情 報 保 護 學 會 誌
第 14 券 第 1 號, 2004. 2

유비쿼터스 네트워크와 시큐리티 고찰

박 춘 식*

요 약

네트워크와 무선통신의 발달에 힘입어 유비쿼터스 시대가 도래하고 있다. 유비쿼터스 컴퓨팅에서의 시큐리티 문제는 인터넷 시대의 시큐리티 문제보다 복잡하며 공격이 용이하나 대책 수립은 보다 더 어려울 것으로 예측된다. 본 논문에서는 안전하지 못한 유비쿼터스 네트워크 기반이 전개되기 전에 유비쿼터스의 시큐리티 문제를 고찰해 보고자 하였다. 유비쿼터스와 국방 정보시스템과의 관계, 유비쿼터스와 시큐리티 고려사항, 유비쿼터스와 시큐리티 서비스인 인증, 무결성, 기밀성, 가용성 등에 관하여 기존의 발표된 자료를 중심으로 고찰하여 보았다.

Ⅰ. 서 론

미국 Xerox사의 Palo Alto Research Center의 Mark Weiser(1952-1999)가 만든 유비쿼터스 컴퓨팅이라는 신조어가 소개된 1991년 9월판 Scientific American의 "The Computer for the Twentity-First Century"[1] 논문의 첫 머리에 "가장 심오한 기술은 사라지는 것들이다. 일상생활에서 구별이 되지 않을 정도로 스며들어버리는 것이다"라는 말로 시작하고 있다.

인터넷 정도의 충격으로 유비쿼터스 컴퓨팅의 등장을 이야기하는 사람들도 많지만, Mark Weiser의 이야기처럼 컴퓨터가 별도의 장치로 인식되는 것이 아니라 가장 심오한 기술로 남기 위해서는 사라져야 되는 것이며 다시 말해서 일상 생활 속으로 스며들어 보이지 않고 일반화되어 보통 명사처럼 사용되어야 하는 것이 어쩌면 자연스럽게 나아가는 정보통신의 방향일지도 모른다. 마치 기계라는 단어가 처음에 등장하였을 때에, 어마어마한 괴물로 세상을 놀라게 하였지만 지금은 기계라는 단어가 특정 물체를 지칭하는 것이 아니라 오히려 일반적인 보통명사가 되어 사용되고 있는 것처럼 말이다. 컴퓨터라는 단어가 책상 위에나 무릎 위에 놓여 이용하는 기계로 인식되는 것이 아니라 어느 곳에나 언제든지 구별 없이 사용되는 일상의 것으로 인식되어 책상 위나 무릎 위에서 사라져서 기계와 같은 보통명사가 되어버리는 시대, 그것이 유비쿼터스 컴퓨팅 또는 유비쿼터스 네트워크 시대가 아닐까 생각해 본다.

한편, Mark Weiser는 컴퓨터에서의 혁명을 25년 주기로 분류하여 소개하고 있다. 첫 번째가 1950년대의 mainframe computing 시대로, 많은 사람들에 의하여 사용되는 한 대의 컴퓨터 시대, 두 번째가 1975년대의 PC computing 시대로, 한 사람에 의하여 사용되는 한 대의 컴퓨터 시대, 세 번째가 2000년대의 ubiquitous computing 시대로, 한 사람에 의하여 사용되는 수많은 컴퓨터로 컴퓨터의 존재가 인식되지 않는 시대로 분류하고 있다. 현재의 유비쿼터스 컴퓨팅의 전개 방향은 각국에서 연구 개발되고 있는 상황에 따라 많이 달라지겠지만 입는 그리고 심는 컴퓨팅(wearable/implant computing), 임베디드 컴퓨팅(embedded computing), pervasive computing, silent computing, nomadic computing, disposable computing, sentient computing, exotic computing 등의 방향으로 나아갈 것으로 예측하고 있는 실정이다.

유비쿼터스 컴퓨팅의 발전은 시간에 흐름에 따라 나아가겠지만, 개인정보보호, 시스템 혼란 방지, 확장성, 보안등의 장기적 이슈가 될 문제점들이 노출되고 있다. 개인 정보보호는 센서와 상황 모델의 적용에 따라 개인의 정보가 쉽게 노출되며, 자동 지원 시스템이

* 국가보안기술연구소(csp@etri.re.kr)

증가할수록 개인 정보의 노출도 심각하게 된다. 그리고 센서와 상황 모델로부터 생성되는 의미 있는 정보와 무의미한 정보가 구별 없이 폭주할 경우, 무의미한 정보로부터의 시스템 혼란 방지를 어떻게 구현할 수 있을는지, 분산 환경에서의 유비쿼터스 컴퓨팅 시스템의 응용레벨에서 하위의 통신 레벨까지 확장성은 어떻게 할 것인지, 마지막으로 네크워크화 된 모든 장치나 시스템이 서로 연결된다면 인증되지 않은 소프트웨어나 하드웨어의 공격에 어떻게 대처할 수 있는 지 등이 장기적으로 해결해야할 숙제가 될 것이다[2].

그러면, 유비쿼터스 시대가 도래하면 시큐리티 문제는 어떻게 될까. 결론적으로 말하면, 시큐리티 문제는 유비쿼터스 시대의 성공의 중요한 열쇠가 되며, 인터넷 시대에서의 시큐리티 역할보다도 더 중요한 역할을 맡게 될 것이다. 이는 더 많은 시큐리티의 문제점들이 발생할 수 있으며, 이에 대한 대책들을 수립하지 않는 한 유비쿼터스의 시대는 많은 혼란과 문제들을 야기할 것이다. 즉, insecure, unreliable, intrusive 한 유비쿼터스 기반이 전개되기 전에 위험 요소들을 연구하여 대책을 마련한 후에 추진하는 것이 보다 중요하다는 의미이다. 본 논문에서는 유비쿼터스의 개념, 연구 및 개발 동향 등 유비쿼터스에 관한 내용보다는 유비쿼터스가 가져올 시큐리티에 관한 내용에 초점을 맞추고자 한다. 먼저, 유비쿼터스 네트워킹의 시큐리티 측면에서의 예상 문제점들을 다루고자 하며, 이를 위한 해결 방안이나 방향에 대하여 고찰하고자 한다.

II. 유비쿼터스와 국방 정보 시스템[3]

이라크 전에서 살펴본 바와 같이 현대전은 정보전의 양상을 띄고 있으며, 정보전의 중심에는 C4ISR이나 정밀타격과 같은 정보 통신 시스템에 의존하는 것들이 많다. 이러한 전쟁의 양상은 유비쿼터스 컴퓨팅이나 네트워크에 의하여 크게 달라지게 될 것이다. 모든 전투 장비와 무기, 군수물자, 시설 등의 지능화와 네트워크화가 이루어질 것이며, 작전 수행 등이 유비쿼터스 공간에서 이루어질 것이다. 즉, 미래전은 현재의 물리적 공간만이 아닌 사이버 공간과 물리적 공간이 연계되어 있는 유비쿼터스 공간에서 전개될 것이다.

유비쿼터스 컴퓨팅 네트워크 기술이 군사적으로 활용되면 군사적 역량은 전술적 센싱, 추적 능력의 확대, 고도화된 전술적 최신 정보(fresh information)의 교환, 공유 확대, 그리고 전술 부대들의 커뮤니티 파워 증대를 실현할 수 있을 것이다. 전술적 센싱 능력의 확대는 군사 시설에 센서가 부착되어, 네트워크에 연결시켜 언제라도 전장에서의 모든 상태 변화 정보를 실시간으로 제공해 주는 것이 가능하다는 의미이다. 또한 전술적 최신 정보의 공유 확대는 훈련 및 전장에서의 지형 및 기상 정보, 무기, 장비, 병력 소재지, 탄약 등의 현황 파악 등 여러 정보의 공유가 이루어지게 된다. 커뮤니티의 파워 증대는 군사작전에 필요한 모든 정보를 구성원이 공유 가능하여 작전 부대의 역량을 강화시킬 수 있는 것이다.

유비쿼터스 컴퓨팅 연구도 미국의 국방성이 선두 주자로 추진하고 있다. 대표적인 것으로, Smart dust[4][5], PAC/C(Power Aware Computing/Communication)[6], u-Logistics[3], 국방 유비쿼터스 통합 뉴런 시스템[3]등이 있다. Smart dust는 2001년 미국 방부의 고등연구계획국(DARPA)이 전장의 감시와 군인의 통제를 위한 군 어플리케이션 개발을 위하여 Network Embedded Systems Technology 프로젝트 차원에서 미국 UC 버클리 대학과의 공동 연구 중인 것으로, $1mm^3$ 크기의 작고 가벼워 공중에 따 다닐 수 있는 실리콘 입자(silicon mote)에 자율적인 센서 네트워크(wireless microelectromechanical sensors:MEMS), 센서, 마이크로프로세서, 태양전지, 레이저, 송수신장치 등을 탑재한 보이지 않는 컴퓨터라고 할 수 있다.

수천 수만 개의 입자(mote)가 작전 공간에 뿌려져 이들 입자간에 서로 통신하여 극소의 전력으로 정보 전달을 수행하는 것으로 병력 및 장비의 이동 감지 등 국방 센서 네트워크, 기상 상태, 생화학적 오염, 제품의 유통 등을 감지하거나 스스로 주어진 임무를 수행하는 데 사용할 수 있다.

PAC/C(Power Aware Computing/Communication)는 미국방부의 고등연구계획국(DARPA)에서 연구 중인 것으로 군 어플리케이션과 플랫폼들을 보다 전력적으로 효율적인 통신이나 컴퓨팅을 할 수 있도록, 적시적소에 적절한 전력 배급을 행하여, 전력 소모량을 100내지 1000배 정도로 최소화하여, 상대적으로 통신이나 컴퓨팅 시간을 최대한으로 증가시키기 위한 방법이다.

u-Logistics는 생산 단계에서부터 모든 military objects에 센싱, 정보처리와 저장, 무선통신기능 칩, RFID,센서, 소형 고성능 컴퓨터 기능 등을 삽입하여 유무선 네트워크로 연결된 웹상의 실시간 유비쿼터스 군수 지원 시스템으로 전장 상황을 반영한 군수 지원 활동, 지휘 통제에 활용 등 전투 역량 향상에 크게 기

여하도록 연구되고 있다.

유비쿼터스 국방 감각 뉴런 시스템, 유비쿼터스 국방 운동 뉴런 시스템, 유비쿼터스 국방 인터뉴런 시스템의 통합 형태인 유비쿼터스 통합 뉴런 시스템으로 유비쿼터스 국방 정보화의 방향은 나아갈 것이다. 이는 인간의 뉴런 구조와 같이 모든 지휘통제소, 전투부대와 지원 부대, 모든 군사 시설들과 네트워크로 연결되어, 언제 어디서나 어떤 네트워크와 디바이스로도 정보를 송수신, 명령, 행동할 수 가 있게 되는 것이다.

먼저, 국방 감각 뉴런 시스템은 부대나 작전 지역 등의 군사적 활동과 관련된 모든 공간과 무기, 탄약 등 군사적 사물에 바이오칩, RFID 등 각종 센서를 삽입하여 지능화하고 네트워크로 연결하는 것이며, 국방 운동 뉴런 시스템은 마이크로머신, 바이오 마이크로 머신, 마이크로 모터와 기어, 로봇, 인공지능시스템을 무기나 장비 등에 탑재하여 언제 어디서나 어떤 네트워크에서도 작동을 명령할 수 있도록 네트워크화 되어 있는 시스템이다. 그리고 국방 인터뉴런 시스템은 수백억개의 디바이스, 수천억개의 센서?칩, 수조개의 RFID 등과의 다발적이며 대용량인 정보를 실시간 처리 및 관리하는 시스템으로 광대역 완전 IP 억세스 망 형태가 될 것으로 보인다.

유비쿼터스와 국방 정보 통신 네트워크는 네트워크의 속도, 용량뿐만이 아니라 유무선, 위성, 이동 통신간의 완전한 통합, IPv6 조기 구축 등과 신뢰성 및 보안이 확보되어 있는 고도의 기반 시스템이 연동되는 네트워크로 발전되어 갈 것이다.

Ⅲ. 유비쿼터스와 시큐리티 고려사항

유비쿼터스 시대에서의 시큐리티는 어떠할 까. 현재로써는 어떤 공격자가 나타나서 어떠한 방법으로 유비쿼터스 환경을 불안전하게 할지 알 수가 없다. 또한 누가 공격자가 될 는 지도 알 수가 없다. 단지 추측해 볼 수 있는 것은 유비쿼터스의 특성상 기존의 해커들로만 공격자의 범위가 한정되는 것이 아니라 보다 더 광범위한 범위에 걸쳐 공격자들이 있을 것으로 생각된다. 보다 구체적인 환경이나 네트워크, 시스템, 응용 등이 나타날 때까지는 취약점이나 공격 형태 그리고 대책 등에 대하여 논하기 어려울 것으로 생각된다.

단지 현재로써는 어떠한 공격이나 취약점, 대책 등에 대해서 상상해보거나 추측해보는 것이 의미가 있을 것이며 발전의 추이를 지켜보면서 보호해야할 범위를 분류해 보는 것이 중요할 것으로 생각된다. 유비쿼터스 컴퓨팅에서 나타나는 각종 기술들 가운데에서 잠재적인 시큐리티 문제가 무엇이 있을지를 상상해보면서 지켜보는 것이 의미가 있으며, 새로운 기술의 등장 시는 시큐리티 문제가 어느 정도 검토된 결과가 반영될 수 있기를 희망하는 차원에서 연구해 보는 것이 현 단계에서는 최선의 것으로 생각된다.

유비쿼터스 특성을 고려해 볼 때 사이버 공간이던 물리 공간이던 기존의 보안은 디지털화되어 컴퓨터에 저장된 정보들이 문제가 되었지만 유비쿼터스 네트워크에서는 개인의 모든 정보가 해킹에 노출될 수 있다. 뿐만 아니라 유비쿼터스 네트워크에서는 개인의 정보뿐만 아니라 사물까지도 침해당할 우려가 높다. 또한, 기존의 네트워크에서는 해커가 침입하는 장소는 개인의 컴퓨터에 국한된 반면, 유비쿼터스 네트워크에서의 해커는, 개인의 사적인 모든 공간에 침입하는 셈이다. 유비쿼터스 네트워크에서의 사이버 테러는 말 그대로 물리공간과 사물, 그리고 육체에 대한 테러를 포함하게 되며, 개인이나 기업과 국가의 정보보호를 뛰어 넘어 광범위한 공간 보호가 요구되고 있다.

또한, 유비쿼터스 네트워크에서는 해커 등 공격자의 범주가 보다 넓어지며, 공격도 보다 용이하여지며, 피해를 입을 경우 피해 범위나 규모도 막대할 것으로 예상된다. 그리고 기존의 환경에서는 심각하게 고려되지 않은 익명의 objects에 대한 인증, 전력 에너지 사용 문제, 위치 정보, 일회성 보안, 각종 암호 도구들의 구현, tamper-resistant, 재밍이나 서비스 거부 공격에 의한 가용성 등이 유비쿼터스 컴퓨팅 환경에서는 우선 고려해 볼 수 있는 시큐리티 사항이다.

그리고, 익명의 principals를 인증해야 하거나, 디바이스 공격이 통신로상의 공격보다 많을 것으로 예상된다. 또한, 전력 소모 등에 의한 서비스 거부 공격이 아주 주요한 문제점이 되며 일시적인 거래를 안전하게 해주는 방안의 필요 등이 크게 다를 것으로 생각된다. 이외에도 기존 분산 환경에서의 시큐리티 문제와 유비쿼터스 컴퓨팅 환경에서의 다른 점을 찾아볼 수 있다.

Ⅳ. 유비쿼터스와 시큐리티 서비스

유비쿼터스 컴퓨팅 환경은 기존의 보안 기술로 적용하기에는 많은 다른 점을 가지고 있다. confidence level이 서로 다른 인증 방식이 필요하거나 또한 사용자의 위치에 대한 프라이버시도 만족해야 하는 인증 방식이 필요하게 될 것이다. 예를 들면, 기존의 대표적인 인증 방식인 kerberos 인증 방식은 사용 범위

가 지정 워크스테이션으로 국한되거나 클라이언트의 안전한 환경을 가정하여 이용되지만 유비쿼터스 컴퓨팅 환경에서는 이러한 조건을 제공하기가 어렵기 때문에 새로운 별도의 방식이 고려되어야한 하는 것이다.

유비쿼터스 컴퓨팅 환경은 무선전송이나 이동통신에 크게 의존하게 되므로 이들 통신 구간에 대한 보안이 중요한 문제로 대두됨은 기존의 보안 방식과 크게 다를 것이 없을 것이다. 그러나, 유비쿼터스의 소형화나 저 전력화에 따른 환경 조건은 기존의 암호 방식이나 프로토콜들을 그대로 사용하기에는 많은 문제점들을 내포하고 있다.

한편, 유비쿼터스 컴퓨팅 환경에서는 인증이 없는 기밀성 제공은 기밀성 여부의 정당성을 확보할 수 없어 인증이 기밀성보다 중요한 문제가 된다. 즉, 인증은 기밀성이나 무결성, 가용성의 선행조건으로 유비쿼터스 컴퓨팅 환경에서는 고려되어야 한다. 따라서 본 장에서는 유비쿼터스 컴퓨팅과 시큐리티 서비스와의 관계를 중심으로 고찰해 보고자 한다.

1. 인증(Authentication)[7,8,11,12]

1.1 유비쿼터스 컴퓨팅 환경에서의 인증의 새로운 요구 조건

분산 네트워크상의 적용 가능한 기존 정보보호 기술들은 대부분 그대로 적용하기가 곤란하며, ad hoc 네트워크에서의 가장 관심 있는 문제가 인증이 될 수 있다. ad hoc 네트워크는 특성상 온 라인 서버의 존재를 가정하기가 어려운 환경이므로 기존의 온라인 서버를 이용한 인증 방식은 적용하기는 어렵다. 예를 들면, Kerberos 인증 방식을 이용할 경우, 새로운 가입자는 티켓을 얻기 위한 인증 서버가 필수적이지만 유비쿼터스 환경에서는 곤란하기 때문이다.

온라인 서버를 고려할 수 없는 유비쿼터스 환경에서, 공개키 암호방식에 의한 인증을 사용할 경우, 즉 공개 키 기반 구조(PKI)를 사용할 경우, 인증서 취소를 위한 revocation list를 인증 서버를 통하여 확인할 수가 없어 인증서 유효 기간 내에 불법 사용이 있을 경우 막을 방법이 없는 실정이다. 또한 기존의 인증서 유효 기간 만료 일자에 관련된 secure clock도 별도로 필요하게 되어 경제적인 부담이 늘어나는 문제가 발생하게 된다. 또한 유비쿼터스 컴퓨팅 환경의 특성상 네트워크 접속이 때때로 중단되거나 보증되지 않기 때문에 온라인 접속을 요구하는 기존의 PKI, Kerberos 등의 인증 방식을 그대로 적용하기도 어려운 실정이다.

유비쿼터스 컴퓨팅 환경에서는 PDA와 같은 범용 리모콘을 사용하게 되는 데, 이 때, 동일 PDA를 사용하면서 사용하던 정보가전만을 매매하거나 또는 정보 가전 등은 그대로 사용하면서 손상 또는 고장난 PDA를 바꿀 수도 있는 환경이 되어야 한다. 즉, 이와 같은 일시적인 거래(transient association) 환경이 유비쿼터스에서는 많이 발생할 것으로 생각된다. 이때 타인들이 제품들을 임의로 제어하는 것은 물론이며 일시적인 거래가 안전하게 이루어지는 보안 대책이 무엇보다도 필요하다.

1.2 안전한 일시 거래 방안(secure transient association)

유비쿼터스 컴퓨팅 환경에서의 일시적인 거래는 주요한 환경이 되며 이에 대한 보안 대책이 새롭게 고려되어야 한다. 현재 이러한 환경에서의 보안 대책은 Frank Stajano의 Resurrecting Duckling Security Policy 모델이 제안되어 있다[7][8].

Stajano 모델의 기본 개념은 각인(imprinting)과 윤회사상을 접목한 것으로 부화한 오리(duckling)는 처음으로 본 움직이는 물체를 어미로 인식하는 현상인 각인(imprinting)과 인간의 육체는 하드웨어이고 영혼은 소프트웨어로 볼 때, 육체에 영혼이 거주하는 단계를 각인, 죽음에 의하여 육체와 영혼의 관계가 분리되어 육체를 출생 전으로 되돌리는 윤회로 구성되어 있다.

모델의 정책 기본 원칙은 다음 4단계로 이루어진다.

1.2.1 두 단계 원칙(Two state principle)

오리는 각인할 수 있거나(imprintable) 각인 당할 수 있는(imprinted) 상태에 있을 수 있으며, 각인할 수 있는 상태는 누구나 수행 가능하나 각인 당할 수 있는 상태는 오로지 어미 오리(mother duck)의 명령에 의해서만 복종한다.

1.2.2 각인 원칙(Imprinting principle)

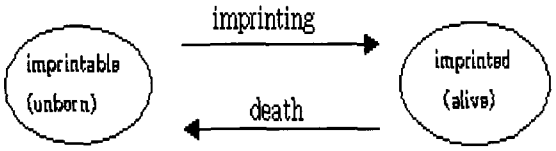
각인하는 것은(imprinting) 각인할 수 있는 상태에서 각인되는 상태로 천이하는 것을 말한다. 어미 오리는 기밀성과 무결성이 보장된 채널을 통하여 각인 키를 오리에게 전송한 후 각인 키는 별도로 백업 관리하여야 한다. 예를 들어, 공장에서 출하된 디바이스는 자신에게 맨 처음 비밀 키를 주입하여 준 Entity를 owner로 인식(어미 오리로 판단)하게 되며 이때의 비밀키를 각인 키인 imprinting key라 할 수 있다.

1.2.3 죽음 원칙(death principle)

각인 당할 수 있는(imprinted) 상태에서 각인 할 수 있는 상태로 천이 하는 것을 말한다. 죽음이 가능한 상황은 어미 오리의 명령에 의할 경우, 사전에 정의된 유효 기간이 경과될 경우, 그리고 특정 거래가 종료될 경우에 한한다.

1.2.4. 암살 원칙(Assassination principle)

공격자가 오리를 암살(죽음원칙에 의한 죽음이외의 죽음)할 경우에는 아주 비싼 비용이 소요되도록 오리가 제작되어야 한다.



Duckling 모델은, 유비쿼터스 환경에서 디바이스인 오리가 서로를 인증하는 모델로, 4가지 원칙으로 인증을 행하여 안전한 일시 거래가 이루어질 수 있는 모델이다. 어미 오리는 상황에 따라서 달라지며 맨 먼저 각인 키를 전송하여 오리가 imprinted 상태로 되었을 경우 전송한 오리가 어미 오리가 된다. 또한, 패스워드 분실이나 리모콘 등의 파괴 시 정당한 사용자나 디바이스인 오리가 각인 키를 분실하였을 경우에는 백업 된 어미 오리의 각인 키를 이용하여 다시 복구가 되도록 하는 방법이 소개되고 있다.

한편, 각인 원칙에서 어미 오리가 오리에게 안전하게 각인 키를 전송하기 위해서는 기존의 공개 키 방식에 의한 키 공유를 고려할 수 있다. 그러나, 유비쿼터스 컴퓨팅 환경에서는 어미 오리와 오리간의 키 공유는 효과적이고 경제적이며 간단한 방식으로 고려되어야 한다. 하나의 방안으로 태어나기 전 상태의 디바이스에 단순한 전기적 접촉만에 의하여 각인을 위한 비밀 공유 정보를 전송하는 방안이 제안되고 있다.

제안 모델은 온라인 서버가 존재하지 않은 상태에서 미확인 principle의 identity를 인증하기 위한 모델로 개발된 것으로 오리에게 각인 키를 보내준 principle이 어미 오리라는 사실은 알지만 어미 오리 자체가 누구인지는 알 수 없는 방식으로 익명의 인증을 제공하고 있다. 그러나 Duckling 모델은 하나의 제안일 뿐 실제 적용 시의 많은 문제점을 내포하고 있어 새로운 모델 개발이나 Duckling 모델의 개선 등의 연구가 필요하다.

2. 기밀성(Confidentiality)[7]

일반적으로 유비쿼터스 컴퓨팅 환경에서 시큐리티 문제를 논할 때에는 무선 네트워크에서의 도청 문제를 맨 먼저 생각하게 된다. 그러나 기존의 정보보호 기술에서 인증이나 키 공유와 같은 어려운 문제를 해결하여 왔으며 기밀성 제공을 위한 암호 알고리즘 개발도 수행되어 왔기 때문에, 유비쿼터스 컴퓨팅 환경에서 기밀성 제공 차원의 새로운 정보보호 기술 개발보다는 기존 정보 보호 기술의 구현이 보다 실질적인 문제가 될 수 있다.

기밀성 제공의 범위는 크게 무선 전송 구간과 디바이스에 저장되어 있는 모든 정보가 해당되며, 디바이스들의 서비스가 중단된 후에도 위협은 여전히 계속될 수 있다. 이러한 경우의 기밀성 제공은 암호 기술을 사용하여 제공될 수밖에 없다. 물론 저장 정보도 암호화한 후 저장해 두는 것이 바람직하다. Dallas DS5002 Bus Encrypting Cryptographic processor와 같이 메인 메모리 암호를 제공하는 형태의 프로세서가 하나의 예가 될 수 있다.

전형적인 유비쿼터스 컴퓨팅 디바이스들은 소형이며 아주 극소의 전력을 요구하는 프로세서(peanut processor) 환경으로 기존의 공개 키 암호 구현에 많은 한계를 가지게 되는 것이다. 전력 소모 문제를 해결하기 위해서는 클럭없이 동작하면서 계산이 이루어지지 않을 때에는 정지하고 있는 Asynchronous processor 개발의 필요성이 야기되고 있지만, 유비쿼터스 컴퓨팅 환경에서의 기밀성 제공을 위해서는 이러한 프로세서의 개발은 물론이고 사용 암호 알고리즘이나 프로토콜들이 이러한 전력 소모 문제나 소형화를 고려하여 최적의 구현이 될 수 있는 알고리즘이나 방식이 되어야 한다.

즉, 다시 말해서 암호 primitives의 적용 여부는 유비쿼터스 컴퓨팅 디바이스들의 계산 능력에 의존하게 되는 것이다. 따라서 기존의 공개 키 암호 방식을 속도도 느리고 메모리 용량도 부족한 유비쿼터스 컴퓨팅 환경의 peanut processor에 그대로 적용하기는 부적합하다. 그러나, 기존의 공개 키 암호 방식을 peanut processor에 적용해 보는 하나의 방안으로 Low exponent RSA(e=3)을 사용하는 방안을 검토해 볼 수 있다. 다소 안전성에는 문제가 있지만, peanut processor에서는 암호화나 서명 검증용으로 그리고 계산 능력이 큰 디바이스에서는 복호화나 서명 생성용으로 사용하는 유비쿼터스 환경에 적용해 볼 수

있다.

또한, 비밀 키 암호의 일종인 불록 암호 알고리즘도 유비쿼터스 컴퓨팅 환경에서는 암호 알고리즘의 구현이 보다 중요하게 된다. 요구되는 암호 처리 속도에 따라 고속의 계산이 요구되며 고속의 계산 실현을 위해서는 높은 주파수의 클럭 동작이 요구된다. 높은 계산 처리 요구는 유비쿼터스 컴퓨팅 환경에서 일반적인 저 전력 소모 문제와 대치되게 된다. 즉, 바테리 사용 용량과의 문제를 고려하지 않을 수 없게 되어 저 전력 고속 처리 가능한 블록 암호 알고리즘의 설계나 개발이 유비쿼터스 컴퓨팅 환경에서는 반드시 이루어져야 한다. 다시 말해서 암호의 안전성 못지 않게 소비 전력 관리 문제가 중요하게 되는 것이다. 즉, b/s 보다 bits/joule이 더 중요할 수도 있다는 것이다. 물론 공개 키 암호 방식에서도 함께 적용된다.

또한 유비쿼터스 컴퓨팅 환경에서는 anonymity, tracebility, traffic analysis 문제가 기밀성보다 더 중요할 수가 있다. 통신 내용 등은 기밀성 제공 차원에서 암호에 의하여 보호될 수 있지만, 언제 어디서 어디로, 누구에게서 누구에게로와 같은 정보는 보호되지 못한다. 또한 트래픽 분석과 같은 공격에도 대처하기가 어려운 실정이다. 이외에도 위치 정보나 사용자 거래 정보는 사용자의 관점에서 아주 중요한 프라이버시 정보가 되며, 유비쿼터스 사회에서는 이러한 정보들을 쉽게 그리고 대량으로 확보할 수 있기 때문에 오히려 유비쿼터스 기반 환경이 유비쿼터스 감시 도구로 변하는 것도 불가능한 것은 아니라고 생각된다.

3. 무결성(Integrity)[7,13]

인증의 일반적인 가정은 네크워크는 안전하지 못하나 디바이스나 사용자는 정직하거나 안전하다는 가정하에서 기존의 정보보호 기술들은 사용되고 있다. 그러나, 유비쿼터스 컴퓨팅 환경에서는 이러한 가정을 유지하는 것이 어려울 것으로 생각되며 공격자들은 보다 쉽게 공격을 시도할 것으로 예측된다.

무결성을 고려할 경우, 전송 중인 메시지와 디바이스에 저장되어 있는 정보가 어떤 위협에 의하여 변경되지 않았는지 여부를 확인하는 것이 일반적이다. 그러나, 유비쿼터스 컴퓨팅 환경이 아닌 기존의 경우에는, 메시지 내용에 대해서만 무결성을 고려하지만 유비쿼터스 컴퓨팅 환경에서는 메시지보다도 디바이스 자체의 무결성이 더욱 중요하게 된다. 공격자가 디바이스 내부의 비밀 정보에 접근하거나 변경하는 것이 불가능하도록 하는 기술들이 유비쿼터스 컴퓨팅 환경에서는 더욱 중요한 것이다. 물론 기존의 tamper-resistant나 tamper-proof 기술들은 고비용이며 기술적으로 어렵지만 유비쿼터스 컴퓨팅 환경에서는 보다 발전될 가능성이 높은 분야로 생각된다.

3.1 메시지 무결성을 위한 방식

point-to-point 메시지 무결성은 기존의 해쉬 함수나 MAC(Message Authentication Code)에 의하여 제공될 수 있다. 그러나, point-to-multipoint 메시지 무결성은 MAC 보다는 공개 키 암호에 의한 디지털 서명이 보다 안전하며 효율적이다. 그러나, 앞에서도 살펴본 바와 같이, 유비쿼터스 컴퓨팅 환경인 peanut processor가 처리하기에는 공개 키 암호 방식은 연산 비용이 너무 많이 소요된다.

이러한 문제점을 개선하기 위하여 디지털 서명 방식을 해쉬와 MAC의 chain 형태로 구현하여 연산 비용을 적게 한 방식으로 Ross Anderson 등에 의한 Guy Fawkes 방식[10]이 있다. Guy Fawkes 프로토콜은 bit commit 방식을 이용한 것으로 송신자가 보내는 패킷에 해쉬함수 결과와 키 그리고 MAC의 결과 값을 첨부하여 보내는 방식으로 전송 패킷의 형태는 다음과 같다.

Pi-1 = Mi-1 || h(Ki) || Ki-2 ||MACKi-1(Mi-1||h(Ki)||Ki-2)
Pi = Mi || h(Ki+1) || Ki-1 ||MACKi(Mi||h(Ki+1)||Ki-1)
Pi+1 = Mi+1 || h(Ki+2) || Ki ||MACKi+1(Mi+1||h(Ki+2)||Ki)

각 패킷 Pi는 메시지 Mi의 패킷이며 Ki는 랜덤한 값이다. 패킷 Pi-1은 랜덤한 값인 Ki의 commitment인 h(Ki)를 포함하고 있으며 패킷 Pi+1에서 Ki 값을 reveal하고 있다. 패킷 Pi의 메시지 Mi의 무결성은 패킷 Pi+1에 포함되어 있는 Ki를 이용하여 확인할 수 있는 방식이다.

Guy Fawkes 프로토콜에서는 수신자가 패킷 Pi를 수신한 사실을 송신자가 반드시 확인한 후에 패킷 Pi+1을 송신하여야 한다. 만일 송신자가 확인하지 않을 경우에는 Ki를 이용하여 위조의 메시지 Mi`와 패킷 Pi`를 만들 수가 있기 때문이다. 그리고 모든 패킷을 수신자가 수신해야만 완전한 무결성 확인을 할 수 가 있는 프로토콜로 패킷 Pj-1의 수신이 실패할 경우 Kj의 commitment가 없어 무결성을 확인할 수가 없게 되는 단점을 가지고 있다.

Guy Fawkes 프로토콜의 단점들을 개선하기 위하여

제안된 방식으로 TELSA(Timed Efficient Stream Loss-tolerant Authentication) 프로토콜[14]이 있다. 이 프로토콜은 Mi+d가 보내어지기 전에 어느 때라도 Mi 가 수신만 된다면 메시지 무결성 확인은 할 수가 있는 방식이다. 지연 파라메터 d를 응용분야나 네트워크 상태에 따라 조정하여 사용할 수가 있으며 d=1일 때가 Guy Fawkes 프로토콜이 된다. 그러나 이 프로토콜은 Guy Fawkes 프로토콜의 단점을 개선하여 전체의 Throughput rate를 개선하였지만 수신 패킷과 패킷 인증간의 지연이 증가되는 단점을 가지고 있다. TELSA 프로토콜의 패킷 형태는 다음과 같다.

Pi = Mi || h(Ki) || Ki-d ||MACKi(Mi)
Pi+d = Mi+d || h(Ki+d) || Ki ||MACKi+d(Mi+d)

한편, 전송 도중의 패킷 손실을 방지하기 위한 개선책으로 Lamport의 패스워드 인증 방식[15]를 이용하는 방식도 있다. 즉, 초기 Kn을 랜덤한 것으로 선택한 후 Ki=h(Ki+1)에 의하여 Tree 구조로 생성하면, 분실된 Kj=fhj-i(Ki), Ki=any previous known good key를 복원하여 사용할 수 있다.

3.2 디바이스 무결성을 위한 방식

기존의 컴퓨터 환경과는 달리 유비쿼터스 컴퓨팅 환경의 디바이스들은 공격자들이 쉽게 가져가거나 파괴하거나 바꿔치거나 분해하는 등의 공격들이 아주 용이한 특징을 갖고 있다. 또한, 기존의 비접촉 공격인 Timing attacks, differential power analysis, protocol failure and glitch attacks, attacks on security sealing 등에도 쉽게 공격받을 수 있다.

이러한 대책의 대표적인 기술들은 tamper-proof, tampering을 시간적으로 추적할 수 있는 tamper-evident, tamper-resistant, 비 접촉 공격에 대한 각종 대응 설계 기술들이 있으나 유비쿼터스 컴퓨팅 환경의 디바이스 무결성 제공을 위해서는 더욱 더 새로운 개념의 기술들이 개발되지 않으면 안될 것으로 생각된다.

4. 가용성(Availability)[7]

무선 시스템에서의 가용성에 대한 고전적 공격의 하나가 통신 채널에 대한 재밍(Jamming)이다. 이러한 재밍 공격은 무선 통신이 주요 기반인 유비쿼터스 컴퓨팅 환경에서도 그대로 적용될 수가 있으며 더욱 취약할 수 있다. 그리고, 유비쿼터스 컴퓨팅 환경의 디바이스들의 제한된 전력을 계속 소모하게 하는 서비스 거부 공격도 가용성 제공에 대한 주요한 위협이 되고 있다.

4.1 통신 채널에 대한 위협

공격자가 모든 무선 대역에 걸쳐서 재밍을 할 수 있는 능력이 있는 경우의 최선의 대책은 방해 공격에 소요되는 비용이 합법적 사용자의 통신소요 비용보다 월등하게 크도록 재밍 공격에 대한 비용을 증가시키는 방법뿐이다. 재밍에 대한 대책은 널리 알려져 있는 것과 같이 frequency hopping이나 direct sequence spread spectrum 방식 등이 있다.

또한, 임의의 공격자는 새로운 클라이언트인 것처럼 서버에 접근을 자주 시도하여 서비스 거부 공격을 행할 수 있다. 이 공격은 이전 클라이언트와 서버가 설정해 놓은 통신에 대해서는 재밍 공격의 어려움이 있지만 새로운 클라이언트의 가입은 곤란하게 할 수가 있다. 이러한 종류의 서비스 거부 공격의 대책으로는 시간 소모를 위한 접속을 시도하는 source를 식별하여 블랙리스트 관리를 하는 것이 하나의 방식이 될 수 있다. 그러나 이러한 방법은 자주 접속하는 사용자가 반드시 공격자인지 구별하기가 쉽지 않으며, 자주 접속하는 사용자가 어떤 사용자인지 판단하기 위해서는 별도의 정보가 더 필요하게 되는 문제점이 있다.

개선 방법으로는 자주 접속하는 사용자는 다소 접속을 자제시키고 추가적인 업무를 수행하는 서버에게는 별도의 이점을 제공하는 방식을 고려해보거나 서버가 암호학적인 퍼즐 문제를 클라이언트의 접속 시 출제하는 방식을 이용하여 접속 횟수를 조절해 보는 방식을 고려해 볼 수도 있다.

4.2 전력 에너지에 대한 위협

유비쿼터스 컴퓨팅 환경에서의 전력 에너지 제한은 peanut 디바이스에서 특히 두드러진다. 이러한 전력 제한 환경에서의 공격자들은 공격 소요 시간은 milli-seconds대로, 방어에 소요되는 시간은 수분대로 가능한 서비스 거부 공격 방법들을 모색할 것이다. 즉, 바테리의 전력을 소비하도록 하여 결국에는 서비스를 제공할 수 없는 상태로 만드는 것이다. 유비쿼터스 컴퓨팅 환경에서의 이러한 공격은 CPU 소비나 통신 채널의 재밍공격보다도 훨씬 더 심각한 공격 형태이다.

이러한 공격의 대처 방안으로는 역시 idle time 동안에는 프로세서들을 중지시켜 전력 소모를 최소화하는 것은 물론이고 priority가 높은 작업에 한하여 바테리 사용을 우선 지정하는 resource별 전력 소모를 관리하는 방법이 하나의 방안이 될 수 있다.

V. 무선 Ad Hoc 네트워크와 RFID 시큐리티

유비쿼터스 컴퓨팅의 핵심 기술로 무선 Ad Hoc 네트워크가 거론되고 있으며 센서네트워크의 일환인 스마트 태그 기술이 최근 활발히 논의되고 있다. 이에 관한 시큐리티를 검토하여 보는 것도 향후 전개될 유비쿼터스 컴퓨팅에서의 시큐리티 문제를 미리 점검해 볼 수 있을 것으로 판단된다.

먼저, 무선 Ad Hoc 네트워크에서의 시큐리티는 각 노드들이 수시로 이동하거나, 모든 노드들간의 무선 전송으로 다른 노드와는 독립적으로 운영되는 등 무선 Ad Hoc 네트워크 특성으로 인하여 기존 네트워크 보다 시큐리티 대책이 쉽지 않을 것으로 인식되고 있다[16][17]. 네트워크 특성상 노드들 사이의 보안 메커니즘의 설계가 기존의 방식으로는 어려울 것으로 판단되며 새로운 개념의 검토가 이루어져야 할 것이다.

한편, 센서 네트워크의 일환인 스마트 태그 기술을 이용한 RFID 기술이 최근 각광을 받고 있다. 리더기로부터의 고주파 신호를 받게 되면 태그 해당 상품 등의 세부 정보(ID)를 전송하여 여러 응용 분야에 활용될 수 있는 이 기술 또한 시큐리티와 프라이버시 문제를 안고 있다[18][19]. 누구든지 태그 정보를 쉽게 읽어볼 수 있는 점, 태그와 리더기간의 상호 인증 문제, 아주 저렴한 가격의 스마트 태그 구현을 위하여 시큐리티 기능 구현의 커다란 제약이 존재하는 등 유비쿼터스 컴퓨팅 환경에서의 문제점들이 등장하게 된다. 또한, 태그에 내장되어 있는 ID 정보를 이용하여 개인의 구매 패턴이나 생활 패턴 등의 프라이버시 문제까지도 나타나게 된다.

물론 무선 Ad Hoc 네트워크나 RFID 기술에 의한 시큐리티 문제는 앞으로의 연구 결과에 따라 많은 해결책들이 등장할 것으로 예상되며 유비쿼터스 컴퓨팅 시대의 시큐리티 문제를 보다 가속화하거나 이슈화하는 계기가 될 것으로 생각된다.

VI. 결 론

본 논문에서는 유비쿼터스 네트워크 기반이 전개되기 전에 유비쿼터스의 시큐리티 문제를 고찰해보았다. 유비쿼터스와 시큐리티 고려사항, 유비쿼터스와 시큐리티 서비스인 인증, 무결성, 기밀성, 가용성 등에 관하여 기존의 발표된 자료를 중심으로 고찰하였다. 특히, 유비쿼터스 네트워크 환경 하에서는 해킹 공격도 보다 용이하여 지며, 정보 접근 범위나 피해 규모도 광대하여 지금까지의 취약점 보다 더 많은 취약점을 예상할 수 있었으며, 온라인 서버 가정이 곤란한 유비쿼터스 컴퓨팅 환경에서의 인증, 전원 등의 제약을 고려해야하는 암호 알고리즘이나 프로토콜의 구현 문제, 서비스거부공격 대책 등의 문제가 거론되었다. 보다 본격적인 연구가 뒤따라서 안전하고 신뢰성 높은 유비쿼터스 네트워크 시대를 맞이할 수 있도록 하여야 할 것이다.

참고문헌

[1] Mark Weiser, "The Computer for the Twentity-First Century", *Scientific American*, 265(3), pp. 94-104, 1991.

[2] 김완석, 백민곤, 박태웅, 이성국, "유비쿼터스 컴퓨팅과 이지리빙 프로젝트", *한국전자통신연구원 주간기술동향 1088호*, pp. 1-12, 2003.3.

[3] 하원규, 김동환, 최남희, 유비쿼터스 IT 혁명과 제3공간, *전자신문사*, 2002.

[4] 민봉기, 심규환, 강진영, 조경익, "유비쿼터스 무선통신 반도체 소자 기술의 동향", *한국전자통신연구원 주간기술동향 1091호*, pp.14-26, 2003.4.

[5] Smart dust, www-bsac.eecs.berkeley.edu/~pister/SmartDust/

[6] PACC, www.darpa.mil/ipto/research

[7] Frank Stajano, *Security for Ubiquitous Computing*, Wiley, 2002.

[8] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing", *IEEE security and Privacy*, 2002.

[9] L. Bussard and Y.Roudier, "Authentication in Ubiquitous Computing", Workshop on Security in Ubiquitous Computing, *4th international UBICOMP*, 2002.

[10] Ross Anderson, "A New Family of Authentication Protocols", *Operating Systems*

Review, 32(4), pp.9-20, 1998.

[11] J Al-Muhtadi, A. Ranganathan, R. Campbell and M. D. Mickunas, "A Flexible, Privacy Preserving Authentication Framework for Ubiquitous Computing Environments", *Workshop on Security in Ubiquitous Computing, 4th International UBICOMP*, 2002.

[12] J.M Seigneur, S. Farrell, C.D.Jensen, "Secure ubiquitous computing based on entity recognition", *Workshop on Security in Ubiquitous Computing, 4th International UBICOMP*, 2002.

[13] J. Falk and S.Bjork, "Privacy and Information integrity in Wearable Computing and Ubiquitous Computing", *Workshop on Security in Ubiquitous Computing, 4th International UBICOMP*, 2002.

[14] A. Perrig, R.Canetti, D.Tygar and D.Dong, "Efficient Authentication and Signature of Multicast Streams over Lossy channels", *Proceedings of IEEE Symp. on Res in Security and Privacy*. 2000.

[15] Leslie Lamport, "Password Authentication with Insecure Communication", *Communication of the ACM*, 24(11), pp.770-772, 1981.

[16] J.Kong, P.Zerfos, H.Luo, S.Lu and L.Zhang, "Providing robust and ubiquitous security support for mobile ad-hoc networks", *IEEE ICNP*, 2001.

[17] 이승형, 홍순좌, 최헌준, "무선Ad Hoc 네트워크에서 서비스 거부 공격의 위험성 분석", *제15회 정보보호와 암호에관한 학술대회(WISC2003)*, pp.660--669, 2003.

[18] S.E.Sarma, S.A.Weis and D.W.Engels, "RFID Systems, Security & Privacy Implications", Auto-ID center, MIT, 2003. http://www.autoidcenter.org/research

[19] Takagi Hiromitsu, "RFID 프라이버시(Japanese)", IC태그와 유비쿼터스사회조사연구위원회, 2003.9.

〈著 者 紹 介〉

박 춘 식 (Choon-sik Park)
평생회원

1995년 : 일본 동경공업대학교 전기전자공학과 공학박사
1989년 - 1990년 : 일본 동경공업대학교 초빙연구원
1982년~현재 : 한국전자통신연구원 부설 국가보안기술연구소 책임연구원
2003년~현재 : 고려대학교 정보보호대학원 겸임교수
1990년~현재 : 한국정보보호학회 이사