유비쿼터스 환경의 인증 및 권한 메커니즘 동향을 통한 분산 인증기법 방안 연구*

오동열** · 성경상*** · 김배현**** · 오해석***

요 약

사용자가 접하는 정보 시스템과 어플리케이션에 대한 관리가 중요한 문제로 대두되면서 시스템 접근과 관리를 위한 방법론이 제기되고 있다. 여러 가지 형태의 인증 기술이 사용되고 있지만, 복잡한 인증 관리 및 운용에 따른 비효율성은 유·무선 환경의 다양하고 새로운 비즈니스의 성공적인 전개를 위해서는 부적절하다. 또한 서로 다른 인증 방식을 사용하는 모바일 컴퓨팅 환경 하에서 유연하고 연속적인 서비스를 기대하기란 매우 어렵다. 유비쿼터스 컴퓨팅 환경하에서는 상호운용성 및 보안성이 지원되는 분산 인증 방안을 연구·개발하는 것은 매우 중요한 사안이다. 이에 따라 본 논문에서는 유선(fixed) 컴퓨팅 환경에서뿐만 아니라 이동(mobile) 컴퓨팅 환경까지 고려한 유비쿼터스 컴퓨팅 환경으로 확장 가능한 분산 인증의 관리 및 운용 방안에 대한 요구사항과 권한 메커니즘에 대해 살펴봄으로써, 향후 진정한 유비쿼터스 환경에서의 분산형 인증기법에 관한 적극적인 참여를 유도할 수 있을 것으로 기대한다.

A Study on the Distribute Authentication Method Scheme through Authentication and Right Mechanism Trend of the Ubiquitous Environment

Dong-Yeol Oh** · Kyung-Sang Sung*** · Baehyun Kim**** · Hae-Seok Oh***

ABSTRACT

While an information system and administration for an application that a user contacts with raise a head by an important problem, a system approach and methodology for administration are mentioned. Authentication technology of various configuration is used, but non-efficiency by complicated authentication administration and operation inappropriate use are for a successful expansion of various and new business of wire/wireless environment. In addition, under the mobile computer environment with different authentic method each other, it is difficult at all to expect flexible and continuous service. Under the ubiquitous computing environment, It is very important thing plan to research and develop compatibility and the side of variance authentication plan that preservation characteristics are helped. Hereby, This paper look around an requirement items and authority mechanism for the administration and the operation mechanism of the distributed authentication considering expansion possibility of the ubiquitous computing environment not only fixed computing environment but also mobile computing. In future, we expect it by can guide positive participation about distributed authentication technique of the genuine ubiquitous environment.

Key words : Mobile Computing, Distribute Authentication Management, Right Mechanism, Compatibility

---

* 본 연구는 2005년도 경원대학교 지원에 의한 결과임.

** 숭실대학교 컴퓨터학과
*** 경원대학교 전자계산학과
**** 호원대학교 사이버수사경찰학부

1. 서 론

본격적인 정보화 시대로 접어들면서 사용자가 접하는 정보 시스템의 수가 급격히 증가하였으며, 서비스 유형에 따라 자원의 접근 권한 제어 기능뿐만 아니라 디바이스를 사용하는 사용자의 신원 확인을 위한 인증기능도 요구된다. 이에 따라 사용자가 이용하는 정보 시스템과 어플리케이션에 대한 관리가 중요한 문제로 대두되고 있다. 그러나 여전히 많은 문제점들이 도래하고 있다. 수많은 컴퓨터들이 유무선 네트워크 환경에서 유기적으로 연결되어 있으나, 비효율적인 인증 관리 및 운용 플랫폼이 마련되지 않다면 새로운 비즈니스 환경에서의 적용 방안은 기대하기가 어려워진다. 이러한 문제를 해결하기 위한 여러 형태의 인증 기술이 사용되고 있지만, 복잡한 인증 관리 및 운용에 따른 비효율성은, 유·무선 환경의 다양하고 새로운 비즈니스의 성공적인 전개를 위해서는 부적절하다. 또한 서로 다른 인증 방식을 사용하는 모바일 컴퓨팅 환경 하에서 유연하고 연속적인 서비스를 기대하기가 어렵다. 따라서, 유비쿼터스 컴퓨팅환경을 고려할 때 상호운용성 및 보안성이 지원되는 분산 인증 방안을 연구·개발하는 것은 매우 중요한 사안이다. 특히, 유비쿼터스 환경과 같이 개체마다 많은 정보를 갖고 있으며, 이에 대한 정보를 어떻게 보호할 것이며, 어떠한 방법으로 서비스를 안전하게 제공할 것인지에 대한 연구가 반드시 요구된다. 그러나 최근의 보안에 대한 연구는 단순한 개체의 인증을 통한 연구만이 이루어지고 있는 실정으로, 실제 유비쿼터스 환경이 구현되었을 때 나타날 수 있는 다양한 형태의 보안 연구가 미흡한 실정이다. 따라서 다양한 보안 요구사항과 이를 만족하는 보안 프로토콜 개발은 안전한 유비쿼터스 환경에 매우 절실히 요구되는 사항이다. 유비쿼터스 컴퓨팅 환경은 네트워크를 기반으로 한 장치간의 연결을 기본으로 하고 있다. 특히 무선중심의 근거리 통신기술이 발달함에 따라 유비쿼터스 컴퓨팅 환경을 이루는 무수히 많은 개체들은 유기적으로 연결되어 서로 데이터를, 주고받고, 이를 통해 서비스를 제공하게 된다. 이러한 개체간의 연결은 보안 취약점을 발생시키고 있으며, 이에 따른 정보보호 관점의 보안 요구사항이 도출될 수 있다.

본 논문에서는 이러한 유비쿼터스 컴퓨팅 환경 내에서 발생할 수 있는 보안 취약점과 보안 요구사항을 도출하고자 한다. 또한, 도출된 보안 요구사항은 유비쿼터스 컴퓨팅의 핵심기반기술인 무선 네트워크 기술을 기반으로 인증기술에 대한 서비스 방향의 구체화를 통해 환경적 모델을 제언하고자 한다. 본 논문을 통해 향후 진정한 유비쿼터스 환경에서의 분산형 인증기법에 관한 적극적인 참여를 유도할 수 있을 것으로 기대한다. 본 논문의 구성은 다음과 같다.

제 2장에서는 보안 및 인증 요구사항에 대해 살펴본 후, 제 3장에서는 유비쿼터스 컴퓨팅 환경에서의 인증 및 권한 메커니즘에 대해 살펴본다. 제 4장을 통해서는 보안 및 인증 기술에 대한 동향을 살펴본 후 분산 인증 모델에서의 적용 가능한 방법론에 대해 제언하고, 마지막으로 제 5장에서는 결론 및 향후 연구 방향에 대해 설명한다.

2. 보안 및 인증 요구사항

2.1 유비쿼터스 환경의 보안 위협사항

유비쿼터스 컴퓨팅 환경은 기존의 연구 분야인 무선 인터넷, 무선랜, 블루투스, 홈네트워크 등의 분야를 통합하는 환경이라 할 수 있다. 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 시스템으로 동작할 수도 있다. 이러한 문제는 실제 유비쿼터스 컴퓨팅이

현실화되는데 있어서 가장 큰 걸림돌로 작용할 수 있다. 무선랜의 경우 단 방향 인증만을 제공한다. 즉, 하나의 액세스 포인트가 한 사람의 사용자를 인증하지만, 사용자는 액세스 포인트를 인증하지도 인증할 수도 없다. 따라서 공격자는 액세스 포인트에 대한 인증없이 네트워크 접근이 가능하게 되고, 그것은 정식 사용자의 클라이언트에 대한 하이재킹(Hijacking)을 통해 서비스 거부 공격의 거점이 될 수 있다. 비밀성에 대한 위협으로는 IP 스푸핑이 대표적인 보안 위협사항으로, 무선 신호 범위 내에 존재하는 어느 누구나 무선 접속이 가능하기 때문에 전송되는 중요 정보가 도청될 위험이 항상 존재한다. 또한 각종 바이러스로 인한 비밀성과 무결성도 침해될 수 있다. 다음으로는 가장 화두가 되고 있는 가용성 침해의 대표적인 DoS 공격과 신호 방해 공격을 들 수 있다. 유비쿼터스 네트워크 환경은 앞서 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 DoS공격으로 이루어진다. 이러한 문제는 배터리 소진 공격으로 이어질 수 있으며, 장치의 제 기능을 마비시키는 것으로 이어질 수 있다.

2.2 유비쿼터스 환경의 보안 요구사항

유비쿼터스 컴퓨팅 보안의 목적은 인가되지 않은 사용자가 공유된 정보에 불법적으로 접근하거나, 사용자 공유 정보를 노출 및 변경하지 못하도록 하는 것이다. 이를 위해서 고려되어야 할 보안의 요건은 인증(authentication), 비밀성(confidentiality), 무결성(integrity) 외에도 가용성(availability), 권한관리, 부인방지, 익명성, 안전한 핸드오프 등의 보안 요구사항이 제공되어야 한다.

유비쿼터스 컴퓨팅에서는 일시적이고 불확실한 연결을 제공하므로 인증을 위한 연결과정에서 합법적이지 않은 사용자에 대한 인증이 발생할 수 있다. 따라서 인증을 보장하기 위한 상호인증과 동적 키 사용, 무선 구간 키 교환 기법 그리고 장치 독립적인 사용자 인증과 같은 기능들이 요구된다. 유비쿼터스 네트워크에서는 어떤 개체가 일시적 접속을 위한 인증 서비스 요구가 필요하게 될 것이며, 보안 사항과 관련된 어떤 협약(association)을 설정하는 절차와 비밀성이 고려되어야 할 것이다. 이를 위해 트래픽 데이터 암호화와 키 관리 기법 제공과 정보의 암호화 그리고 효율성이 좋은 공개키 암호 시스템과 같은 “저 전력 암호 알고리즘” 연구가 필요하다. 또한 유비쿼터스 컴퓨팅에서 가장 심각한 무결성 문제는 이동 중인 메시지의 무결성이 아니라, 유비쿼터스 장치 자체에 대한 “객체 무결성”이다.

마지막으로, 안전한 핸드오프는 사용자 인증, 키 관리정책, 암호화 알고리즘 협상, 그리고 과금 정책을 포괄적으로 고려하여 구현되어야 한다. 동일한 서브넷에 위치한 액세스 포인트 사이를 이동할 때 핸드오프 보안이 제공되어야 하고, 핸드오프 과정에서 보안 접속 유지와 보안 컨텍스트 정의 및 관리 등을 고려해야한다.

위에서 언급한 보안 요구사항들은 하나의 서비스를 위해 반드시 갖춰져야 하는 것은 아니라, 서비스목적에 맞는 보안 요구조건을 새롭게 정의하며 구현해야 할 것이다.

3. 유비쿼터스 컴퓨팅 환경에서 인증 및 권한 메커니즘

유비쿼터스 환경에서 사용자가 원하는 결과를 얻기 위한 과정에는 인증 및 권한이 요구된다[10]. 제 3장을 통해 이러한 요구에 대해 알아보고, 그 요구를 충족할 수 있는 인증 및 권한 메커니즘을 제언한다.

3.1 정보보호와 인증 및 권한

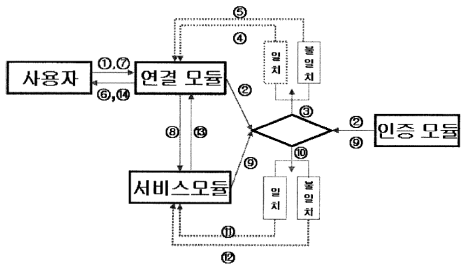
각종 정보매체나 인터넷을 통한 정보 노출로 인권 침해 및 범죄의 활용 가능성에 매우 쉽게 허용되고 있다. 사용자에게 실시간으로 서비스를 제공하는 유비쿼터스 환경에서는 이러한 현상이 더욱 심해질 것이라고 예측할 수 있다. 현행에서 침해되고 있는 유형을 분류해보고, 유비쿼터스 환경에서는 어떻게 침해될 수 있는지 알아보고, 그에 대한 대책 마련을 해야 할 것이다[13].

정보주체의 동의 없는 개인정보의 노출로 인해 정보주체가 인식할 수 없는 상황에서 자기정보 통제권을 상실할 가능성이 크다. 또한 부적절하게 수집된 정보 및 분석을 통해 개인에 대한 통제행위가 심화될 것이며, 이로 인한 개인의 라이프스타일 등 개인의 생활 전반이 노출될 것이다.

유비쿼터스 컴퓨팅 환경에서는 모든 사물에 전자 태그가 부착되고, 정보에 대해 직·간접적으로 얻을 수 있고, 사물을 제어할 수 있는 가능성을 제공해 줄 수 있다. 이러한 이유로 유비쿼터스 컴퓨팅 환경에서는 위에서 언급된 개인정보보호뿐만 아니라, 개인, 집단등과 관련된 사물의 정보보호측면을 확장하여 고려해야 할 것이다.

3.2 일반적인 인증 및 권한 메커니즘 방식

위에서 언급한 것과 같은 이유로 유비쿼터스 컴퓨팅환경에서 정보보호의 필요성이 요구되고, 이런 요구를 해결하기위한 여러 방안이 연구되고 있으며[2, 8], (그림 1)과 같은 사용자의 인증 및 권한, 서비스 이용 등급 메커니즘이 일반화되고 있다. 사용자의 서비스 이용 범위에 따라 여러 그룹으로 분류되며, 각 그룹은 취급 정보의 중요성에 따라 다른 서비스 이용 등급을 부여 받는다. 서비스는 개인정보 취득, 사물 정보 취득, 사물 제어 등 유비쿼터스 컴퓨팅환경 내에서 원하는 결과를 얻기 위해 처리 되는 모든 행위를 의미한다.



(그림 1) 인증 및 권한 메커니즘

(그림 1)은 사용자와 서비스 간의 연결과 처리에 대한 인증 및 권한 메커니즘의 단순화된 작동 시나리오를 보이며 설명은 다음과 같다.

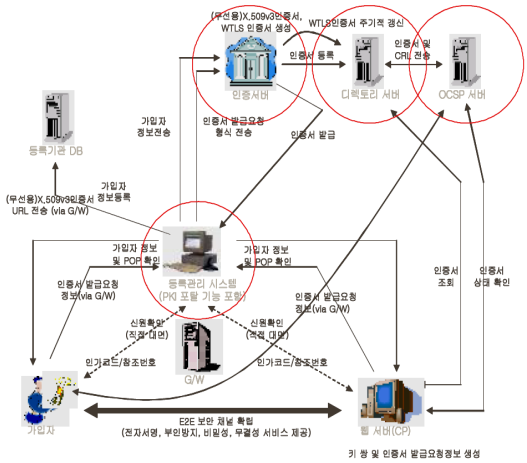
서비스 제공은 등록된 사용자에 맞게 제공되며, 시스템 사용자는 인증 모듈로부터 인증절차를 받아야 한다. 인증 모듈에서는 그에 따른 적절한 등급을 설정하여 키 값을 생성하게 된다. 적법한 절차를 거친 인증된 사용자는 필요한 서비스를 연결 모듈를 통해 사용자가 요청한 서비스를 서비스 모듈로 요청하는 절차를 거친다. 서비스 모듈은 요청한 서비스가 적법한지 여부를 인증 모듈을 통해 확인한 후, 그에 따라 서비스 제공 여부를 결정한다.

4. 보안 및 인증 기술연구

4.1 무선PKI 기술

무선환경의 특성상 정보노출이 용이하고 제한된 자원을 사용해야 하므로 기밀성, 무결성, 인증, 부인봉쇄와 같은 서비스를 제공하기 위한 무선 PKI 기술의 개발과 규격화가 필요하다. 무선 PKI란 기존의 유선 PKI의 구성요소를 그대로 이용하며, 무선환경에 적합하도록 기능을 최소한 변화시킨 것이다. 무선 PKI를 구축할 경우에는 유선과는 달리 클라이언트(무선 단말기)와 서버간의 제한된 대역폭, 클라이언트의 처리능력, 클라이언트의 제한된 메모리를 고려해야한다. 또한 기존 유

선환경과는 달리 인증서 검증 메커니즘의 경량화가 필요하다.

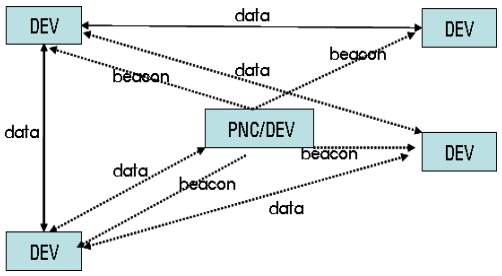


(그림 2) 무선 PKI 기술 컴퍼넌트

(그림 2)는 무선 PKI 기반의 구조를 나타낸 것으로 PDA, Mobile Phone 등의 이동 Device 기반의 통신 수단을 기반으로 "무선 WTLS 인증서 프로파일 규격"에서 제시하고 있는 인증서 형식을 따른다. CP와 통신상 발생하는 보안취약성을 극복하기 위해 End to End Security를 지원하여야 하며, 암호화 알고리즘(ECC 등)에 대한 코드 및 성능 최적화를 기반으로 해야 한다.

4.2 IEEE 802.15.3 WPAN 보안

IEEE 802.15.3 WPAN의 보안 메커니즘은 PNC (Piconet Coordinator)와 DEV 사이, DEV들 간의 보안 관련성을 바탕으로 데이터에 대한 암호화를 지원하지만, 장치인증과 같은 절차는 지원하지 않는다. 데이터 프레임, Command, Beacon을 보호하기 위해 128-Bit AES방식의 대칭키 암호화 알고리즘을 사용한다. 이때 DEV에게서 다른 DEV로 전송되는 모든 키는 KeyRequest와 Distribute Key Protocol에 의한 방법으로 전송된다.

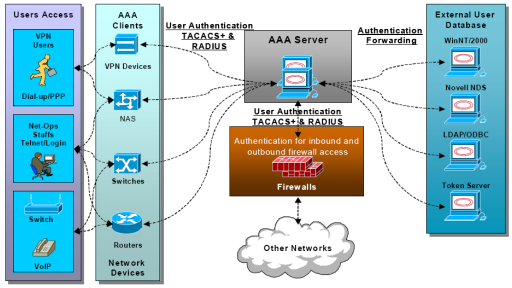


(그림 3) IEEE 802.15.3 WPAN 보안

(그림 3)은 DEV/PNC간 data와 beacon의 관계성을 도식화한 것이다. 데이터, Beacon, Command에 대한 무결성(Integrity) 검사는 알맞은 키에 의해 이루어진다. Beacon에 대한 무결성 검사가 실패하면, DEV와 PNC는 동기화된 보안 상태를 가지지 못한다. 그러므로 Beacon내에는 Strictly-Increasing Time Token을 포함하여 한번 사용된 메시지가 재사용되는 것을 막는다. 또한 DEV는 Token 값을 사용하여 메시지 보호뿐만 아니라 beacon의 보안이 훼손되지 않았음을 보장한다.

4.3 AAA 기술

통신 사업자들은 단순히 모뎀 포트를 제공하는 것에서 그치는 것이 아니라 불법적 서비스 사용을 방지하고(Authentication), 가입자의 권한레벨을 부여하고 검증하며(Authorization), 과금(Accounting) 및 자원 계획을 수립하기 위해 네트워크 사용에 대한 측정이 필요하다. AAA는 이러한 요구사항을



(그림 4) AAA Service 구조

만족시키는 보안 기술 규격이며[9], (그림 4)는 일반적인 AAA service 구조를 나타낸 것이다.

현재까지는 서버 프로토콜의 표준으로 AAA RADIUS와 TACACS+가 주로 사용되어 왔으나, 이러한 프로토콜들은 단지 서버 기반의 인증이 필요한 소수 가입자들을 지원하는 소규모 망 장치를 위한 프로토콜에 불구하다. 따라서, 이러한 문제점을 해결하기 위한 방안으로 현재 AAA WG에서 표준화하고 있는 프로토콜은 Diameter로서, 기존 프로토콜의 한계점 극복, 로밍에 필요한 도메인 간 이동성 지원, 강화된 보안 제공, 보안 및 신뢰성을 기반으로 하는 하부 프로토콜 수용, 미래 서비스를 수용할 수 있는 유용한 확장성 등을 특징으로 하고 있다. 인터넷 프로토콜인 Diameter는 현재의 키워드가 되고 있는 유무선 인터넷 통합에 적용될 그리고, 4세대 이동통신 시스템에도 적용될 주요 기술 중의 하나로 발전될 것이라 판단된다.

4.4 센서 네트워크 보안기술

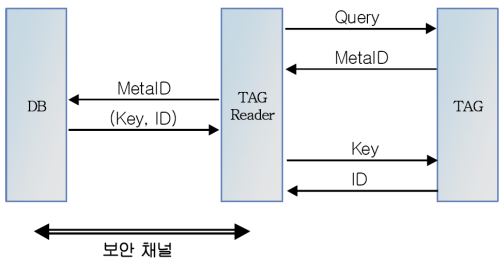
센서 네트워크 기반의 서비스에 대한 기술이 구체화되어지면서 센서 네트워크상에서 보안에 대한 필요성과 기술에 대한 연구가 활발해지고 있다[10]. 일반적으로 센서 네트워크를 위해 운영되어지는 센서 노드는 안전하지 않은 위치에 설치되어지므로, 각 노드에 대한 신뢰성을 보장 받을 수 없다. 그러므로 한 노드의 보안 노출이 다른 노드에 영향력을 미치지 않도록 보안 사고의 최소화가 절대적으로 필요하다. 즉, 각 노드에게 broadcasting 하는 것은 안전하지 않은 무선망에서 공격자(Adversary)의 도청이 언제든지 가능하며 메시지의 재사용 공격에 매우 취약할 수 있기 때문이다.

센서 네트워크 보안 요구사항으로는 데이터에 대한 비밀성, 인증성, 무결성 그리고 신선성 등을 언급할 수 있다. 센서 네트워크 환경의 많은 응용에서는 민감한 데이터 교류가 노드 간에 빈번하게 이루어므로, 비밀 키로 데이터를 암호화한 상태에서 데이터 교류가 이루어져야 한다. 즉 데이터의 비밀성을 보장해야 한다. 또한 메시지 위·변조에 따른 진위를 검증하기 위한 인증은 센서 네트워크에서 중요한 보안 요구사항으며, 수신한 데이터의 위·변조 여부를 확인하는 것으로 SPINS에서는 데이터 인증을 통한 데이터 무결성을 보장한다. 그리고 데이터에 대한 재 사용을 방지하기 위한 기술로서 가장 최근에 보낸 데이터임을 보장하는 보안 서비스 요소로서 데이터 신선성(Freshness)을 언급한다[7].

4.5 RFID 보안기술

RFID 기술은 장소와 시간에 제약없이 언제나 최상의 서비스를 제공하기 위한 유비쿼터스의 목적을 쉽게 이룰 수 있는 기술로 현재 주목을 받고 있다. 그러나 RFID를 위한 컴퓨팅 환경은 일반적인 인터넷 환경과는 달리 많은 제약적 사항을 갖는다. 따라서 보안 기술 적용에 대한 부분에 있어서 운영·환경 측면을 충분히 고려해야한다[8]. 현재 RFID의 환경적 제약에 적합한 최적의 보안 기술이 연구되고 있으나, 아직은 기술적 표준화가 이루어지지 않았다.

현재의 RFID Tag는 일반적인 접근 통제나 인증 메커니즘을 적용하기 위한 컴퓨팅 자원에 대한 제약이 존재함으로 Hash Lock 메커니즘을 통한 인증과 접근통제 보안 서비스에 적합한 모델이 제안되고 있다. (그림 5)는 Hash Lock 메커니즘을 보여준다.



(그림 5) Hash Locked Tag 메커니즘

Hash Lock 스킴에서 Tag는 Hash 메커니즘을 처리할 수 있는 H/W 기반의 암호화 모듈로서 보안적 요구사항을 처리할 수 있다. Tag에는 MetaId 정보만을 보관할 수 있는 저장 공간을 보유하고 있어야 하며, Tag Reader 장비와의 운영이 불가능케 하는 Lock과 장비 운영이 가능케하는 Unlock 처리 기능만을 동작하면 된다. Hash Lock 메커니즘은 단순 해쉬 알고리즘과 Key 보관의 안전성만 보장되어지면 쉽게 적용할 수 있다.

6. 결 론

서로 다른 인증 방식을 사용하는 컴퓨팅 환경하에서는 유연하고 연속적인 서비스뿐만 아니라 사용자에게는 비효율적인 결과를 초래한다. 결국 유비쿼터스 컴퓨팅 환경 하에서는 상호운용성 및 보안성이 지원되는 분산 인증 방안의 연구는 매우 중요한 사안이다. 따라서 본 논문에서는 유선(fixed) 컴퓨팅 환경에서뿐만 아니라 이동(mobile) 컴퓨팅 환경까지 고려한 유비쿼터스 컴퓨팅 환경으로의 확장 가능한 분산 인증 관리 및 운용 방안에 대한 모델을 도출할수 있는 기반 마련을 위한 연구를 주 목적으로 한다.

본 논문을 통해 유무선 네크워크 환경간의 인증 연동 기술을 개발할 수 있는 기반을 마련하며, 유비쿼터스 컴퓨팅 환경의 인증 모델 연구에 대한 활발한 참여를 유도할 수 있고 다른 선진국들과 경쟁을 할 수 있으며, 더 나아가 분산 인증 관리 기술 분야에서 우위를 선점할 수 있을 것으로 기대한다. 그리고 서비스 제공자와 망 사업자에게 분산 인증 관리 기술의 필요성과 사업성을 이해시킴으로써 유비쿼터스 컴퓨팅 환경에 적합한 다양한 분산 인증 기술을 연구 및 개발하기 위한 적극적인 참여를 유도할 것으로 기대한다.

참 고 문 헌

[1] J. Deng, R. Han and S. Mishra, “The Performance Evaluation of Intrusion Tolerant Routing in Wireless Seosor Networks”, In Proc. of IEEE 2nd International Workshop on information Processing in Sensor Networks(IPSN 2003), LNCS

[2] C. Karlog and D. Wagner, “Secure Routing in Wireless First IEEE International Workshop on Sensor Networks and Application(WSNA 2003), San Diego, CA, Sep, 2003.

[3] D. Liu and P. Ning, “Efficient Distribution of Key Chain Commitments for Broadcast Authentication in Network and Distributed System Security Symposium. San Diego”, California. Feb. 2003.

[4] H. Han, A. Perrig, D. Song, “Random Key Predistribution Schemes for Sensor Networks”, Appears in IEEE Symposium on Security and Privacy 2003.

[5] L. Eschenauer, V.D. Gigor, “A Key Management Scheme for Distributed Sensor Networks”, Conference on Computer and Communications Security, CCS 2002, Washington DC, USA, Nov, 2002.

[6] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Cullar, K. Pister, “System architecture directions for network sensors”, ASPLOS 2000, Cambridge, Nov 2002.

[7] Y, J, Zhao, R. Govindan, and D. Estrin, “Computing Aggregates for monitoring Wireless Sensor Networks”, The First IEEE International Workshop on Sensor Network Protocols and Applications (SNPA 2003), Anchorage, AK, USA, May Vol. 11, 2003.

[8] Security and Privacy Aspects of Low Cost Radio Frequency Identification System, First Intern. Conference on Security in Pervasive Computing, 2003, Weis S. et.
[9] Diameter Base Protocol, RFC 3588, www.ietf.org/html.charters/aaa-charter.html.
[10] 조명섭 외, "유비쿼터스 컴퓨팅과 보안요구사항 분석", 한국정보보호학회지, 제14권, 제1호, pp. 22-29, 2004.
[11] 이승종외, "유비쿼터스에 이용하는 무선기술", 한국정보처리학회 추계학술발표대회 논문집, 제10권, 제2호, 2003.
[12] 주학수, "암호인증기술 이슈 리포트-유비쿼터스환경에서 보안 및 프라이버시 관련 프로젝트 현황", 한국정보보호진흥원 전자거래보호단 암호인증기술팀 2004.
[13] 김태중, "RFID 프라이버시 보호 추진 동향 분석", 한국정보보호진흥원 개인정보보호팀/암호인증기술팀 2004.
[14] 양대헌 외 4인, "차세대 컴퓨팅 환경에서 디바이스 인증을 위한 PKI 적용기술 연구", 한국정보보호진흥원, 2003.

오 동 열

1999년 경희대학교 전자계산학과 졸업
2002년 숭실대학교 컴퓨터학과 석사
2004년 숭실대학교 컴퓨터학과 박사 수료
2007년~현재 인젠트(주) 연구개발 본부 차장
관심분야 : 유비쿼터스 컴퓨팅, P2P, 멀티미디어

성 경 상

2001년 호원대학교 전자계산학과 졸업(학사)
2003년 숭실대학교 대학원 컴퓨터학과 졸업(석사)
2004년 현재 경원대학교 대학원 컴퓨터학과 박사과정
관심분야 : 전자거래학, 유비쿼터스, 보안

김 배 현

1995년 호원대학교 전자계산학과 졸업
1997년 수원대학교 전자계산학과 석사
2003년 경희대학교 컴퓨터공학과 박사수료
2004년~2007년 한신대학교 정보통신학과 겸임교수
2007년~현재 호원대학교 사이버수사경찰학부 연구교수

오 해 석

서울대학교 대학원 전자계산학 졸업(석사, 박사)
미국 스탠퍼드대학교 객원 교수
한국 정보처리학회 회장(역임)
1982년~2003년 숭실대학교 컴퓨터학부 교수/부총장(역임)
2003년~현재 경원대학교 소프트웨어대학 교수
관심분야 : Multimedia, Database, 지식경영