제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

유비쿼터스 컴퓨팅 & 네트워크 보안분석

정 상 일*, 송 원 덕*, 이 원 찬*, 윤 동 식*
* 안동과학대학 사이버테러대응학과

요 약

유비쿼터스 컴퓨팅(Ubiquitous Computing)은 많은 분야의 실생활에서 적용이 되고 있다. 이미 각 선진국에서는 좀 더 사용자들에게 편리한 유비쿼터스 환경을 제공하기 위해 유비쿼터스에 대한 다양한 연구를 추진 중 이다. 언제 어디서나 사용자가 원하는 정보와 서비스를 제공받을 수 있다는 이점이 있지만 다른 한편으로는 유비쿼터스 네트워크의 취약점을 이용한 여러 가지 공격 즉 Rogue AP, IP spoofing, DoS 등의 공격에 사회적으로 큰 혼란을 가져올 수 도 있다. 이에 본 논문에서는 유비쿼터스 컴퓨팅 네트워크 환경에서의 보안요구 사항등을 분석해보고 유비쿼터스 컴퓨팅 환경의 네트워크 인프라 구축을 위한 핵심기술인 무선 "Ad hoc"와 RFID에 대해 연구하고자 한다.

Ubiquitous Computing & Network Security Analysis

Jung Sang il*, Lee Won Chan*, Song Won Duck*, Yun Dong Sic*
* Andong Science College Dept. of Cyberterror Defense

ABSTRACT

Ubiquitous Computing is gradually accepting in our real society. Already some Advanced State has studying of Ubiquitous for more convenience Ubiquitous environment. Anywhere, Anytime user can be provided information and service that he want, but it has some problem such as Rogue AP, IP spoofing, DoS attack, Warm which can causing social confusion in Ubiquitous society. In this situation we must analytics that security requirement in the Ubiquitous network environment and investigate "Ad hoc" and RFID which is main technique for network infra construction.

1. 서 론

유비쿼터스 컴퓨팅(Ubiquitous Computing)이라는 신조어가 처음 소개된 것은 미국 Xerox사의 Polo Alto Research Center의 Mark Weiser(1952~1999)가 1991년 9월판 Scientific American의 "The Computer for the Twentity-First Century" 논문의 첫 머리에 " 가장 심오한 기술은 사라지는 것들이다. 일상생활에서 구별이 되지 않을 정도로 스며들어버리는 것이다" 라는 말로 시작하고 있다.

Mark Weiser의 이 비전이 제시되었을 때는 당시의 기술로는 불가능한 것으로 많은 사람들이 생각하고 있었다. 그러나 마이크로프로세서의 지속적인 가격하락과 소형화에 따라 더욱 많은 사물에 칩을 내장시킬 수 있게 되었으며, 센서의 기능 향상으로 사물의 식별과 위치 확인이 용이해졌으며 통신기술의 진보에 따라 사물간의 통신이 좀더 쉬워짐에 따라 유비쿼터스 컴퓨팅 개념의 실현이 가능해 지고 있다. 유비쿼터스 컴퓨팅은 도시개혁, 산업혁명, 정보혁명에 이어 인류 역사상 네 번째의 혁명을 불러일으킬 정도로 그 파급효과가 클 것으로 예상되며 현재 많은 국가에서 전략적으로 연구가 진행되고 있다. 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, 자동지원 시스템이 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 네트워크화 된 모든 장치나 시스템이 서로 연결된다면 인증되지 않은 소프트웨어나 하드웨어의 공격에 어떻게 대처할 구 있는 지 등이 장기적으로 해결되어야 할 숙제가 될 것이다.

본 논문에서는 유비쿼터스 시큐리티 고려사항 및 유비쿼터스환경 보안요구사항, 그리고 이 논문의 핵심인 "Ad hoc" 네트워크와 RFID에 대해 연구하고자한다.

2. 유비쿼터스 시큐리티 고려사항

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

2.1 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, IP스푸핑(Spoofing), DoS 공격, 트로이목마, 웜, 바이러스 등, 신호방해 공격 배터리 소진 공격 등이 있다.

2.1.1 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 소

유한 사람은 유비쿼터스 장치에 저장된 MAC 주소와 WEP 키 등 인증정보를 소유하게 되기 때문에 이러한 인증 정보들을 사용하여 어떠한 네트워크 침해로 이어질 수 있으며 공격의 일부로서 정보를 요청할 수 있다. 이것은 유비쿼터스 장치가 사용자가 아닌 장치에 대한 인증을 요구할 경우 발생한다.

2.1.2 Rogue 엑세스 포인트

대부분의 기존 인증은 공개키 암호시스템 기반으로 신뢰기관에 의해 발급된 공개키인증서를 바탕으로 인증하고자 하는 개체의 서명을 통해 이루어진다. 그러나 유비쿼터스 네트워크 환경은 고정된 망 구조가 없으며 수시로 망구조가 변경되기 때문에 망의 기반 시설이 존재하지 않는다. 따라서 네트워크 장치가 일시적으로 네트워크에 연결되며, 그 연결은 확실한 연결성을 보장하지 않는다.

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 무선LAN에 위치하면, 공격자는 액세스 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.

2.1.3 IP 스푸핑(Spoofing)

IP 스푸핑은 기밀성에 대한 위협이다. 무선 신호는 무선 신호 범위 내에 존재하는 어느 누구나 무선 접속이 가능하기 때문에 전송되는 정보가 암호화되어 있지 않을 경우 공격자가 중요 정보를 도청할 위험이 항상 존재한다.

2.1.4 DoS 공격

Dos(Denial-of-Service) 공격은 가용성을 침해한다. 유비쿼터스 네트워크 환경은 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.

2.1.5 트로이 목마, 웜, 바이러스 등

트로이목마, 웜, 바이러스 등은 가용성에 영향을 미칠 수 있고, 기밀성과 무결성도 침해를 가할 수 있다.

2.1.6 신호방해 공격

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

2.1.7 배터리 소진 공격

배터리 소진 공격은 유비쿼터스 장치의 배터리를 짧은 시간 내에 방출시켜 장치를 더 이상 사용하지 못 하게 만드는 것이다.

이러한 공격이 네트워크 보안을 침해하지는 않지만, 결국에 장치가 제대로 기능을 할 수 없게 되어 사용자가 네트워크에 접속할 수 없게 만든다.

2.1.8 신원 정보 및 위치 정보 노출

메시지에 대한 기밀성은 메시지의 내용에 대한 비밀 유지를 가능하게 한다.

3. 유비쿼터스환경 보안요구사항

3.1 기밀성

기밀성은 장치의 분실 및 도난, IP 스니퍼, 장치간의 동기화 등에 의해 침해될 수 있다. 기밀성을 유지하기 위해서는 선택할 수 있는 최선의 방법은 암호화이다. 따라서 유비쿼터스 장치의 특성에 맞는 저 전력 알고리즘이 필요하다.

유비쿼터스 컴퓨팅 장치는 모양과 크기가 다양하며, 주로 소형으로 휴대하는 장치들이 많다. 이로 인해 새로운 제약 조건이 배터리 전력의 한계를 극복하지는 못한다. 많은 연산량을 갖는 공개키 암호시스템의 사용을 최대한 줄이는 방향으로 연구가 되어지거나, 효율성이 좋은 공개키 암호 시스템 연구가 필요하다.

3.2 무결성(Integrity)

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

3.3 가용성(Availability)

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

3.4 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 불확실한 연결에 대비한 인증 솔루션이 필요하며, 연구 되어야 한다.

3.5 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 보장되어야 한다. 또한 서비스에 따라 자원을 사용하는 것에 대하여 과금할 수도 있다.

3.6 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. 사용자의 익명성을 보장할 수 있는 기술과 익명성을 선택적으로 제공받을 수 있는 방안이 함께 연구되어야 한다.

3.7 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 포괄적으로 고려하여 구현되어야 한다.

[표 1] 유비쿼터스환경 보안요구사항

보안 요구사항		추가 고려사항
기존 보안 요구 사항	인증	상호인증
		동적인 키 사용
		무선 구간 키 교환 기법 제공
		장치 독립적인 사용자 인증
		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

4. Ad hoc 네트워크 분석

4.1 Ad Hoc 네트워크 보안 요구사항

유비쿼터스 컴퓨팅이 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.

"Ad hoc" 네트워크는 기존의 네트워크와는 여러 가지의 다른 특성들이 있어서, 일반적으로 보안 메커니즘의 설계가 어려운 것으로 평가되고 있다. 예를 들어, 무선 "Ad hoc" 네트워크의 특징들은 각 노드들이 수시로 이동을 하므로 네트워크 포톨로지가 동적으로 변하게 되고, 모든 모드가 무선으로 전송을 하며 다른 노드에 독립적이며, 노드들은 한정된 배터리에 의해 동작하므로 네트워크의 각종 프로세스에 비협조적(non-cooperative)이 될 수 있다는 점등이다. 이러한 특성을 가진 "Ad hoc" 네트워크에서의 보안 요구사항은 일반 네트워크와 마찬가지로 인증 (authentication), 비밀성 (confidentiality), 무결성 (integrity), 부인방지 (non-repudiation), 접근통제 (access control) 및 가용성 (availability) 등이 무선 네트워크에서 마찬가지로 보장되어야 하는 보안 요구사항들이다. 먼저 인증은 통신을 하고자 하는 상대 노드의 신분을 확인하는 것인데, 이러한 인증이 필요한 경우에, 예를 들면 CA의 역할을 노드가 있어서 이를 확인해 주어야한다. 그러나 무선 "Ad hoc" 네트워크에서는 Infra-structure의 부재와 노드들 사이의 일시적이고 동적인 관계로 인하여 이러한 인증이 매우 힘들게 된다.

비밀성(confidentiality)은 특정 정보가 비인가자에게 누출되지 않도록 하는 것으로써, 이는 "Ad hoc" 네트워크에서 매우 중요한 요소가 될 수 있다. 예를 들어, 군사적인 목적으로 "Ad hoc" 네트워크가 사용되어 전장에 적용이 된다면, 전략적 혹은 전술적 군사기밀들에 대한 비밀은 통신 중에 철저히 유지 되어야 하며, 또한 라우팅 정보 역시 철저한 비밀이 요구되는데, 이는 그 정보가 네크워크의 구성 및 각 이동 노드의 위치를 알려줄 수 있기 때문이다. 또한, 홈 네트워크의 구축에 "Ad hoc" 네트워크가 적용되는 경우에는 개인의 사생활 정보가 외부로 유출되지 않도록 보장이 되어야 한다. 무결성 (integrity) 역시 마찬가지 관점에서 전장, 홈 네트워크, 센서 네트워크 등의 "Ad hoc" 환경에서 자료의 불법적인 변경이 불가능하도록 보장이 되어야한다. 부인방지(non-repudiation)는 데이터

의 송신자가 전송사실을 부인하지 못하도록 하는 것인데, 이는 "Ad hoc" 네트워크에서 해킹을 당한 노드를 식별하는데 다음과 같이 적용될 수 있다. 만일 노드 A가 노드 B로부터 에러가 있는 메시지를 받았는데 노드 B가 이를 보낸 사실을 부인한다면, 노드 A는 노드 B가 해킹 당한 것으로 판단하고 이 사실을 다른 이동 노드들에게 알려서 네트워크에서 분리를 시킬 수 있다.

마지막으로 가용성(availability)은 서비스 거부(DoS: Denial of Service) 공격에 대하여 네트워크의 생존성을 유지하는 것으로써, 본 논문에서 집중적으로 분석하고자 하는 무선 "Ad hoc" 네트워크의 보안 요구사항이다. 무선 네트워크에서의 DoS 공격은 다양한 계층에서 이루어질 수 있다. PHY와 MAC에서는 재밍(jamming)이나 불법적인 프레임의 송신으로 다른 이동 노드들의 통신을 방해하고, 전송률을 저하시키거나, 에너지를 고갈시킬 수 있다. 특히 무선 이동 노드들은 일정량의 배터리에 의존하기 때문에 다른 노드들의 에너지 절약 모드를 방해하거나 불필요한 전송에 의해 서버노드 및 중간 노드들의 에너지를 고갈시키는 것은 매우 큰 문제로 인식되고 있다. 네트워크 계층에서는 "Ad hoc" 라우팅 정보를 조작 혹은 변조하거나 패킷의 전달을 거부하는 등의 방법으로 네트워크 전체의 성능을 크게 저하시킬 수 있다. 상위 계층의 경우에도 응용 프로그램 등을 공격함으로써 시스템의 서비스를 마비시킬 수 있다.

4.2 RFID

RFID(Redio Frequency Identification)즉 무선 주파수 인식기술은 20세기 중반에 개발되어 1990년 대말에 재고 관리 및 공급 체인 관리 등에서 사용됨으로써 두각을 드러낸 기술이다. RFID는 앞에서 언급 한데로 무선 주파수 인식 기술을 말하는 것이다. RFID는 주파수를 이용하여 개별 상품을 식별하는 방식을 일컫는다. RFID와 바코드를 비교하여 보면 바코드의 경우 레이저 판독기를 바코드에 직접 접촉시켜야 하지만 RFID는 안테나와 테그만 있으면 판독기를 직접 접촉하지 않아도 쉽게 상품의 정보를 식별할 수 있으며 필요한 정보를 삽입할 수도 있다.

RFID 구성 요소는 데이터를 저장할 수 있는 RFID TAG와 RFID에 있는 데이터를 읽을 수 있는 Reader 그리고 중간에서 데이터를 트랜스퍼하는 안테나 등으로 구성되어 있다.

RFID의 상업적으로 많이 이용되어 지금은 산업 전반에서 공급 체인의 투명성과 효율성을 높이고 있다고 한다. 미국 월마트가 RFID 기술을 접목시키는 프로젝트를 파일럿 형태로 100개의 Supplier 와 추진 중이며, 2005년 1월 달에 가시화할 것으로 보인다. 그리고 DHL은 화물 추적 조회를 위해서 전 세계를 대상으로 RFID 시스템을 곧 운영할 계획이라고 한다. 싱가폴을 포함한 여러 곳에서 공공 도서관의 도서 대출 및 도난 방지에 이 기술이 사용되고 있다고 한다.

유비쿼터스를 실현시키는 핵심이 바로 RFID이다. 과거에는 시스템이 개별적인 실체를 인식할 수 없었지만 이제 RFID를 통해 모든 실체들이 무선 네트워크 상에서 인식될 수 있는 존재가 된 것이다. 공급 체인에 있는 모든 품목의 개별적 식별이 가능해짐으로써 공급체인의 효율은 증가하며, 완벽한 유통이 실현되는 것이다. 시스템은 상품을 자동으로 인식하여 그 처리를 하게 된다. 시스템은 사람의 개입 없이 상품을 모니터링하고 판단하고 필요한 조치를 취할 수 있도록 상품 정보를 신속히 검색한다. 그렇게 됨으로써 시스템의 재고와 실제 재고가 일치되고, 거래업체와의 상품 인수인계가 자동화된다. 수많은 점포에 대해 재고관리, 판매, 보충, 도난방지 등 모든 업무가 일괄 관리제어되며, 상품 보충 및 생산 주문이 자동화될 것이다. 판매 계산대로부터 원자재 구매에 이르는 공급체인 업무 전체가 통합된 수요 주도의 네트워크 체제로 형성될 것이다.

4. 결 론

본 논문에서는 유비쿼터스 네트워크 기반이 전개되기 전에 유비쿼터스의 시큐리티 문제를 연구해 보았다. 유비쿼터스와 시큐리티 고려사항, 유비쿼터스와 시큐리티 서비스인 인증, 무결성, 기밀성, 가용성 등에 관하여 기존의 발표된 자료를 중심으로 연구하였다. 특히, 유비쿼터스 네트워크 환경은 기존의 네트워크 환경보다 정보 접근 범위나, 방법 및 피해 규모도 광대하여 지금까지의 취약점 보다 더 많은 취약점을 예상할 수 있었으며, 온라인 서버 가정이 곤란한 유비쿼터스 컴퓨팅 환경에서의 인증, 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 Twe ntity First Century", Scientific Ameri-can, 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] 이승형, 홍순좌, 최현준, "무선"Ad hoc" 네트워크에서 서비스 거부 공격의 위험성 분석", 제15회 정보보호와 암호에 대한 학술대회(WSC2003), pp.660-669, 2003.

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

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

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

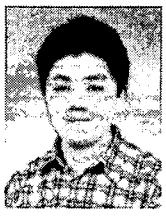
정 상 일

2004년 ~ 현재 안동과학대학 사이버테러대응학과 재학

송 원 덕

2004년 ~ 현재 안동과학대학 사이버테러대응학과 재학

이 원 찬



2004년 ~ 현재 안동과학대학 사이버테러대응학과 재학

윤 동 식

1992년 관동대학교 전자계산학과(공학사)
1994년 관동대학교 컴퓨터공학과(공학석사)
2000년 관동대학교 컴퓨터공학부(공학박사)
1999년 ~ 현재 안동과학대학 사이버테러대응학과 교수