유비쿼터스 컴퓨팅 보안

경북대학교 황성민 · 김순자*

1. 서 론

유비쿼터스(ubiquitous)란 언제 어디서나 네트워크에 접속할 수 있는, 즉 우리의 일상이 네트워크로 연결되어 있는 상태를 의미한다. 이 유비쿼터스 컴퓨팅 환경에서는 모든 정보가 공유되고 누구나 쉽게 접근할 수 있다. 그 이면에는 개인의 정보가 다른 사람에게 알려지는 비밀없는 세계가 될 수 있다. 이외 크래킹에 의한 정보 유출, 바이러스 유포, 컴퓨터 범죄, 프라이버시 침해, 저작권 침해 등 가상 세계에서 벌어지는 각종 부작용도 일어날 수 있다[1]. 개인정보나 구매내역이 기업들 사이에서 상업적인 목적으로 공유되고, 통행인의 얼굴을 인식해서 범죄 혐의자와 대조하는 무인 감시 카메라에 이르기까지 문제가 노출될 수 있다.

유비쿼터스 컴퓨팅 환경에서는 이와 같이 각 개체마다 많은 정보를 갖고 있으며, 또 이에 대한 정보를 수집, 분석하여 필요한 서비스를 알아서 해주는 서버도 필요할 것이다. 여기에는 필연적으로 개인의 정보를 어떻게 보호할 것이며, 필요한 서비스를 어떤 방법으로 안전하게 제공할 것인지에 대한 고려가 필요하다.

현재 유비쿼터스에 관련된 국내외로 연구가 많이 진행되고 있지만, 보안에 관련해서는 아직 미흡한 편이다. 국외에서는 Ubicomp 컨퍼런스에 보안 분야 워크샵이 있어 매년 유비쿼터스 보안에 관련된 논문이 발표되고 있지만, 국내에는 유비쿼터스 보안 관련 학회도 없으며, 논문 발표도 미흡하다.

유비쿼터스 컴퓨팅 환경은 기존의 연구분야인 무선 인터넷, 무선랜, 블루투스, 홈네트워크 등의 분야를 통합하는 환경이라 할 수 있다. 각각의 연구자들은 자신의 연구분야를 기반으로 유비쿼터스 컴퓨팅 환경을 상상하며 연구를 진행한다. 유비쿼터스 컴퓨팅 보안도 마찬가지이다. 무선 인터넷 보안 연구자들은 무선 인터넷의 진보된 개념으로 유비쿼터스 환경 보안을 생각하며, 무선이라는 제약점과 모바일 디바이스의 제한된 전력을 고려하여 연산량이 적은 인증 프로토콜 개발에 그 초점을 두고 있다. 무선랜이나 블루투스 연구자들은 통신 개체에 대한 사용자에 대한 신뢰문제와 어떤 방법으로 두 개체 간에 기밀성을 제공할 수 있을지에 대한 연구에 그 초점을 둔다. 이와 같이 각 연구분야에 따라 유비쿼터스 컴퓨팅에서의 보안의 관점을 달라 질 수 있다. 유비쿼터스 컴퓨팅에 대한 보안의 정의는 아직 개념 정립이 정확히 이뤄지지 않고 있다. 또, 유비쿼터스 컴퓨팅의 이용분야에 따라서 그 분야에 맞는 보안의 요건이 달라질 수 있다. 그렇기 때문에 정확한 보안의 개념 정립은 힘들 것이다. 하지만, 각 분야에서 연구되어지는 보안의 요건들 중에는 공통된 것들이 많고, 필수적인 것들이 있으므로 이들을 중심으로 유비쿼터스 컴퓨팅의 보안을 살펴보고자 한다.

유비쿼터스 컴퓨팅 보안(ubiquitous computing security)의 목적은 인가되지 않은 사용자가 공유된 정보에 불법적으로 접근하거나, 사용자 공유 정보를 노출 및 변경을 하지 못하도록 하는 것이다. 이를 위해서 고려되어야 할 보안의 요건을 인증(authentication), 기밀성(confidentiality), 무결성(integrity), 가용성(availability)을 중심으로 기술한다. 또한, 기존의 보안 요건을 그대로 적용할

* 종신회원

경우 문제점을 분석하고, 유비쿼터스 환경에 적합한 해결방안도 아울러 기술한다. 즉, 인증은 보안 정책모델 기반으로 하며, 기밀성은 에너지 효율이 높은 암호 알고리즘 개발이 필요하고, 무결성은 크게 메시지에 대한 무결성과 개체에 대한 무결성으로 나누어 전자는 체이닝 프로토콜(chaining protocol), 후자는 tamper protection 기법으로, 가용성은 암호퍼즐(cryptographic puzzle)[6] 등을 통해서 보장할 수 있다[2, 3].

유비쿼터스 컴퓨팅 환경에서 보안 요구 사항은 2장에서 일반적인 보안 요구사항인 기밀성, 인증, 무결성, 가용성에 대해 살펴보고, 유비쿼터스 컴퓨팅 환경에서 좀더 고려되어야 할 사항들도 언급할 것이다. 또, 유비쿼터스 컴퓨팅 환경에서 제공될 수 있는 서비스 타입에 따라 필요한 보안 사항들도 살펴볼 것이다. 3장에서는 기존의 분산 시스템이나 무선 환경에서 사용되는 보안 솔루션들에 대해 알아보고, 유비쿼터스로의 전환시에 발생할 수 있는 문제점에 대해 언급할 것이다.

2. 유비쿼터스 컴퓨팅 환경에서의 보안 요구 사항

일반적으로 계층간 통신이나 분산 시스템에서 보안은 사용자나 개체에 대한 신뢰를 할 수 있는지 또는 주고 받는 메시지를 신뢰할 수 있는지에 관한 인증, 주고 받는 메시지에 대한 내용을 비밀로 하는 기밀성, 메시지가 통신 중간에 변질이 되지 않았음을 검증하는 무결성과 많은 데이터 유입에 대해 어떤 방법으로 시스템의 서비스를 제공할 것인지에 관한 가용성의 관점으로 많이 다뤄진다[3]. 유비쿼터스 컴퓨팅은 무선 통신을 기본으로 개체 간에 통신을 하고, 모든 개체에 컴퓨팅이 가능한 소형 칩이 내장될 것이라는 비젼에 따라 기존의 보안과는 크게 다르지는 않지만, 추가적인 고려사항이나 제약점이 생길 것이다. 따라서 유비쿼터스 컴퓨팅 보안은 기존의 관점에서 보는 보안 요건들-인증, 기밀성, 무결성, 가용성에 관해 살펴보고 추가적인 사항들을 서술할 것이다.

2.1 인증(Authentication)

기존의 인증은 공개키 암호시스템 기반으로 신뢰기관에 의해 발급된 공개키 인증서를 바탕으로 인증하고자 하는 개체의 서명 검증을 통해 이뤄진다. 유비쿼터스 컴퓨팅 시스템은 일시적으로 네트워크에 연결이 되며, 그 연결은 확실한 연결성을 보장하지 않는다. 유선에서 사용되는 커브로스(Kerberos)에서부터 공개키 인증서(public-key certificates)를 이용한 인증방법은 인증을 위해 인증 서버나 철회 서버에 온라인(on-line) 연결을 해야 한다. 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, 연구되어져야 한다.

2.1.1 안전 천이 협약(secure transient association)

유비쿼터스 네트워크에서는 어떤 개체가 일시적 접속을 위한 인증 서비스 요구가 많이 필요하게 될 것이며, 이를 안전 천이 협약(secure transient association)이라 한다[2, 3].

안전 천이 협약을 구체적으로 설명하면 TV, 스테레오, DVD, VCR, 에어컨, 히터 등의 원격 제어장치(remote controller)가 거실 탁자 위에 놓여 있다고 하자. 유비쿼터스 컴퓨팅 환경에서는 모든 가전 제품을 PDA와 같은 하나의 제어서버를 두고 각 제품을 원격으로 제어할 수 있을 것이다. 만약 하나의 장치로 모든 디지털 전자 제품들을 제어할 수 있다면, 각 제품의 원격 제어장치는 필요없다. 그러나 제품을 구매한 후에 PDA가 각각의 디지털 전자 제품을 제어할 수 있도록 어떤 협약(association)을 설정하는 절차가 필요하다. 이러한 경우에 필요한 보안 사항들을 고려해 보자. 손님이 집을 방문했을 때 주인의 허락없이 전자 제품을 동작시키는 것을 제한할 필요가 있다. 그리고 PDA가 제어하고 있는 제품들을 교체하거나 처분할 수 있어야 하며, PDA가 고장이 났을 때 각각의 전자 제품의 제어 기능을 잃지 않고 다른 PDA로 교체가 가능해야 한다. 따라서 PDA가 전자 제품들과 맺는 협약은 수정 가능하고 또는 복구 가능해야 한다. 안전 천이 협약은 기존 환경과는 달리 제어장치, 제어 대상 개체가 수시로 바뀔

수 있으므로 협약 또한 수시로 바뀔 수 있음을 뜻한다.

안전 천이 협약은 기존의 인증 시스템을 기반으로 하여 사용목적에 맞는 보안 정책을 필요로 한다. Frank Stajano가 제안한 'Resurrecting Duckling Policy'과 같은 보안 정책 모델이 그 예가 될 수 있다[3].

2.2 기밀성(Confidentiality)

2.2.1 저전력 암호 알고리즘

인증 서비스에서는 인증과 더불어 두 개체 간에 공유키 교환을 하게 되며 이 공유키는 대칭키 암호 시스템 키로 사용된다. 따라서 두 개체간 인증 단계를 통과하면 안전한 비밀 통신 채널을 제공할 수 있으므로 쉽게 기밀성을 보장할 수 있다. 그러나 유비쿼터스 컴퓨팅에서의 기밀성을 보장하기 위한 에너지의 사용량이 중요한 고려사항이다. 유비쿼터스 컴퓨팅 장치는 모양과 크기가 다양하며, 주로 작은 장치들이 많다. 이로 인해 새로운 제약 조건이 생긴다. 이러한 장치들은 배터리 전력에 한계가 있어서 빠르고 계산 능력이 뛰어난 프로세서를 유용하게 사용할 수 없다. 유비쿼터스 컴퓨팅 장치들은 아주 작은 peanut 프로세서들을 갖고 있으며, 이 프로세서들은 공개키 암호와 같은 계산을 하기에는 속도가 늦기 때문에 적합하지 않다.

이러한 제약 조건들은 무선 인터넷이나 블루투스(bluetooth) 등이 발달하면서 널리 알려진 사실들이며, 이를 해결하기 위한 방안으로서 사전 계산 등의 방법이 많이 이용되었다. 하지만 배터리는 유한하고 적은 에너지를 갖고 있기 때문에 사전 계산 방법은 그 순간의 처리 속도를 향상시킬 수는 있으나, 배터리의 소모 전력은 사전 계산을 한 것과 하지 않은 것의 차이가 없기 때문에 배터리 전력의 한계를 극복하지는 못한다. 따라서 peanut 장치에서 암호 시스템의 효율성을 평가할 때나 암호 시스템을 설계할 때 초당 비트 처리율보다 줄(joul)당 비트 처리율을 고려하여야 하며, 줄당 비트 처리율이 좋은 칩(chip) 개발과 암호 알고리즘 개발이 필요하다[2]. 아울러, 많은 연산량을 갖는 공개키 암호시스템의 사용을 최대한 줄이는 방향으로 연구가 되어지거나, 효율성이 좋은 공개키 암호 시스템 연구가 필요하다.

2.2.2 디바이스 제어서버 보안의 기밀성

지금까지 살펴본 것이 무선 트랙픽 상에서 기밀성을 보호하는 것이라면, 유비쿼터스 장치 자체가 가지고 있는 정보에 대한 기밀성도 중요하다. 예를 들어 PDA를 잃어버리거나 도난당했을 때, 패스워드로 PDA 자체를 보호하고 있을지라도 PDA 속에 저장된 정보는 암호화 되지 않고 저장될 것이기 때문에, 적절한 리소스를 갖는 공격자는 저장된 정보를 열람하고 유출시킬 수 있다.

가까운 미래의 유비쿼터스 컴퓨팅에서는 PDA와 같은 장치들이 개인의 행동에 관한 정보를 저장할 기회가 훨씬 많아 질 것이다. 이런 장치는 사용자의 개성과 개인의 취향, 습성에 관한 가능한 한 많은 것들을 기억하고 발견하는 디지털 비서로서 역할을 할 것이다. 이러한 PDA에 개인의 정보들이 다량으로 저장될 것이므로 개인의 프라이버시의 침해를 막는 것이 중요하다. 그러므로 PDA와 같이 여러 장치와 통신을 하며 개인의 정보를 모으는 서버 장치는 저장된 정보를 비밀로 유지하는 것이 매우 중요하다.

2.2.3 메타데이터의 기밀성

마지막으로 메타데이터를 보호하는 것도 고려해야 한다. 익명성(anonymity), 추적성(traceability)과 트래픽 분석(traffic analysis)은 지금까지 소홀하게 다뤄진 기밀성의 한 부분이지만, 유비쿼터스 컴퓨팅에서는 꼭 필요한 보안 요구사항이다[2]. 암호화는 주고 받는 메시지의 내용이 무엇인지에 대한 비밀유지는 가능하다. 그러나 언제, 누구에게, 누구로부터 전달되는 메시지인지는 비밀로 유지할 수가 없기 때문에 사용자의 프라이버시가 드러날 우려가 있다. 통신 주체가 누구인지 감추는 익명성은 어려운 문제이다. 만약 익명성이 보장될 경우 익명성으로 인한 공격자 추적이 어려울 것이다. 따라서 익명성을 보안 요건으로 고려할 때는 익명성 보장에 따른 공격자 추적 방안도 함께 연구 되어져야 한다. 그리고 트래픽 분석에 대한 보호대책은 아직 어려운 실정이다. 사용자의 관점에서 사용자의 위치에 대한 프라이버시와 한 사용자에 대한 메시지 트랜잭션을 동일 사용자의 다른

메시지 트랜잭션과 연결짓는 것을 어렵게 만드는 방법도 개인의 프라이버시를 위해 고려되어야 한다. 그렇지 않다면, 우리가 추구하는 유비쿼터스 컴퓨팅이 사용자의 프라이버시를 침해하는 감시자의 역할을 하게 될 것이다.

2.3 무결성(integrity)

2.3.1 메시지 무결성

기본적인 무결성 문제는 하나의 개체에서 다른 개체로 가는 메시지가 제3의 악의적인 개체(공격자)에 의해 방해받지 않는 것이다. 즉, 상대방 개체와 메시지를 주고 받을 때 내용이 변경되지 않은 원본 메시지임을 보장하는 것이다. 인증 및 키 교환 과정이 어떻게 이뤄지는지 알고 있다면, 메시지 인증 코드(MAC: message authentication code)와 같은 잘 알려진 암호학적인 메카니즘을 사용하면 큰 문제없이 메시지 무결성을 보장할 수 있다.

인증을 하기 위해 브로드캐스트 되어지는 데이터에 전자 서명값이 존재하고, 이를 각 개체들이 검증을 위해 전자서명에 필요한 연산을 계산할 때 많은 전력이 소모된다. 계산량이 많고 전력 소비가 많은 전자서명을 사용하지 않는다면, 인증을 하기 위해 브로드캐스트 되어지는 데이터를 변경하지 못하도록 전자서명 역할을 대신할 것이 필요하다. 이는 체이닝 프로토콜(chaining protocol)로써 해결이 가능할 것이다[4, 5].

2.3.2 개체 무결성

유비쿼터스 컴퓨팅에서 가장 심각한 무결성 문제는 이동중인 메시지의 무결성이 아니라 유비쿼터스 장치 자체에 대한 무결성이다. 이는 유비쿼터스 장치에 공격자가 사용자의 정보를 유출시키기 위해 인증과는 무관하게 어떤 조작이 가능할 수도 있고, 장치 자체를 다른 것으로 변경시킬 수도 있다. 어떤 측면에서 인증과 유사한 면이 있지만, 약간의 차이는 있다. 인증에서의 기본 가정은 네트워크는 공격자들의 공격에 노출되어 있고, 안전하지 못하지만, 네트워크에 소속된 개체들은 그들의 비밀을 지킬 수 있는 능력이 있다는 것이다. 유비쿼터스 컴퓨팅에서는 이러한 가정도 받아들이지만, 공격자들이 네트워크에 소속된 개체들을 바꿀 수 있다는 가정도 한다. 이를 해결할 수 있는 방법이 물리적인 매수 보호(physical tamper protection) 장치이다.

높은 등급의 매수 저항(tamper resistance) 장치를 사용한다면, 공격자는 장치 내부에 유지되고 있는 비밀들에 대해 수정이나 접근조차 불가능하게 할 수 있으나 이는 가격이 너무 비싸고 어려운 문제이다. 이런 이유로 매수를 시도하는 공격자들을 추적할 수 있게 하는 매수 증거(tamper evidence) 장치를 이용하는 것이 더 나을 것이다. 물리적 봉인에 의한 무결성은 인증 프로토콜의 한 부분으로 검증되어 질 수 없으며, 이것은 물리적인 장치이므로 인간에 의한 정밀 검사가 필요한 것이다.

2.4 가용성(availability)

무선 시스템에 대한 고전적인 공격은 통신 채널을 혼선시키는 것이다. 좁은 범위에서 RF 통신을 하는 유비쿼터스 시스템들도 이러한 통신 채널의 혼선이 존재한다면 유비쿼터스 시스템은 서비스를 제공 할 수 없을 것이다. 하지만 이것을 다루는 것은 유비쿼터스 컴퓨팅에서 보안에 관한 설계를 할 때 고려 대상에서 제외된다. 왜냐하면 유비쿼터스 컴퓨팅에서 다룰 수 있는 범위 밖의 문제이고, 통신 채널의 혼선을 일으키는 잼머(jammer)가 통신 범위를 벗어나게 되면, 그 네트워크는 다시 정상적으로 동작하기 때문이다.

2.4.1 서비스 거부 공격

앞서 언급한 보안과 전력 보전의 관계로부터 서비스 거부(denial-of-service)공격이 출현하게 된다. 유비쿼터스 장치는 제한된 배터리 에너지를 가지고 있고, 그것을 아끼기 위해 필요시에만 깨어 있고 불필요시에는 휴면 상태에 접어들게 할 수 있다. 이때 효과적인 공격 방법은 배터리가 방전될 때까지 장치를 깨어 있게 하는 것이다. 배터리가 방전되고 나면, 공격자는 유비쿼터스 장치를 사용 불가능하게 만든 후 사라질 것이다. 이를 일컬어 cruel treatment sleep deprivation torture라 한다[2, 3].

인증이 이러한 공격을 막을 수 있을 것이라고

생각할 수 있으나, 실제적으로는 막을 수가 없다. 인증은 서비스 요구가 있을 때 합법적인지 아닌지를 구분해 준다. 그러나 웹서버 같은 경우에는 서비스 요구자를 거절 할 수 없다. 서버의 딜레마는 서비스 요구자에게 질의에 대한 응답을 할 것인지 아닌지 결정하는 것이다. 서버가 서비스 요청이 있을 때 이 요구를 서비스 거부 공격으로 받아들이고 응답을 주지 않았으나, 실제로는 요청에 대한 응답을 기다리는 순수한 의도의 서비스 요구자일 수도 있다. 서비스 거부 공격자들에게 반복적으로 신원 확인을 요구하는 것은 효과 없는 일이다. 왜냐하면 서비스 요구자의 신분 정보는 쉽게 속일 수 있으며, 분산 서비스 거부 공격(distiributed denial-of-service)도 가능하기 때문이다.

해결 방안으로는 서비스 요구자들에게 우선순위를 부여하는 것이고, 중요하지 않은 요구에 대해 할당할 자원을 줄이고, 중요한 요구에 대한 자원의 할당을 늘리는 것이다. 이것은 좀더 중요한 사용을 위해 서비스의 등급을 보장하는 것이다. 물론 이것은 서비스 사용이 허가된 내부 공격자에 의한 공격에는 취약하다.

또 하나의 접근 방법은 돈을 지불하면 서비스를 제공하는 방법(plutocratic access control)이다. 자원에 접근하기 위해 요금을 지불하기 전까지 서버는 클라이언트가 자원을 무분별하게 요청하는 것을 제한할 수 있다.

실제 돈을 요금으로 부과하는 것이 비실용적이라면, 서버는 서비스 교환을 위해 약간의 비용이 드는 자원에 대한 희생을 강요하므로써 위의 방법과 같은 제한 전략을 사용할 수 있다. 서버는 클라이언트에게 암호적인 퍼즐(cryptographic puzzle)을 풀게 하거나 [6], 인간이 대답하기는 쉽고 기계가 하기 어려운 질문을 하는 방법을 사용할 수 있다. 후자는 계층별 어플리케이션에 보다 적합하고 전자는 유비쿼터스 컴퓨팅 환경에 좀 더 적합할 것이다.

2.5 서비스 목적에 따른 보안 요구조건

앞서 언급한 보안 요구조건들은 유비쿼터스 환경에서 추가적으로 고려해야 할 보안 요구사항 들이다. 이들은 하나의 서비스를 위해 반드시 갖춰져야 하는 것은 아니다. 그 서비스 목적에 맞는 보안 요구조건을 새롭게 정의하며 구현해야 할 것이다. 따라서 유비쿼터스 환경에서 제공될 수 있는 서비스를 구분하며 그에 맞는 보안 요구사항을 살펴보자[8].

2.5.1 정보 서비스에서의 보안 요구조건

정보 서비스는 사용자의 위치에 따른 호텔 및 식당의 위치, 교통 수단이나 열차시간 등을 알려주며 예약 등이 가능한 서비스이다. 정보 서비스에서 가장 중요한 것이 사용자의 프라이버시 보호이다. 사용자에게 안전하고 편리한 서비스를 제공하기 위해서는 사용자가 위치하고 있는 지역의 신뢰된 서비스 제공자들에게만 사용자 정보를 제공할 수 있어야 한다. 따라서, 사용자의 정보를 신뢰되지 않는 공격자에게 노출시키지 않는 것이 중요하다. 이를 위해서는 정보에 대한 기밀성, 사용자에 의해 서비스 제공자들에게 주어진 신뢰수준에 따라 사용자 정보의 접근 정도를 달리 해야 하는 사용자 정보의 접근 제어와 서비스 제공자들의 신뢰 수준을 식별하고 검증하는 개체 식별과 검증이 보장되어야 한다.

2.5.2 U-커머스(U-commerce)

U커머스는 개인이 쇼핑목록을 PC나 휴대전화에 입력해 놓으면 차량 이동 중이거나 걷고 있을 때 원하는 물건을 파는 상점이 있을 경우 상가의 위치 정보, 가격, 재고현황 등을 쉽게 통보 받을 수 있고, 주문, 결재할 수 있는 서비스이다. 이를 위해서는 주문 정보나 결재 정보에 대한 기밀성은 반드시 필요하며, 사용자나 서비스 제공자가 합법적인지를 알 수 있게 하는 인증도 요구 되어진다. 또, 주문 정보가 통신 도중 공격자에 의해 변질될 수 있으므로 데이터에 대한 무결성과 서비스 요구나 응답후 서비스에 대한 책임을 회피하지 못하도록 하는 부인봉쇄의 기능도 필요하다.

2.5.3 장치의 공유

회의실, 사무실, 공항의 대합실 등에서 설치되어 있는 장비들을 사용하고자 할 경우 공유된 자원을 인증된 사람들만이 자원에 접근할 수 있도록 자원에 대한 접근제어가 필요하며, 공유된 장비에 저장되는 데이터의 기밀성도 보장되어야 한다. 또,

공유된 자원을 사용하는 것에 대한 요금 부과도 함께 이뤄져야 할 것이다.

3. 분산 시스템이나 무선 환경에 사용되는 보안 솔루션

유비쿼터스 컴퓨팅 환경은 현재까지 많이 연구되어왔던 무선 인터넷, 블루투스, 무선랜 등을 수용한다. 유비쿼터스 컴퓨팅 보안도 마찬가지로 기존의 환경에서 사용되던 보안 요소들을 살펴봄으로써 개념 정립이 좀 더 명확해 질 것이다.

3.1 커베로스(Kerberos)

커베로스는 미국 MIT의 Athena 프로젝트에서 개발되어 개방된 컴퓨터 네트웍 내에서 서비스 요구를 인증하기 위한 수단으로 사용되어왔다. 커베로스는 Needham-Schroeder 인증 프로토콜에 타임스탬프(timestamp)를 사용하고 [18], 제 3의 인증서버, 철회서버를 둠으로써 보안 정책 관리를 쉽게 할 수 있도록 설계되었다. 커베로스는 타임스탬프를 사용하므로써 시간의 동기화가 매우 중요한 요소이다. 유비쿼터스 컴퓨팅 환경과 같은 불확실한 연결성을 제공할 때 인증서버와 철회서버에서의 ticket 요청 시간차에 의해 불법적인 사용자를 합법적인 사용자로 인증할 수 있는 단점이 생긴다[3].

3.2 공개키 기반 구조(Public Key Infrastructure)

공개키 기반 구조는 키의 생성과 인증, 그리고 분배와 안전한 관리의 기능을 제공한다. 공개키 기반 구조의 구성을 살펴보면 공개키에 대한 인증서를 발급하는 인증기관, 사용자들의 인증서 신청 시 인증기관 대신 그들의 신분과 소속을 확인하는 등록기관, 인증서와 사용자 관련정보, 상호인증서 및 인증서 취소목록 등을 저장 검색하는 장소인 디렉토리, 또한 다양한 응용에서 공개키를 이용하여 전자서명을 생성하고 검증하며 데이터에 대한 암호, 복호를 수행하는 사용자 등이 포함된다. 전자상거래를 할 경우, 전자상거래를 위해 전자서명을 한 뒤 공인 인증기관의 인증을 받아 상대에게 제시함으로써 거래가 이루어지는데 개인 정보나 거래 정보가 외부에 노출되지 않아 안전하게 거래할 수 있다. 이 시스템은 인터넷 상의 보완을 위한 광범위한 기업 응용 프로그램에 보안 솔루션을 제공한다. 솔루션은 웹 보안, 전자우편 보안, 원격접속, 전자문서, 전자상거래 어플리케이션 등 매우 다양한 분야에서 사용된다. 현재 무선 인터넷에서도 무선 공개키 기반구조를 이용해서 많은 서비스를 제공한다[19]. 하지만, 공개키 기반 구조가 필수적으로 갖는 연산량의 증가와 공개키에 대한 인증서를 관리하기 어려운 단점이 생긴다[21].

3.3 IPSEC

IPSEC은 인증, 가밀성, 무결성을 기본적으로 제공하는 프로토콜이다. IPSEC은 다양한 관련 프로토콜을 실제로 수집한 것으로, 완벽한 VPN 프로토콜 솔루션이나 L2TP 또는 PPTP 내의 암호화 방법으로 사용될 수 있다. IPSEC은 OSI 모델의 네트워크 계층(layer 3)에 존재한다. IPSEC은 보다 안전한 인터넷 기반 서비스 지원을 위한 목적으로 표준 IP를 확장했으며 IP 어드레스를 숨겨 네트워크 침해로부터 보호될 수 있다. IPSEC은 암호화, 인증 및 키 관리 등 강력한 보안 기능을 탑재하고 있기 때문에 IP 환경에 있어 최고의 터널링 프로토콜로 받아들여지고 있다. 하지만 IP-only 환경에서만 효과를 갖는다. IPSEC의 지나친 복잡성은 시스템의 구현은 물론 구현된 시스템의 상호 호환을 어렵게 할 뿐만 아니라, 구현 과정에서 눈에 보이지 않는 보안상의 약점(security holes)을 포함할 수 있다는 위험성을 내포하고 있다. 특히 대부분의 IPSEC 표준의 복잡성은 IKE(internet key exchange)의 복잡성에 기인하며 IKE와 관련되어서는 시스템의 복잡성과 함께 DoS(Denial-of- Service) 공격에 취약하다는 문제점이 있다[20].

3.4 무선 인터넷

무선 인터넷 보안은 인증, 무결성, 기밀성, 가용성을 제공한다. 무선 인터넷의 보안 구성이 유선 인터넷과 유사하지만, 자원의 제한과 이동 통신 사업자의 개입 등으로 유선 인터넷 보안에 사용되던 SSL이나 TLS를 사용하지 않고, WTLS 등의

경량화된 보안 메카니즘을 사용한다. 유선에 비하여 상대적으로 제한된 대역폭, 약한 CPU와 더 적은 메모리를 채택하고 전원도 제한, 이동통신 사업자가 모든 가입자의 서비스 관리하는 유선 인터넷과 다른 제한적인 요소들을 고려해야 하며, 이를 보완하기 위해 암호 알고리즘 및 프로토콜 개발이 필요하다[21].

3.5 무선랜

무선랜 보안은 접근제어(access control)와 프라이버시(privacy)를 제공한다. 무선랜 보안 프로토콜 중의 하나인 WEP에서는 access point에 접근할 수 있는 사용자를 인증하고, wep key를 이용해서 클라이언트와 access point 사이에 주고 받는 패킷을 인증을 통해 자동 생성되는 키를 가지고 암호화 해서 보낸다. 클라이언트에 WEP키를 할당하는 일반적인 방법은 클라이언트의 저장장치에 저장하거나, 클라이언트 무선랜 장비의 아답터에 기억시키는 방법을 사용한다. 클라이언트의 MAC주소나 WEP키를 사용하여 무선랜에 접근권한을 획득할 수 있다. 또 WEP는 단방향인증만을 제공하므로 불법적인 access point를 두어 DOS 공격의 시발점이 되게 할 수 있다. 또, access point와 클라이언트 사이에 패킷당 암호화는 되지만, 인증이 되지 않으므로 패킷들을 스푸핑 할 수 있다. 이를 개선하기 위해서는 상호인증을 위한 키가 클라이언트 및 엑세스포인트의 저장 메체에 정적으로 저장되는 방식이 아닌 사용자의 네트워크 로그온 시에 동적으로 WEP키가 생성되어 사용자 세션방식으로 관리되어야 하며. 중앙집중 제어방식으로부터 무선랜의 사용자들에 대한 전반적인 보안을 관리할 수 있어야 한다[22].

4. 결 론

유비쿼터스 컴퓨팅은 차세대 IT 기술로서 알려져 있으며, 현재 실현중이다. 유비쿼터스 컴퓨팅 환경이 미래에 아주 많은 편리함을 가져다 줄 것으로 많은 사람들이 기대하고 있다. 우리에게 많은 편리함을 가져다 주는 만큼 악의적인 사람들에 의해서 개인의 정보 유출과 같은 큰 희생을 강요받을 지도 모른다. 따라서 유비쿼터스 컴퓨팅 보안의 정의가 필요하고, 기존의 보안 개념인 인증, 기밀성, 무결성, 가용성과 유비쿼터스 만의 추가적 고려사항인 안전 천이 협약, 에너지 효율성, 메타데이터의 기밀성, 메시지와 개체에 대한 무결성, 서비스 거부 공격을 종합적으로 고려한 일반적인 유비쿼터스 컴퓨팅 보안을 정의하였다. 또, 유비쿼터스 컴퓨팅 환경에서 제공하고자 하는 서비스의 용도에 따라 보안 요구사항은 달라질 수 있다. 이와 같은 사항들은 표 1과 같이 정리 할 수 있고, 이에 대한 해결책은 메시지 무결성을 위한 체이닝 프로토콜이나 서비스 거부 공격에 대한 암호퍼즐 같은 기존의 연구로서 해결 가능한 것도 있으며, 저전력을 소비하는 암호 암고리즘이나 메타데이터의 기밀성과 같이 추가적인 연구가 필요한 것도 있다. 또한 서비스 목적별, 분산 시스템 및 무선 환경에서 IPSEC, 무선랜, 무선 인터넷 등의 보안을 분석하였다.

u-커머스(u-commerce)나 유비쿼터스 전자정부(ubiquitous government) 등과 같은 유비쿼터스 기반 환경들은 앞서 정의한 보안 요구사항들을 고려하여 설계되어야 하며, 또한 각 유비쿼터스 기반 환경에 맞는 보안의 추가요소를 정의하고 그에 따른 해결책도 연구되어야 한다.

표 1 유비쿼터스 컴퓨팅 보안

보안요건	추가적인 고려 사항	해결방안
인증	안전 천이 협약	보안 정책 모델 설계
기밀성	저전력 소모	저전력 암호 알고리즘 연구 필요
	익명성, 추적성, 트래픽 분석	추가 연구 필요
무결성	메시지 무결성	Chaing protocol (예: Guy Fawkes protocol, TESLA[4] 등)
	개체 무결성	Tamper resistanc (예: IBM 4758) Tamper evidence
가용성	DOS 공격 DDOS 공격	Plutocratic access control Crytographic puzzles[8]

참고문헌

[1] 윤정로, 최장욱 역, 유비쿼터스, 21세기북스, 2003.
[2] F. Stajano, R. Anderson, The Resurrecting

Duckling: Security Issues for Ubiquitous Computing, Wiley, 2002.

[3] F. Stajano, "Security for Ubiquitous Computing" first Security & Privacy supplement to IEEE Computer, April, 2002.

[4] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA Broadcast Authentication Protocol," Cryptobytes, Volume 5, No. 2 RSA Laboratories, Summer/Fall pp. 2-13, 2002.

[5] R. J. Anderson, F. Bergadano, B. Crispo, J.-H. Lee, C. Manifavas, and R. M. Needham. A new family of authentication protocols. Operating Systems Review, 32(4):9-20, October, 1998.

[6] A. Juels and J. Brainard. "Client Puzzles: A Cryptographic Defense Against Connection Depletion Attacks," In Proceedings of NDSS '99, pp.151-165, 1999.

[7] R. Zimmer, "Structured Analysis of Security in Ubiquitous Computing," UBICOMP2002, October, 2002.

[8] F. Vieira, J. Bonnet, C. Loba, R. Schmitz, P. Windrisch, C. Byrne, T. Wall, "Operator specific security requirements for ubiquitous computing," EURESCOM Technical Information P1005, June, 2001.

[9] N. Shankar, W. Arbaugh, "On Trust for Ubiquitous C]omputing," Workshop on Security in Ubiquitous Computing, UBICOMP 2002, Sep. 2002.

[10] J. Seigneur, "Secure Ubiquitous Computing based on Entity Recognition," Workshop on Security in Ubiquitous Computing, UBICOMP 2002, Sep. 2002.

[11] M. Wu, A. Friday, "Integrating Privacy Enhancing Services in Ubiquitous Computing Environments," Workshop on Security in Ubiquitous Computing, UBICOMP 2002, Sep. 2002.

[12] L Bussard, Y. Roudier, "Authentication in Ubiquitous Computing," Workshop on Security in Ubiquitous Computing, UBICOMP 2002, Sep. 2002.

[13] M. Kreutzer, "Identity Management," Workshop on Security in Ubiquitous Computing, UBICOMP 2002, Sep. 2002.

[14] N. Shankar, D. Bilfanz, "Enabling Secure Ad-hoc Communication using Context-Aware Security Services," Workshop on Security in Ubiquitous Computing, UBICOMP 2002, Sep. 2002.

[15] U. Hengartner, P. Steenkiste, "Protecting People Location Information," Workshop on Security in Ubiquitous Computing, UBICOMP 2002, Sep. 2002.

[16] Philip Robinson, "Threats, Risk Assessment and Policy Management in UbiComp," Workshop on Security in Ubiquitous Computing, UBICOMP 2002, Sep. 2002.

[17] Hakan Kvarnstrom, "A Protection Scheme For Security Policies In Ubiquitous Environments Using One-Way Functions," Workshop on Security in Ubiquitous Computing, UBICOMP 2002, Sep. 2002.

[18] R. M. Needham and M. D. Schroeder, "Using Encryption for Authentication in Large Networks of Computers," Communications of the ACM, Vol. 21 (12), pp. 993-99.

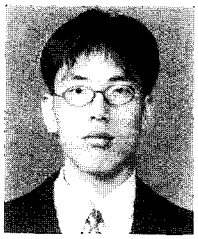
[19] Public-Key Infrastructure (X.509) (pkix), http://www.ietf.org/html.charters/pkix-charter.html, 1998. 4

[20] 엄봉식, "IPSec VPN의 현재, 그리고 미래", 시사컴퓨터, 2002년 12월호

[21] 무선 인터넷 기반의 인증 및 키 교환 프로토콜에 관한 연구, 최종연구보고서, ETRI, 2002.

[22] 무선랜보안, http://www.superuser.co.kr/security/certcc/wireless_lan_security.pdf

황 성 민



2000 경북대학교 전자공학과 학사
2002 경북대학교 전자공학과 석사
2002~현재 경북대학교 전자공학과 박사과정
관심분야 : 유비쿼터스 보안, 전자지불, 암호 시스템, 정보보호
E-mail : mivri@palgong.knu.ac.kr

김 순 자

1975 경북대학교 수학교육학과 학사
1977 경북대학교 수학과 석사
1988 계명대학교 수학과 박사
1993~현재 경북대학교 전자·전기 공학부 교수
관심분야 : 정보보호 및 보안 기술, 정보 보호 응용 기술
E-mail : snjkim@ee.knu.ac.kr

Japan-Korea Joint Workshop
• on Algorithms and Computation •
(워크샵 개최)

- 일 자 : 2003년 7월 3~4일
- 장 소 : 일본 동북대학(Tohoku University, Sendai, Japan)
- 주 최 : 컴퓨터이론연구회
- 상세안내 : http://www.dais.is.tohoku.ac.jp/waac03/index.html