 특수한 전용 의복 등을 착용하여 컴퓨터 안에서 실세계와 같은 경험을 얻을 수 있는데 반해, 유비쿼터스 컴퓨팅은 사물과 환경으로 구성되는 물리적인 공간에 컴퓨터가 스며들어가고 이러한 컴퓨터가 도처에 편재되어 일상생활에 통합되는 것이다.

〔그림 1〕은 유비쿼터스 컴퓨팅과 기존의 가상현실 공간간의 차이점을 보여준다.

실세계에 편재되는 유비쿼터스 컴퓨팅 기술은 다양한 방향으로 발전되어 오고 있다. 컴퓨터를 옷이나 안경처럼 착용할 수 있게 하여 서비스를 제공하는 웨어러블 컴퓨팅, 다리, 빌딩, 자동차 등과 같은 사물에 컴퓨터 칩을 이식하여 사물을 지능화 하는 임베디드 컴퓨팅(Embedded Computing), 컴퓨터가 매우 작고



〔그림 1〕 유비쿼터스 컴퓨팅과 가상현실
출처:http://www.ubiq.com/hypertext/weiser/VRvsUbi.gif



〔그림 2〕 전자공간과 물리공간을 연결하는 유비쿼터스 컴퓨팅
출처:유비쿼터스 IT혁명과 제3공간, 하원규 외, 2002

저렴화 되어 1회용 종이처럼 사용할 수 있도록 하는 1회용 컴퓨팅(Disposal Computing) 그리고 IBM에서 제시된 개념으로 어디든지 어떠한 사물이든지 컴퓨터를 심어 도처에 컴퓨터가 편재되도록 하는 퍼베이시브 컴퓨팅 등 다양한 분야로 발전되고 있다. 이러한 다양한 분야는 모두 유비쿼터스 컴퓨팅의 하나의 분야로 생각할 수 있다. 〔그림 2〕는 유비쿼터스 컴퓨팅과 연계된 기술을 도식화 한 것이다.

2. 유비쿼터스 컴퓨팅 연구 동향

본 절에서는 미국, 유럽, 일본의 유비쿼터스 컴퓨팅 연구 동향을 기술한다.

2.1 미국

미국에서는 유비쿼터스 컴퓨팅에 대한 연구가 정부, 대학, 기업 등 다양한 주체에 의해 진행되고 있다.

정부 차원의 유비쿼터스 컴퓨팅 연구로는 DARPA, NIST 등을 중심으로 진행되고 있다.

DARPA의 정보처리기술국(IPTO)은 유비쿼터스 컴퓨팅과 관련된 대표적 프로젝트인 Smart Dust 및 Endeavour 프로젝트, Info-Sphere 프로젝트, Portolano, Aura 및 Oxygen 프로젝트 등을 지원하고 있다.

미 국립 표준기술원(National Institute of Standards and Technology)의 정보기술응용국(ITAO)은 첨단 기술 프로그램(Advance Technology Program)으로 퍼베이시브 컴퓨팅(Pervasive Computing)을 지원하고 있다.

NIST 산하의 정보기술연구소(Information Tech-

nology Laboratory)는 퍼베이시브 컴퓨팅 프로그램을 통해 일상생활 및 활동과 컴퓨터를 통합하기 위해 자연스러운 형식의 인간-컴퓨터 상호작용(Human-Computer Interaction)의 필요성을 강조하며, 동시에 스마트 공간 통합(Smart Space Integration), 퍼베이시브 소프트웨어 도구(Pervasive Software Tools), 퍼베이시브 네트워킹 기술(Pervasive Networking Technology) 등의 연구 프로그램을 지원하고 있다.

대학 및 연구소 차원에서는 다음과 같은 다양한 연구가 진행되고 있다.

버클리 대학에서는 Smart Dust라고 하는 1mm 크기의 실리콘 모트(Silicon Mote)에 자율적인 센싱과 통신 플랫폼 능력을 갖춘 보이지 않는 컴퓨팅 시스템에 대한 연구가 진행 중이다. 워싱턴 대학에서 보이지 않는 사용자 인터페이스, 보편적 접속, 지능화 서비스를 통해 이용자가 의식하지 않는 컴퓨팅 환경의 실현을 통해 현실세계와 가상세계를 결합하는 것을 목적으로 하는 Portolano 프로젝트를 진행하고 있다. MIT에서는 DARPA와 기업체로부터 총 5,000만 달러의 연구기금을 지원받아 Oxygen 프로젝트를 진행하고 있다. Oxygen 프로젝트는 특별한 사용자와 시스템 기술들을 조합하여 퍼베이시브하며, 인간 중심형 컴퓨팅 기술을 가능하게 하고, 음성, 비전 기술들을 이용하여 우리가 다른 사람과 이야기 하는 것처럼 시간과 노력을 절약시키는 것을 목적으로 하고 있다. 이외에도 MIT의 생각하는 사물 프로젝트, Auto-ID Center, 카네기 멜론 대학의 Aura 프로젝트 등 다양한 연구가 진행되고 있다.

기업 차원에서는 다음과 같은 연구가 진행되고 있다.

Xerox사는 PARC(Palo Alto Research Center) 연구소를 통해 세계 최초로 유비쿼터스 컴퓨팅 개념을 제시하였다.

AT&T 사는 고도의 이용가능성이 있는 컴퓨팅(Ultravailable Computing) 서비스 전략을 가지고 글로벌 e-Business를 수행하는데 있어 유연성, 서비스 질 보장, 확장성, 안정성, 재앙에 대비한 컴퓨팅 환경을 제공한다.

IBM은 다음과 같은 프로젝트를 진행 중이다.

- Deep Computing : data의 복잡성과 관련된 문제해결
- 자율(Autonomic) 컴퓨팅 : 스스로 알아서 인간을 대신하는 컴퓨팅
- meta pad : 3인치 정도의 포터블 컴퓨터

Microsoft 사 역시 다음과 같은 유비쿼터스 관련 연구를 진행하고 있다.

- SmartMoveX 프로젝트 : 빌딩 내에 있는 사람과 사물의 위치를 측정, HW/SW로 나타내는 것을 실현해 주는 액티브 배지 시스템
- Easyliving 프로젝트 : 컴퓨팅 생활공간 창조, 현실공간+센싱 및 세계 모델링(Sensing & World Modeling)+분산 컴퓨팅 시스템의 결합

Intel 사의 경우에는 SoC와 MEMS를 중심으로 다기능 칩과 기계/로봇에 탑재 가능한 프로세서를 개발중이며, Accenturer 사는 유비쿼터스 정부(U-government) 및 유비쿼터스 상거래(U-commerce)에 대한 연구를 진행하고 있다. HP 사는 모바일 환경에서 멀티미디어 데이터 처리가 가능하고, 사용자는 웹에 항상 접근 가능하며, 실세계와 사이버공간이 자연스럽게 연결되는 환경을 목표로 하는 Cooltown 프로젝트를 진행하고 있다.

2.2 유럽

유럽은 2001년에 시작된 EU의 정보화사회기술계획(IST)의 일환으로 미래기술계획(FET, Future and Emerging Technology)이 자금을 지원하는 사라지는 컴퓨팅(Disappearing Computing)을 중심으로 유비쿼터스 컴퓨팅에 대한 대응 전략을 모색하고 있다.

사라지는 컴퓨팅은 정보기술을 일상사물 및 환경 속에 통합하여 인간의 생활을 지원하고 개선하고자 하는 것을 목적으로 하고 있다. 흔히 사용하는 일상 사물에 센서, 구동기, 프로세서 등을 탑재하여 사물 고유의 기능에 정보처리 및 교환 기능이 증진된 정보 인공물(Information Artifacts)의 고안과 정보 인공물 상호간의 지능적이고 자율적인 감지와 무선통신을 통해 새로운 가능성과 가치를 창출하고, 궁극적으로는 인간의 일상 활동을 지원 및 향상시킬 수 있는 환경 구축을 목표로 한다. 이러한 목적을 달성하기 위해 연구소, 대학 및 기업 공동으로 연구하고 있는 "Smart Its", "Paper++", "Grocer" 등 16 개의 독립 프로젝트를 지원하고 있다.

또한 유럽은 미래 기술로 엠비언트 인텔리전스(Ambient Intelligence)에 관한 연구가 활발히 진행되고 있다. 주로 위치, 시간 등에 따른 상황인식 및 멀

티미디어 중심의 서비스 관련 연구와 홈 네트워크, 센서 망, 단말 등에 관한 플랫폼 연구가 이루어지고 있다.

■ Smart-Its 프로젝트

사라지는 컴퓨터 이니셔티브(Disappearing Computer Initiative)의 연구 프로젝트 중에서 가장 대표적인 것으로 스위스의 ETH, 독일의 TecO, 핀란드의 VTT, 스웨덴의 Interactive Institute, 영국의 Lancaster university 등이 수행하고 있다.

이 프로젝트의 목표는 일상사물의 지능화와 지능화된 사물간의 커뮤니케이션이다. 즉 Smart dust와 유사한 기능을 가진 지능형 센서를 우리가 일상생활에서 사용하는 일용품에 부착하고, Bluetooth와 같은 무선 통신 환경 하에서 상호 통신하여 사용자에게 유용한 서비스를 제공하는 것이다.

- 일상사물의 지능화 : 사물에 소형의 내장형 디바이스인 "Smart-Its"를 삽입하여 감지, 인식, 컴퓨팅 및 무선통신 등의 기능을 지닌 정보 인공물(Information Artefacts) 개발
- 지능화된 사물간의 커뮤니케이션 : 사물간의 협력적인 상황인식 및 활동

■ Paper++ 프로젝트

영국의 Kings College, HP 연구소, 독일의 Anitra, 스위스 ETH, 프랑스의 Arjo Wiggins 등이 공동으로 진행하고 있다. 센서가 포함되어 있는 투명한 잉크와 단순한 위치 기반 디바이스를 이용하여 종이의 기능을 향상시키는 것이 목적이며 주로 책이나 학습 자료와 같은 교육용 어플리케이션 개발에 중점을 두고 있다.

■ Grocer 프로젝트

스페인의 Navarra 대학에서 추진하고 있으며 식료품 가게의 개별상품에 블루투스, WAP, RFID 등과 같은 통신 기능을 갖는 마이크로프로세서를 식재하여 장소에 구애받지 않고 소비자는 PDA나 휴대전화 등을 통해 상품을 구매할 수 있으며, 관련 상품의 광고를 제공받을 수 있도록 하는 것을 목적으로 하고 있다.

2.3 일 본

일본의 유비쿼터스 컴퓨팅 연구는 "어디에나 컴퓨터 환경"이라는 미래를 겨냥한 신기술 체제의 확립을 목표로 1984년 동경대학 사카무라 겐(坂村 健) 교수가 중심이 되어 제안한 TRON 프로젝트(The Realtime Operating System Nucleus Project)에서 출발한다.

이 프로젝트의 기본 개념은 미국의 Mark Weiser에 의한 유비쿼터스 컴퓨팅 연구보다도 앞선 것으로 모든 컴퓨터의 기본소프트웨어(OS)를 공통화하여 제작자, 기종의 종류에 관계없이 호환성을 실현하는 환경을 구축하는 것이다.

현재 일본에서 준비하고 있는 유비쿼터스 대응 전략은 물리공간에 존재하는 모든 물체 및 생활공간 그리고 사람이 착용하는 의복, 안경, 신발, 시계 등의 신변용품 등에 다양한 기능을 갖는 마이크로컴퓨터 칩들이 이식되고 상호간에 연결됨으로써 "언제 어디서나 컴퓨터의 능력이 발휘되는 네트워크의 편재화" 즉, 유비쿼터스 네트워크가 산·학·관의 연계 연구로 진행되고 있다.

총무성은 2001년 11월 27일 "유비쿼터스 네트워크 기술의 장래 전망에 관한 조사연구회"를 만들고, 유비쿼터스 네트워크 기술에 관한 국·내외 연구개발 동향 등을 조사 및 분석하였다. 또한, 종합과학학술회의 및 IT 전략본부에서의 검토상황과 "e-Japan 전략", "e-Japan 중점계획" 등에 입각하여 유비쿼터스 네트워크 사회의 실현을 위하여 대응해 가야할 연구개발 과제나 연구개발 추진대책 등에 대하여 검토하고 있다. 또한 총무성 주관으로 민간, 대학, 정부관련 부처 전문가들로 구성된 '유비쿼터스 포럼'을 정식 발족시켜(2002.6.11.) 차세대 국가 정보화 방향인 유비쿼터스 정보기반 구축에 본격적으로 나설 것임을 천명한 바 있다.

현재 2005년까지 "무엇이든, 어디서든 네트워크"의 요소기술의 확립을 위한 연구개발 프로젝트를 추진하고 있다. NTT, NTT 도꼬모, SONY, 샤프, 도시바, 일본전기 등이 참여하고 있다.

3. 유비쿼터스 컴퓨팅 기술 발전 방향

유비쿼터스 컴퓨팅과 같은 개념으로 통용되는 유선·무선·근거리 무선 통신 영역을 기반으로 하는 퍼베이시브 컴퓨팅은 다양한 단말들이 발산하는 대량의 정보를 수렴하기 위하여 슈퍼 서버 컴퓨팅과 온라인의 실시간 정보처리기술을 주요한 이슈로 삼고 있다. 이러한 사실로 미루어 보면 미래 기술의 구체적인 모습은 근거리 통신 기반의 초소형 내장형 컴퓨터로 이루어지는 망기반의 복합응용으로 판단된다. 따라서 네트워크로 연결된 지능형 컴퓨팅에 의해 구축되는 환경에

〔표 1〕 유비쿼터스 네트워크 기술 분류

기술유형	세부기술내용	
유비쿼터스 시스템기술	- 프렉시블 퍼스널라이즈드 시스템기술 - 고정밀 광역 위치특정 기술 - 환경정보처리/배신 시스템 기술 - 뉴 테크놀러지 적응형 네트워크 아키테처기술 - 실시간OS기술	- 모빌리티 제어·관리기술 - 프로필 포터빌리티 기술 - 고도 센싱 시스템 기술 - 데이터 GRID 기술 - 유비쿼터스 어드레스 운용·관리 시스템기술
고성능 네트워크기술	- 이종 네트워크간 무결절 접속기술 - 네트워크 총괄형 Zero Administration 기술 - 네트워크간 QoS 기술 - 플렉시블 경로제어 기술	- 포토제닉 네트워크 기술 - 풀 IPv6 네트워크기술 - 네트워크 부하 분산기술 - 대용량무선기술
애플리케이션 고도화 기술	- U-에이전트 기술(기기설정기술, 정보검색기술, 에이전트간 협상기술, 리마인더 시스템기술) - 고 현실 영상 스트리밍 배신 기술 등	- 인텔리전트 콘텐츠 기술 - 트랜스 코딩 기술 - 다언어 대응 화상·음성융합 인식처리 기술
어플라이언스 기술	- 초소형 원 칩 컴퓨터기술 - 저소비·장수명 전력기술 - 전자이종기술	- 오감활용 인터페이스 기술 - 유기EL 기술 - 복수 미디어 대응단말기술 등
플랫폼기술	- IC 카드 고도 인증기술 - 개인인증기술(바이오메트릭스 인증기술, DNA 개인인증기술) - 자기최적형 보안 시스템 기술	- 컴팩트 보안 실시간 프로토콜기술 - 고기능과금·결제 시스템 기술 등 - DRM 기술(동화음영 기술, 개작·정취 방지기술)등

서 인간은 명령하지 않아도 자율형 컴퓨팅 서비스를 받는 생활을 하게 될 것으로 예측된다.

유비쿼터스 컴퓨팅 시대는 서버, PC 중심의 컴퓨팅 기술에서 AV기기, 정보가전, 휴대전화, 게임기, 제어기기 등과 같은 다양한 기기가 접속됨에 따라 소형화기술, 휴대전화기술, 정보가전기술, 전자제어기술, 네트워킹 제어기술 등이 주요한 원천 기술로 대두될 것으로 예측된다.

표 1은 일본의 유비쿼터스 네트워크 프로젝트의 기술 분류에 대한 것이다.

Ⅲ. 유비쿼터스 네트워크 보안 요구사항 분석

본 장에서는 무선통신을 중심으로 한 유비쿼터스 네트워크 환경에서의 보안위협을 분석하고 이를 해결하기 위한 보안 요구사항에 대하여 기술한다.

1. 유비쿼터스 네트워크 환경의 보안위협

유비쿼터스 컴퓨팅 환경은 무선통신을 기본으로 장치들 간에 통신을 하게 된다. 따라서 본 절에서는 유비쿼터스 컴퓨팅 환경의 보안 요구사항을 도출하기 위해서 우선 현재 무선 네트워크 환경을 중심으로 유비쿼터스 컴퓨팅 환경에서의 보안위협을 설명한다.

유비쿼터스 네트워크 환경에서 발생할 수 있는 위협으로는 장치의 절도 및 분실, Rogue AP, IP 스푸핑(Spoofing), DoS 공격, 트로이목마, 웜, 바이러스 등, 신호방해 공격, 배터리 소진 공격 등이 있다.

1.1 장치의 절도 및 분실

장치의 절도 및 분실은 기밀성에 대한 위협으로 유비쿼터스 장치가 분실되어 공격자가 접근해서는 안 되는 정보를 접근 및 수신할 수 있어 기밀성이 손상된다. 또한 유비쿼터스 장치를 소유한 사람은 유비쿼터스 장치에 저장된 MAC 주소와 WEP 키 등 인증정보를 소유하게 되기 때문에 이러한 인증 정보들을 사용하여 어떠한 네트워크에 대한 접근 권한을 얻을 수 있다. 따라서 네트워크 침해로 이어질 수 있으며 공격의 일부로서 정보를 요청할 수 있다. 이것은 유비쿼터스 장치가 사용자가 아닌 장치에 대한 인증을 요구할 경우 발생한다.

1.2 Rogue 엑세스 포인트

대부분의 기존 인증은 공개키 암호시스템 기반으로 신뢰기관에 의해 발급된 공개키인증서를 바탕으로 인증하고자 하는 개체의 서명을 통해 이루어진다. 유선에서 사용되는 커버로스(Kerberos)에서부터 공개키 인증서(Public Key Certificates)를 이용한 인증방법은 인증을 위해 인증 서버나 폐지 서버에 온라인

(On-line)으로 연결해야 한다. 그러나 유비쿼터스 네트워크 환경은 고정된 망 구조가 없으며 수시로 망구조가 변경되기 때문에 망의 기반 시설이 존재하지 않는다. 따라서 중앙집중형 온라인 서비스 제공이 어렵다. 또한 네트워크 장치가 일시적으로 네트워크에 연결되며, 그 연결은 확실한 연결성을 보장하지 않는다. 따라서 인증 서비스에 대하여 근본적인 문제를 가지고 있다. 무선랜의 경우 단 방향 인증만을 제공하게 되면, 하나의 엑세스 포인트가 한 사람의 사용자를 인증하지만, 사용자는 엑세스 포인트를 인증하지도 인증할 수도 없다. 따라서 Rogue 엑세스 포인트가 무선 LAN에 위치하면, 공격자는 엑세스 포인트에 대한 인증 없이 네트워크 접근이 가능하게 되고, 그것은 정식 사용자의 클라이언트에 대한 하이재킹(Hijacking)을 통해 서비스 거부 공격의 거점이 될 수 있다는 취약점이 알려져 있다.

1.3 IP 스푸핑(Spoofing)

IP 스푸핑은 기밀성에 대한 위협이다. 무선 신호는 건물의 벽을 통과할 수 있기 때문에 건물 외부로 전달될 수 있고, 적어도 무선 신호 범위 내에 존재하는 어느 누구나 무선 접속이 가능하기 때문에 전송되는 정보가 암호화되어 있지 않을 경우 공격자가 중요 정보를 도청할 위험이 항상 존재한다.

패킷별(Per-Packet) 암호화의 경우 공격자는 알려진 데이터 패킷의 응답으로부터 데이터 스트림을 재구성할 수 있기 때문에 다음 패킷을 스푸핑할 수 있다.

1.4. DoS 공격

DoS(Denial-of-Service) 공격은 가용성을 침해한다. 유비쿼터스 네트워크 환경은 앞에서 언급한 것처럼 고정된 망구조가 없으며 수시로 망구조가 변경되기 때문에 임시로 구성된 노드들 간에 데이터 교환을 위해서는 멀티 홉 라우팅 프로토콜에 의존하며 노드들은 인접한 노드의 패킷을 전송해 주어야 한다. 그런데 노드들 중 하나가 협력을 거부할 경우 DoS 공격으로 이루어진다.

배터리 소진 공격은 결국 DoS 공격으로 이어질 수 있다.

1.5. 트로이목마, 웜, 바이러스 등

트로이목마, 웜, 바이러스 등은 역시 유비쿼터스 장치에 위협을 가할 수 있다. 이들은 가용성에 영향을 미칠 수 있고, 기밀성과 무결성도 침해를 가할 수 있다.

1.6 신호방해 공격

신호방해 공격은 가용성을 침해한다. 무선 시스템에 대한 고전적인 공격은 통신 채널을 혼선시키는 것이다. 이러한 통신 채널의 혼선이 존재한다면 유비쿼터스 시스템은 정상적인 서비스를 제공 할 수 없을 것이다.

1.7 배터리 소진 공격

배터리 소진 공격은 유비쿼터스 장치의 배터리를 짧은 시간 내에 방출시켜 장치를 더 이상 사용하지 못 하게 만드는 것이다. 공격자는 계속적으로 공격 대상 장치에게 데이터 전송 요청이나 네트워크 연결 생성 요청을 보낸다. 이러한 공격이 네트워크 보안을 침해하지는 않지만, 결국에 장치가 제대로 기능을 할 수 없게 되어 사용자가 네트워크에 접속할 수 없게 만든다.

1.8 신원 정보 및 위치 정보 노출

메시지에 대한 기밀성은 메시지의 내용에 대한 비밀 유지를 가능하게 한다. 그러나 언제 누가 어디로 전달되는지는 메시지 기밀성만으로는 유지할 수가 없다. 이러한 정보는 공격자가 관심을 갖는 정보이기도 하지만 사용자의 프라이버시 문제이기도 하다. 또한 무선 환경에서 이동하는 사용자에게 서비스를 제공하기 위해서는 사용자의 위치가 추적되어야 한다. 그러나 사용자의 위치 정보가 제 3자에게 제공되지 않기를 원할 경우 프라이버시를 침해 할 것이다. 특히 유비쿼터스 컴퓨터 환경에서는 도처에 존재하는 유비쿼터스 장치와 수시로 정보교환이 이루어지기 때문에 사용자 위치정보 노출은 더욱 심각한 문제가 될 수 있다. 이 문제들은 기밀성 침해로 볼 수 있다.

표 2는 앞에서 설명한 유비쿼터스 네트워크 환경의 보안 위협을 정리한 것이다.

2. 유비쿼터스 네트워크 환경의 보안 요구사항

앞 절에서 설명한 유비쿼터스 네트워크 환경의 보안 위협에 대처하기 위해서는 현재 무선 네트워크 환경에서 보안 서비스로 주로 제공하고 있는 인증, 기밀성, 무결성 외에도 권한관리, 부인방지, 가용성, 익명성, 안전한 핸드오프 등의 추가적인 보안 요구사항이 제공되어야 한다.

2.1 기밀성

기밀성은 장치의 분실 및 도난, IP 스니퍼, 장치간의 동기화 등에 의해 침해될 수 있다. 기밀성을 유지하기 위해서는 다음과 같은 기능이 요구된다.

- 트래픽 데이터를 암호화한다.
- 키 관리 기법이 제공되어야한다.
- 이동형 장치는 중요한 정보를 암호화하여야 한다. 유비쿼터스 컴퓨팅 환경에서는 트랙픽 상에서 기밀성의 보호뿐만 아니라 유비쿼터스 장치 자체가 가지고 있는 정보에 대한 기밀성도 중요하다. 만약 장치를 분실하거나 도난당했을 때 저장된 정보는 암호화되지 않고 저장되어 있다면 공격자는 저장된 정보를 열람하고 유출시킬 수 있다.
- 서버 장치는 저장된 정보를 암호화하여야 한다. 여러 장치들과 통신을 하며 개인의 정보를 수집하는 서버 장치는 많은 사용자의 정보가 저장되기 때문에 저장된 정보를 비밀로 유지하는 것이 매우 중요하다.
- 저 전력 암호 알고리즘이 필요하다
  기밀성을 유지하기위해 선택할 수 있는 최선의 방법은 암호화이다. 따라서 유비쿼터스 장치의 특성에 맞는 저 전력 암호 알고리즘이 필요하다. 유비쿼터스 컴퓨팅에서의 기밀성을 보장하기 위한 에너지의 사용량이 중요한 고려사항이다. 유비쿼터스 컴퓨팅 장치는 모양과 크기가 다양하며, 주로 소형으로 휴대하는 장치들이 많다. 이로 인해 새로운 제약 조건이 생긴다. 이러한 장치들은 배터리 전력에 한계가 있어서 빠르고 계산 능력이 뛰어난 프로세서를 사용하는데 제약이 있다. 배터리는 유한하고 적은 에너지를 갖고 있기 때문에 사전 계산 방법은 그 순간의 처리 속도를 향상시킬 수는 있으나, 배터리의 소진 전력은 사전 계산을 한 것과 하지 않은 것의 차이가 없기 때문에 배터리 전력의 한계를 극복하지는 못한다. 많은 연산량을 갖는 공개키 암호시스템의 사용을 최대한 줄이는 방향으로 연구가 되어지거나, 효율성이 좋은 공개키 암호 시스템 연구가 필요하다.

〔표 2〕 유비쿼터스 네트워크 환경의 보안 위협

보안위협	침해 유형	원인 및 문제점	대응방법
장치의 분실 및 도난	기밀성 인증	장치 소유자가 인증 정보 소유	장치 독립적인 사용자 인증, 암호화
Rogue 엑세스 포인트	인증	단방향 인증 환경에서 공격자 엑세스 포인트가 인증없이 네트워크에 접근	양방향 인증
IP spoofing	기밀성	무선 신호가 원하지 않은 사용자에게 전달	암호화
DoS	가용성	가용성 침해	가용성
트로이 목마, 웜,바이러스	가용성 기밀성 무결성	가용성, 기밀성, 무결성 침해	백신 프로그램
신호 방해 공격	가용성	통신 채널 혼선	확산대역 주파수 호핑
배터리 소진 공격	가용성	짧은 시간 내에 배터리 소진	가용성
신원정보 및 위치정보 노출	기밀성	프라이버시 침해	익명성

2.2 무결성(Integrity)

장치의 분실 및 절도, 악의적 프로그램 등에 의해 무결성이 침해될 수 있다. 메시지 무결성을 유지하기 위해서는 암호학적인 메커니즘을 사용한다.

- 유비쿼터스 장치의 특징에 맞는 무결성 보장을 위한 암호학적 메커니즘이 필요하다. 무결성을 위해 전자서명을 사용할 경우 전자서명에 필요한 연산량이나 전력 소모량을 줄이거나, 유비쿼터스 장치의 특징에 맞게 메시지 무결성을 보장할 수 있는 암호학적 메커니즘이 필요하다.

2.3 가용성(Availability)

가용성은 DoS 공격, 악의적인 프로그램, 신호방해 공격, 배터리 소진 공격, 멀티 홉 라우팅 프로토콜에 의존하며 노드들 중 하나가 협력을 거부, 등에 의해 침해당할 수 있다.

DoS 공격의 해결 방안으로는 다음과 같은 것이 고려될 수 있다.

- 서비스 엑세스 우선순위
  중요하지 않은 요구에 대해 할당할 자원을 줄이고, 중요한 요구에 대해 자원의 할당을 늘리는 방식이다. 이것은 좀 더 중요한 서비스에 대하여 높은 우선순위를 할당하는 것이다.
- 대가 지불 서비스

비용을 지불하면 서비스를 제공하는 방법(Plutocratic Access Control)이다. 자원에 접근하기 위한 비용을 지불하기 전까지 서버는 클라이언트가 자원을 무분별하게 요청하는 것을 제한할 수 있다. 실제 과금하는 것이 비실용적이라면, 서버는 서비스 교환을 위해 약간의 비용이 드는 자원에 대한 희생을 강요함으로써 위의 방법과 같은 제한 전략을 사용할 수 있다 서버는 클라이언트에게 암호적인 퍼즐(Cryptographic Puzzle)을 풀게 하거나 인간이 대답하기는 쉽고 기계가 하기 어려운 질문을 하는 방법을 사용할 수 있다.

2.4 인증

동기화를 수행하는 유비쿼터스 장치, 장치의 분실 및 도난, Rouge 엑세스 포인트 등을 방지하기 위해서는 인증 서비스가 필요하다. 또한 유비쿼터스 컴퓨팅에서는 일시적이고 불확실한 연결을 제공하므로 인증을 위해 연결을 시도하는 과정에서 연결에 대한 불확실성으로 인해 합법적이지 않은 사용자에 대해 합법적인 사용자로 인증할 가능성이 발생한다. 따라서 불확실한 연결에 대비한 인증 솔루션이 필요하며, 연구되어야 한다.

유비쿼터스 환경에서 필요한 인증 방법은 다음과 같다.

- 상호인증을 제공해야 한다.
- 동적인 키를 사용해야 한다.
- 무선 구간 키 교환 기법을 제공해야한다.
- 장치 독립적인 사용자 인증이 필요하다.
  장치를 분실 및 도난당했을 경우 또는 여러 사용자가 공동으로 사용하는 장치의 경우 사용자에 대한 인증이 필요하다. 장치와 사용자 인증을 위해 사용될 수 있는 방법은 다음과 같다.
  - 장치인증 방법 : flash ID, device ID, ESN (Electronic Serial Number)
  - 사용자 인증 방법 : PIN 코드, 패스워드, 생체인증, 스마트카드 등
- PKI의 오버헤드 감소
  PKI는 기밀성과 무결성을 보장한다. 그러나 PKI 관리의 오버헤드, 추가적인 H/W, S/W 구입비용 증가 등의 문제가 해결되어야 한다.
- 서비스 제공을 위한 효율적인 인증/과금 방법이 필요하다.
- 안전 전이 협약이 필요하다.

기존 환경과는 달리 유비쿼터스 환경에서는 일시적이고 불확실한 연결이 많을 것이다. 따라서 어떤 개체가 일시적인 접속을 위해 인증 서비스 요구하는 경우가 많아질 것이다. 안전 전이 협약(Secure Transient Association)은 제어장치, 제어 대상 개체가 수시로 바뀜에 따라 협약 또한 수시로 바뀔 수 있음을 의미한다. 안전 전이 협약은 기존의 인증 시스템을 기반으로 하여 사용자 목적에 맞는 보안정책이 필요하다.

2.5 권한 관리

유비쿼터스 컴퓨팅 환경은 여러 가지 형태의 서비스가 제공될 것이다. 따라서 공공장소 등에서 여러 사용자가 자원을 공유할 수 있기 때문에 공유된 자원에 대한 접근제어가 필요하며, 공유된 장치에 대한 데이터의 기밀성도 보장되어야한다. 또한 서비스에 따라 자원을 사용하는 것에 대하여 과금할 수도 있다.

- 개체 식별과 검증
  서비스 제공자들의 신뢰정도를 식별하고 검증하는 것이다.
- 사용자 정보 접근 제어
  서비스 제공자의 신뢰수준에 따라 사용자 정보의 접근 정도를 다르게 해야 한다.

2.6 익명성(Anonymity)

암호화는 메시지의 내용이 무엇인지에 대한 기밀성 유지는 가능하지만, 통신 사실 자체를 비밀로 유지할 수가 없기 때문에 사용자의 통신 사실 및 위치 등에 대한 프라이버시를 완전히 보호하지는 못한다. 익명성은 이러한 사용자의 프라이버시 보호 측면에서 필요한 기능이다. 그러나 익명성이 보장될 경우 공격자의 추적이 어려울 수 있어, 위급한 상황에서는 관계기관에 사용자의 위치를 알릴 수 있는 기능이 필요하다. 따라서 유비쿼터스 환경에서는 사용자의 익명성을 보장할 수 있는 기술과 익명성을 선택적으로 제공받을 수 있는 방안이 함께 연구되어야 한다.

2.7 안전한 핸드오프

유비쿼터스 컴퓨팅 환경에서 무선 공중망을 이용하여 서비스를 제공할 경우 안전한 핸드오프 기술이 고려되어야 한다. 안전한 핸드오프는 사용자 인증, 키 관리정책, 암호화 알고리즘 협상, 그리고 과금 정책을

〔표 3〕 유비쿼터스 네트워크 환경의 보안 요구사항

보안 요구사항		추가 고려사항
기존 보안 요구 사항	인증	상호인증 동적인 키 사용 무선 구간 키 교환 기법 제공 장치 독립적인 사용자인증 PKI의 오버헤드 감소 집중형 인증/과금 방법 안전 전이 협약
	기밀성	키 관리 기법 이동형/서버 장치 내 데이터 암호화 서버 장치에 저장된 정보 암호화 저 전력 암호 알고리즘
	무결성	유비쿼터스 장치의 특징에 맞는 무결성 보장을 위한 암호학적 메커니즘
추가적인 보안 요구 사항	가용성	DoS 공격 서비스 엑세스 우선순위 대가 지불 서비스
	권한 관리	개체 식별과 검증 사용자 정보 접근 제어
	익명성	익명성에 대한 사용자의 선택 권한
	안전한 로밍	동일한 서브넷 내의 안전한 핸드오프 글로벌 로밍 서비스 핸드오프 과정에서 보안 접속 유지와 보안 컨텍스트 정의 및 관리, 분산인증 및 실시간 패킷 과금에 대한 문제

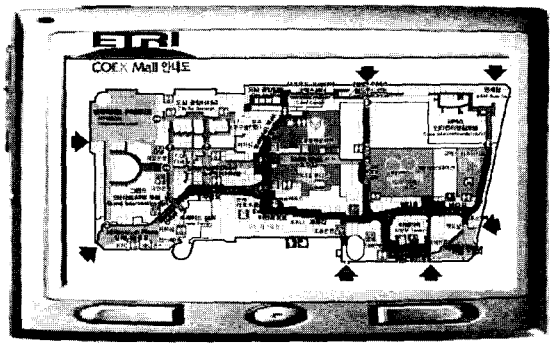
포괄적으로 고려하여 구현되어야 한다.

- 동일한 서브넷에서의 안전한 핸드오프
  동일한 서브넷에 위치한 엑세스 포인트 사이를 이동할 때 핸드오프 보안이 제공되어야 한다. 핸드오프 과정에서 보안 접속 유지와 보안 컨텍스트 정의 및 관리 등을 고려해야 한다.
- 글로벌 로밍 서비스
  무선 네트워크에서 글로벌 로밍 서비스가 제공되기 위해서는 분산인증 및 실시간 패킷 과금에 대한 문제를 해결해야한다.

표 3은 유비쿼터스 네트워크 환경의 보안 요구사항을 기술한 것이다.

Ⅳ. 유비쿼터스 응용 보안 요구사항 분석

본 장에서는 유비쿼터스 컴퓨팅 환경에서 실행 가능한 응용 시나리오를 도출하고 이 시나리오가 동작할 수 있는 유비쿼터스 컴퓨팅 환경인 Smart Space를 정의한다. Smart Space 상에서의 보안 요구사항을 도출함으로써 유비쿼터스 응용 보안 요구사항을 분석한다.



〔그림 3〕 PDA에 출력될 수 있는 가상 쇼핑몰 지도

1. U-쇼핑몰 시나리오

컴퓨터의 편재라는 목적을 가지는 유비쿼터스 컴퓨팅은 일상생활에서 실현될 수 있다. 유비쿼터스 컴퓨팅은 목적하는 실제 적용 환경에 따라 매우 다양한 형태를 갖게 된다. 이러한 다양한 유비쿼터스 컴퓨팅은 교통, 의료, 쇼핑, 회사, 정부 등 사회 전 분야에서 현실화될 수 있으며 적용되는 각 분야에 따라 그 형태가 달라질 수 있다. 본 절에서는 이러한 응용 환경 중에서 사용자가 일정한 물리적인 공간상에서 상품 구매와 개인 업무 처리를 제공하는 유비쿼터스 쇼핑몰(U-쇼핑몰: Ubiquitous Shopping Mall)의 시나리오를 도출한다. U-쇼핑몰의 사용 시나리오는 다음과 같을 수 있다.

Alice라는 사용자가 U-쇼핑몰에 들어선다. U-쇼핑몰은 Alice가 소지한 PDA에 쇼핑몰의 상점의 위치와 통로를 나타내는 기본 지도 정보를 제공한다. 다음 〔그림 3〕은 Alice의 PDA에 가상의 쇼핑몰의 지도가 표기되는 경우를 보이는 것이다.

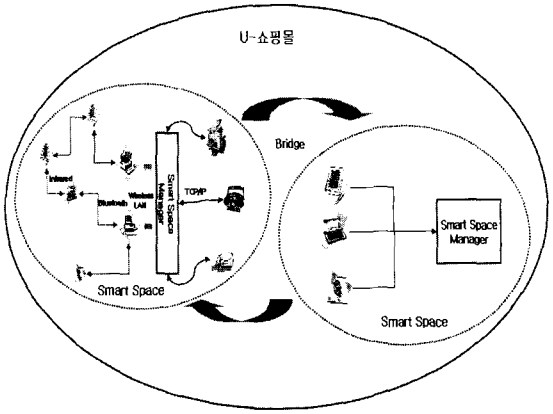
Alice의 PDA에 지도를 보여 준 후에, U-쇼핑몰은 Alice의 쇼핑 리스트를 조회하여 최적의 쇼핑 루트를 알려준다. Alice는 제시된 쇼핑 루트를 확인하여 비디오 상점을 먼저 들르는 것이 효율적이라는 사실을 알게 된다. Alice가 비디오 상점에 들어서면 상점에서는 그녀가 자연 다큐멘터리를 좋아한다는 사실을 자동으로 감지하여 해당 비디오 부스가 어디 있는지를 Alice의 PDA에 출력한다. Alice가 비디오를 고르는 순간 U-쇼핑몰에 Alice의 친구인 Bob이 들어온다. Bob은 U-쇼핑몰에서 Alice를 만나기로 약속했기 때문에 U-쇼핑몰에 Alice가 어디 있는지 자신의 PDA를 통해 물어본다. U-쇼핑몰은 Alice에게 Bob이 쇼핑몰에 들어왔음을 알리고 Alice는 식당에서 만나자는 메시지를 Bob에게 전달한다. 둘은 PDA에 출력된

식당의 위치를 확인하고 몇 분 후에 식당에서 만난다. 식당의 메뉴판은 오늘의 특선 요리가 무엇이고 어떠한 재료로 만들어졌는지 PDA에 자세히 설명한다. 두 사람은 이러한 메뉴 설명을 듣고, 게 요리를 주문한다. 식사를 마치고 Alice와 Bob은 아쿠아리움에 들어선다. 아쿠아리움을 거닐면서 물고기를 볼 때, 아쿠아리움은 Alice의 PDA에 물고기에 대한 자세한 설명을 출력해 준다. 아쿠아리움에 있을 때, Bob이 갑자기 배탈이 나고, Alice는 현재 위치에서 가장 가까운 약국의 위치를 U-쇼핑몰에 확인하여 약국으로 달려가 약을 Bob에서 먹인다. 그리고 둘은 U-쇼핑몰에서 나온다. U-쇼핑몰에서는 사용자의 전체 쇼핑 금액을 확인하여 적정 금액 이상이 구입되었음을 확인하고 주차비를 면제해 준다.

2. Smart Space

Smart Space는 앞 절에서 도출한 U-쇼핑몰 사용 시나리오에서 사용자와 상호작용을 수행하는 물리적인 최소 단위 공간이다. Smart Space는 기존의 물리적인 공간과는 달리 사용자의 위치를 감지할 수 있는 센서, 사용자에게 적절한 서비스를 제공하기 위한 컴퓨팅 파워, 사용자 디바이스 또는 다른 Smart Space간의 통신 능력을 가지고 있는 지능적인 공간이다. Smart Space에는 사용자 디바이스가 포함되는데 Smart Space에서는 일정 수준의 컴퓨팅 파워를 가지고 있는 PDA 또는 Notebook 등을 가정한다. U-쇼핑몰의 경우 비디오 대여점, 식당, 그리고 아쿠아리움 등이 Smart Space에 해당된다. U-쇼핑몰은 이러한 Smart Space 들이 상호작용을 수행하면서 사용자에게 다양한 서비스를 제공하는 공간이다. 다음 [그림 4]는 U-쇼핑몰의 컴퓨팅 환경을 구성한 개념도이다.

[그림 4]에서 보이듯이, U-쇼핑몰은 Smart Space와 이들 간의 상호작용을 지원하는 Bridge로 구성된다. Smart Space는 기본적으로 사용자가 소지한 디바이스와 통신 기능을 제공하며 Bluetooth나 Infrared를 사용한다. 사용자 디바이스는 노트북 또는 PDA, 휴대폰 등으로 구성된다. 또한 Smart Space는 사용자의 움직임을 감지하는 장치와 서비스를 제공하는 다양한 컴퓨팅 디바이스로 구성된다. 개개의 Smart Space는 각각 자신의 특성을 반영한 독립적인 서비스를 제공한다. 스마트 스페이스의 위치 정보에 대한 감지(Sensing)는 스마트 스페이스 관리자에 연결된



[그림 4] U-쇼핑몰 구성도

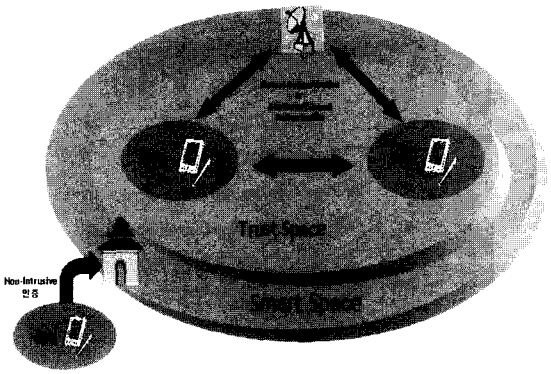
컴퓨터들에 의해 수행된다.

이러한 개개의 Smart Space는 Bridge를 통해 연결된다. Bridge는 Smart Space 들을 연결하는 기능을 제공하며 두 가지 연결 방법이 제공된다. 첫 번째는 단순한 연결로서, 사용자의 위치를 확인하거나 추적하는 등 단순 정보만을 서로 공유하는 기능을 수행한다. 두 번째는 지능적 연결로서, 사용 환경에 대한 Context를 확인하여 Proactive 와 같은 지능적인 서비스를 제공한다.

U-쇼핑몰은 이와 같이 Smart Space와 Bridge를 통해 기존의 Cyber Space와 물리적인 공간을 결합하여 지능적인 서비스를 제공한다.

3. Smart Space를 위한 보안 개념 모델

U-쇼핑몰에서 사용자는 자신의 ID, Attribute, Preference 등에 대한 정보를 디바이스에 저장한다. 이러한 정보는 개인에 대한 프라이버시 정보에 해당되기 때문에 디바이스에서 개인 프라이버시 정보가 누출되지 않도록 하는 프라이버시 보호 공간(Privacy Protection Space)이 구성된다. 사용자가 Smart Space에 진입하게 되면 Smart Space는 사용자의 진입을 확인하고 사용자의 개입을 없애거나 최소화하는 Non-Intrusive Authentication을 수행한다. 일단 인증을 거친 후에, 사용자는 다른 사용자들과 또는 서비스 제공자와 상호 작용을 하면서 서비스를 제공받게 된다. 이 때, 다른 사용자 또는 서비스 제공자와 상호 인증, 인가를 수행하게 된다. 이 때, 상호 인증, 인가가 가능하기 위해서는 서로간의 신뢰(Trust)를 구성하고 확인하는 Trust Space가 구성된다. 결국 Smart Space는 개인의 프라이버시를 보호하는



〔그림 5〕 Smart Space의 보안 개념 모델

Privacy Protection Space와 개인들 간의 또는 개인과 서비스 제공자간의 신뢰를 구성하는 Trust Space로 구성된다.

Smart Space가 제대로 동작하기 위해서는 여러 가지 보안 기능이 필수적으로 제공되어야 한다. 사용자의 개입을 최소화하는 Non-Intrusive Authentication, 유비쿼터스 컴퓨팅의 특성인 Context에 기반한 Access Control, 동적인 신뢰관리 그리고 개인정보에 대한 보호 기능을 제공하는 Privacy Protection이 필수적이다. 위 〔그림 5〕는 Smart Space에 대한 보안 관점에서 개념적인 모델을 도식화 한 것이다.

4. Smart Space 보안 요구 사항

앞 절에서 기술하였듯이, Smart Space는 개인의 정보보호 공간인 프라이버시 보호 공간, 신뢰 공간인 Trust Space 그리고 상호간의 인증 또는 인가에 의해 정보보호 기능을 제공한다. 본 절에서는 이들 정보보호 기능을 제공하기 위해 필요한 각각의 세부 보안 요구 사항에 대하여 기술한다.

4.1 Non-Intrusive Authentication

Smart Space에서 기존의 인증 기술을 적용하는 것은 여러 가지 문제를 발생시킨다. 즉 현재의 인증 기술은 매번 사용자의 개입(Intrusion)을 요구한다. 사용자가 서비스를 받기 위해서는 서비스 공간에 진입할 때 자신을 인증해야 한다. 그러나 Smart Space에서는 사용자의 진입이 매우 빈번히 그리고 동적으로 수행된다. 따라서 기존의 인증 방법은 Smart Space 환경에서는 적절하지 않게 된다. 또한 기존의 컴퓨팅 환경에서는 중앙의 TTP(Trusted Third Party)가 존재하여 사용자의 인증을 수행하게 되지만 Smart Space에서는 TTP를 구성하는 인프라가 존재하지 않게 된다. 사용자에게 패스워드를 요구하는 기존 인증 기술은 Smart Space를 넘나 들 때마다 매번 패스워드를 제출해야 하는 불편함을 초래하게 된다.

따라서 이와 같은 문제를 해결하기 위해서 Smart Space에서는 사용자의 개입이 없거나 또는 최소화하는 Non-Intrusive인증 기술을 제공해야 한다. Non-Intrusive 인증 기술은 다음과 같은 기술을 포함하여야 한다.

- 개입을 최소화하며 인증하기 위해서는 사용자의 속성 정보, 선호도 등과 같은 다양한 정보를 인증에 활용
- 이름, 주소, 전화번호 등과 같은 사용자 정보에 기반한 인증 기술
- 생체 인증과 같은 높은 강도의 인증 기술
- Smart Space에 따라 동적으로 변하는 인증 기법

4.2 프라이버시 보호

Smart Space는 사용자의 위치를 감지하며 서비스를 제공하게 된다. 이러한 사용자 위치 정보는 사용자가 어떠한 장소를 방문했는지에 대한 정보를 노출시키며 이들 정보는 사용자의 취미, 건강, 생활 패턴 등에 대한 정보의 유추가 가능하게 된다. 따라서 Smart Space에서는 기존의 컴퓨팅 환경과는 달리 사용자의 위치 정보를 보호하는 기술이 매우 중요하게 된다. 또한 Smart Space에서는 사용자에게 프로액티브(Proactive), 인비저블 서비스를 제공하기 위해서는 사용자의 Preference 등과 같은 다양한 정보의 수집이 필요하다. 이 때 이러한 정보의 오남용은 사용자 개인정보에 대한 중대한 침해를 가져올 수 있다. EU의 The Directive 등 많은 국가에서 법률적으로 개인정보 수집시 사용자의 명확한 동의를 얻을 것을 규정하고 있다. Smart Space에서 사용자의 프라이버시 보호 기능을 제공하기 위해 사용자의 명확한 동의를 얻도록 하는 것은 Smart Space가 제공하는 또 다른 보안 기능인 Non-Intrusive 인증 서비스를 어렵게 한다는 문제가 발생한다.

따라서 이와 같은 문제를 해결하기 위해서 Smart Space에서 제공하는 프라이버시 보호 기술은 다음과 같은 기능이 포함되어야 한다.

- 인비저블 및 자동화된 프라이버시 보호를 위해서 사용자의 개입이 최소화되는 Minimally-Intrusive

Privacy Protection 프레임워크
- 사용자 위치 정보에 대한 사용자의 통제 기능
- Smart Space 내의 사용자 위치에 대한 정보 질의시 Smart Space의 통제 기능
- 위치 추적 정보에 대한 조회 대상자의 제한
- 법적, 제도적인 개인정보 보호와 연계되는 기술 개발

4.3 분산 신뢰 관리

Smart Space에서는 수많은 사용자와 Smart Space 간에 빈번한 상호작용이 있다. 현재의 신뢰 관리 시스템의 신뢰 관리 주기(Life-Cycle)는 사용자의 등록, 인증, 신뢰 형성 등으로 구성된다. 그러나 Smart Space에서 이러한 신뢰 관리 주기는 사용자에게 Seamless하고 인비저블한 서비스가 제공되기에는 불가능하다는 단점이 있다. 즉, Smart Space에서는 중앙 집중적인 TTP를 가지기가 힘들다는 단점이 있다. 이는 상점마다 다양한 사용자 인증 방법과 사용자에 대한 신뢰가 서로 다르기 때문에 중앙 집중적으로 TTP를 형성하기 어렵다는 점에 기인한다. 또한 Smart Space에서는 공간에 진입하는 사용자의 정보를 미리 습득하여 신뢰 관리를 위해 등록하는 것이 어렵기 때문이다. 또한 물리적인 공간에서 사용자에 대한 신뢰는 중앙 집중적인 TTP와 사용자와의 선-신뢰 관계가 없이 진행되는 것이 일반적이다. 즉, Smart Space가 사용자와의 거래가 진행됨에 따라 자신의 신뢰 관계를 구축하는 것이 일반적이다.

따라서 이와 같은 문제를 해결하기 위해서 Smart Space에서는 분산 신뢰 관리(Decentralized Trust Management)를 통해 신뢰 관리를 수행한다. 분산 신뢰 관리 기술은 다음과 같은 기술을 포함하여야 한다.

- 단계적으로 사용자를 등록하고 관리하는 신뢰 관리 메커니즘
- 순차적인 신뢰관리 형성 프로세스의 지원
- 사용자의 다양한 속성을 기반으로 신뢰 값을 평가하는 프레임워크

4.4 접근 제어

접근제어의 기본 구조는 사용자에게 정보 및 자원에 대해 접근할 수 있는 권한을 부여하고 나중에 사용자가 접근을 시도할 때 부여된 권한이 자원 및 정보에 설정된 권한에 부합되는 지를 결정하는 것인데 Smart Space에서는 이러한 기본 메커니즘에 사용자가 물리적인 공간에 있어서 발생하는 다양한 환경적인 변수를 접근제어 설정 및 결정에 반영하여야 한다. 또한 동적으로 시스템에 접근하는 사용자를 제어하기 위해서는 등록되지 않은 여러 가지 사용자 속성을 기반으로 접근제어를 결정하는 모델도 필요하다.

Smart Space에서는 사용자가 사이버 공간인 인터넷과 같이 거리의 제한 없이 접근하는 것이 아니라 물리적인 거리에 따라 서비스가 달라진다. 예를 들어 은행에 있는 ATM의 경우에는 사용자와의 물리적인 거리, 즉 접근도(Proximity)에 따라 사용자를 인식하고 서비스 메뉴를 출력할 것이다. 따라서 Smart Space에서는 제공되는 서비스에 따라 사용자의 물리적인 거리가 사용자에게 접근 권한을 부여하는데 판단 근거가 된다.

따라서 이와 같은 문제를 고려하여 Smart Space에서 제공하는 접근 제어 기술은 다음과 같은 기술을 고려하여야 한다.

- Context 기반 접근 제어 모델
- 사용자의 속성에 따른 접근 제어 기술
- Smart Space의 환경인 Context에 따라 접근 권한 등이 달라지는 접근 제어 기술

4.5 Digital Identity 관리 기술

유비쿼터스 컴퓨팅 환경에서는 시간과 공간에 제약을 받지 않고 다양하게 분산된 서비스를 제공받을 수 있다. 따라서, 사용자의 식별자(Identifier)와 속성정보(Attribute Information)로 구성된 디지털 신원(Digital Identity) 정보를 기존의 IT 환경에서처럼 중앙집중형으로 관리하기가 어려워진다. 또한 분산된 다양한 서비스를 사용자에게 Seamless 하게 제공하기 위해서는 매번 사용자가 Id를 입력하지 않고도 사용자의 신원과 권한을 확인할 수 있는 Identity 연동 기술이 필요하다. 또한, 유비쿼터스 컴퓨팅 환경에서는 사용자의 Id의 중요성이 더욱 커지기 때문에 Id의 가용성을 확보하는 것이 매우 중요해진다. 따라서 이와 같은 문제를 고려하면 유비쿼터스 응용에서는 다음과 같이 사용자의 Identity 정보를 관리하는 기술이 필요하다.

- 분산된 다양한 서비스에서 사용자의 Identity를 관리할 수 있는 분산 Identity 관리 기술
- 분산된 서비스 환경에서 seamless 서비스를 제공할 수 있는 Identity Federation 기술

- Identity 보장(Assurance) 기술

Digital Identity 관리 기술은 위에서 설명한 단위 기술로써 뿐만 아니라 앞 절에서 설명한 인증, 인가, 개인정보, 분산인가 기술과 매우 밀접한 관련을 갖는다.

V. 결 론

본 고는 최근 그 연구가 활발히 진행되고 있는 유비쿼터스 컴퓨팅의 보안 요구사항에 대하여 고찰하였다. 먼저 유비쿼터스 컴퓨팅의 개요, 연구동향 및 기술 발전 방향에 대하여 기술하였다. 이를 바탕으로 유비쿼터스 컴퓨팅 환경에서의 보안 요구사항을 분석하였다. 유비쿼터스 컴퓨팅 보안 요구사항은 네크워크와 응용으로 분류하여 분석하였다. 먼저 유비쿼터스 네트워크 상에서의 보안위협과 이를 해결하기 위한 보안 요구사항에 대하여 기술하였다. 그리고 유비쿼터스 응용 환경에서의 보안 요구사항을 분석하기 위해 실현 가능한 시나리오를 도출하였고 이러한 시나리오를 동작시키는 Smart Space를 정의하였으며 Smart Space의 안전성을 제공하기 위한 보안 개념 모델을 도출하였다. 이를 통해 유비쿼터스 응용 보안 요구사항으로 인비저블 인증, 프라이버시 보호, 분산 신뢰 관리, 접근 제어, Digital Identity 관리 기술을 도출하였다.

참고문헌

[1] Frank Stajano, Security for Ubiquitous Computing, Jonh Wiley & Sons, 2002.

[2] Ginger Myles, et al., Preserving Privacy in Environments with Location-Based Applications, No. 1, pp. 56-64, 2003.

[3] Jalal Al-Muhtadh, et al., A Flexible, Privacy-Preserving Authentication Framework for Ubiquitous Computing Environments, IEEE ICDCSW Proc of the 22nd, 2002.

[4] Mark Weiser., The Computer for the Twenty-First Century, Scientific American, Vol. 256, No. 3, pp. 94-104, Sep 1991.

[5] Urs hengartner, Peter Steenkiste, Protection People Location Information, Proc. of Workshop on Security in Ubiquitous Computing, September, 2002.

[6] 기술경제연구부, "유비쿼터스 컴퓨팅의 연구동향", ETRI, 2002.

[7] 사카무라 겐, Ubiquitous Computing, 동방미디어북스, 2002.

[8] 조영섭, 조상래, 이대기, 진승헌, 유비쿼터스 컴퓨팅 환경을 위한 보안 요구사항 분석, COMSW 2003, 2003.07

[9] 조영섭, 조상래, 최대선, 진승헌, 정교일, 박치항, A Location Privacy Protection Mechanism for Smart Space, WISA 2003, 2003.08

[10] 조영섭, 조상래, 노종혁, 진승헌, 정교일, Smart Space 상에서의 보안 요구 사항 분석, WISC 2003, 2003.09

[11] 하원규, 김동환, 최남희, 물리공간과 전자공간의 융합: 유비쿼터스 IT혁명과 제3공간, 전자신문사, 2002.

〈著 者 紹 介〉

조 영 섭 (YeongSub Cho)

1993년 2월 : 인하대학교 전자계산공학과 졸업
1995년 2월 : 인하대학교 대학원 전자계산공학과 석사
1999년 2월 : 인하대학교 대학원 전자계산공학과 박사
1998년 12월~현재 : 한국전자통신연구원 인증기반연구팀 선임연구원
〈관심분야〉 I&AM, 인증인가, 정보보호, EC

조 상 래 (Sangrae Cho)

1996년 9월 : Imperial College London, 전산과 졸업(학사)
1997년 9월 : Royal Holloway, University of London, 정보보호 석사
1997년 10월~ 1999년 7월 : LG 종합기술원 연구원
1999년 7월~현재 : 한국전자통신연구원 연구원
〈관심분야〉 I&AM, 인증, 인가, 정보보호,

유 인 태 (Intae Ryoo)

1987년 2월 : 연세대학교 전자공학과 학사
1989년 2월 : 연세대학교 대학원 전자공학과 석사
1994년 2월 : 연세대학교 대학원 전자공학과 박사
1997년 9월 : 동경대학 정보통신공학 박사
1999년 3월~현재 : 경희대학교 전자정보대학 부교수
〈관심분야〉 인터넷, 네트워크 보안, 무선 LAN

진 승 헌 (Seunghun Jin)

1993년 2월 : 숭실대학교 전자계산학과 학사
1995년 2월 : 숭실대학교 대학원 전자계산학과 석사
2004년 2월 : 충남대학교 대학원 컴퓨터과학과 박사
1994년 12월~1996년 4월 : (주)대우통신 종합연구소 연구원
1996년 5월~1999년 5월 : (주)삼성전자 통신연구소 전임연구원
1999년 6월~현재 : 한국전자통신연구원 인증기반연구팀장/선임연구원
〈관심분야〉 I&AM, PKI, Network Security, EC

정 교 일 (Kyoil Chung)

1981년 2월 : 한양대학교 전자공학과 졸업
1983년 8월 : 한양대학교 산업대학원 전자계산학과 석사
1997년 8월 : 한양대학교 대학원 전자공학과 박사
1980년 12월~1981년 11월 엠시스템즈 사원
1981년 12월~1982年 2月 한국전기통신연구소 위촉연구원
1982년 3월~현재 한국전자통신연구원 정보보호기반연구그룹장/책임연구원
〈관심분야〉 IC Card, Security, Biometrics, 국가기반보호, 신호처리