근거리 무선 통신의 안전한 보안 모니터링 기법

서 대 희† · 이 임 영††

요 약

무선 정보 환경의 변화에 따라 다양한 정보에 대한 풍족감이 요구되고 이에 따라 많은 근거리 무선 통신 기술들이 연구 개발되어 왔으며, 그 중에서도 최근 근거리 무선 통신의 표준으로 각광받고 있는 블루투스와 무선랜은 많은 관심을 받고 있다. 그러나 근거리 무선 통신을 실제 무선 환경에 적용하기엔 많은 문제점들이 제기되고 있다. 따라서 본 논문에서는 현재 근거리 무선 통신의 보안적 취약점 뿐만 아니라 무선 환경이라는 특수한 환경에서 보안적 사항과 사용자의 프라이버시와 밀접한 관계가 있는 비보안적인 사항까지 고려한 일반화된 중앙 집중형 보안 모니터링 기법을 제안한다. 또한 제안된 방식을 근거리 무선 통신의 대표적인 기술인 블루투스와 무선랜에 적용시켜 사용자 중심으로 흩어져 있는 모바일 디바이스에 대한 안전한 보안 모니터링 기법을 제안한다.

A Secure Monitoring Mechanism for Short Distance Wireless Communication

Dae-Hee Seo† · Im-Yeong Lee††

ABSTRACT

In accordance with the changes in the wireless communication environment, there has been a great need to satisfy the demand for diverse modes of information exchange. Various types of short-distance wireless communication technology have been developed and studied to meet this demand. Among them, Bluetooth and WLAN which has recently been acclaimed as the standard for short-distance wireless communication, has been the focus of many such studies. However, Bluetooth and WLAN has weaknesses in its security features when its in real services are applied to m-commerce. The purpose of this study is to propose techniques that affinity considers to item that is non-security enemy who is although there is no public secure division direct connection in peculiar environment of radio environment as well as limitation security enemy of short distance radio communication. Propose secure monitoring techniques for straggling device to user center also applying proposed way to Bluetooth and WLAN that are short distance communication representative technology based on item that is security enemy and item that is rain security enemy.

키워드 : 근거리 무선통신(Wireless Communication), 블루투스(Bluetooth), 무선랜(WLAN), 보안 모니터링(Secure Monitoring)

1. 서 론

최근 유동성 디바이스가 많이 사용되고 있으며 각 장비의 계층 사이에 통신 채널에 대한 연구들이 진행되고 있다. 이러한 연구들은 모든 유동성 디바이스가 일정한 장소에 놓여질 수도 있으며 그렇지 않을 수도 있는 한계를 극복하고 서로의 디바이스들이 통신할 수 있는 무선 환경의 인터페이스에 대한 고려로부터 시작되었으며 이러한 기술이 근거리 무선통신 기술이다[1, 2].

근거리 무선 통신의 특성상 사용자 중심으로 흩어져 있는 모바일 디바이스에 대한 통신을 위한 기술로서 최근 많은 연구가 진행되고 있으며 국내에서는 2001년 무선국에서 블루투스와 무선랜을 국내 근거리 무선 통신 기술의 표준으로 제정하기 위한 많은 연구가 진행되어가고 있다. 그러나 근거리 무선 통신 기술의 특성상 사용자의 프라이버와 매우 밀접한 관계가 있어 실제 적용하기엔 많은 취약점들이 문제시되고 있다. 최근 근거리 무선 통신과 연관된 보안에 관한 연구는 보안 서비스에 그 초점이 맞추어져 있어 보안 서비스에 포함되지는 않지만 보안 서비스와 직접적인 영향이 있는 비보안적인 사항까지 고려되는 연구는 매우 미흡한 실정이다.

따라서 본 논문은 2장에서 근거리 무선통신의 일반적인 개요를 살펴보고 3장에서는 근거리 무선 통신 기술의 대표적인 블루투스와 무선랜에 대한 분석을 한 뒤 4장에서는 새로운 제안 방식들을 제안하고 5장에서는 제안 방식을 분석한 후 마지막으로 6장에서는 결론을 맺도록 한다.

† 준 회 원 : 순천향대학교 전산학과
†† 종신회원 : 순천향대학교 정보기술공학부 교수
논문접수 : 2002년 9월 19일, 심사완료 : 2002년 12월 24일

2. 무선 PKI와 근거리 무선 통신 개요

무선 통신에 대한 많은 연구가 진행되고 있는 가운데 국내에서도 이에 대한 연구가 활발히 진행되고 있으며 최근 무선 PKI와 블루투스, 무선랜으로 대표되는 근거리 무선 통신 기술을 국내 표준으로 정착시키기 위한 노력이 계속되고 있다. 따라서 본 장에서는 무선 PKI와 블루투스, 무선랜에 대한 일반적인 개요에 대해 살펴보고자 한다.

2.1 무선 PKI

현재 국내에서는 기존에 구축된 전자사명법에 기반을 두고 있는 전자서명인증 관리체계가 존재하며, 공인인증 기관을 중심으로 사용자에게 금융서비스, 전자결제 서비스, 전자상거래 서비스 등을 제공하고 있다. 그러나 무선 인터넷 환경에서 사용하기에는 시스템이 무겁고 여러 가지 제약점을 가지고 있다(단말기 화면 제한, 네트워크 대역폭 제한, CPU 처리 속도 제한, 메모리 제한, 입력장치 제한 등). 무선 인터넷 환경에서는 이러한 제약점을 고려한 기술 개발이 필요하였으며 이를 이해 무선 PKI 기술 규격을 만들게 되었다. 다음은 무선 환경에서 여러 가지 제약사항들로 인해 무선 인증 시스템이 유선인증 시스템과 구별되어지는 차이점들을 살펴보았다. 첫 번째, 인증 시스템이 핵심인 공개키 암호 알고리즘으로 대표되는 RSA 알고리즘은 안전성에 비해 상당한 연산량을 요구한다. 특히 키 쌍 생성(공개키, 개인키 쌍)시에는 현재 핸드폰에서 사용하고 있는 MSM 3100 또는 MSM 5000 칩에서는 10분 이상의 시간이 소요됨으로 인해 서비스가 불가하다. 그러나 향후 이동 단말기의 성능 향상과 유무선 통합을 고려하여 RSA 공개키 알고리즘도 규격안에 포함시켰다. 현재의 기술로 구현 가능하도록 하기 위해 유선에서는 사용하지 않았던 ECC 알고리즘이 무선 환경을 위한 공개키 알고리즘으로 선택되었으며, RSA와 비교해 적은 키 사이즈로도 동일한 비도를 보장할 뿐만 아니라 빠른 연산 속도를 보장한다. 두 번째 단말기의 CPU 처리속도와 메모리 제한으로 인증서의 상태정보를 획득하기 위해 CRL을 다운로드하고 분석하는 일련의 작업이 관리되는 인증서가 많아짐에 따라 처리가 어려워진다. 이러한 문제점을 극복하기 위해 X.509v3 인증서를 단순화시킨 WTLS(Short-lived) 인증서를 정의하여 짧은 유효기간을 변경하여 발행한다. 유선의 CRL 메커니즘을 Short-lived 메커니즘이 대행한다. 세 번째, 이동 단말기에서 인증서 요청 형식을 유선에서 사용하고 있는 PKC #10, RFC 2511을 사용하지 않고 WAP Forum에서 정의하고 있는 스크립트 함수인 signText 함수를 응용하여 무선 환경에 맞는 인증서 요청 및 관리 프로토콜 규격을 정의하여 사용하는 것을 권고한다.

네 번째, 유선용과 무선용 X.509v3 인증서 프로파일에 <표 1>에서 알 수 있듯이 유선에서는 AKI와 SKI의 생성, 처리가 Mandatory로 되어 있는데 무선 단말기에서는 처리부분을 가볍게 하기 위해 두 필드에 대하여 처리부분은 선택사항(option)으로 정의하였고 인증서 상태검증의 방법으로 OCSP 사용을 위해 DI 필드와 AIA 필드를 포함하였다[11, 12].

〈표 1〉 인증서 프로파일 비교

항 목		Critical	생 성	처 리
Authority Key Identifier	유 선	n	m	m
	무 선	n	m	o
Subject Key Identifier	유 선	n	m	m
	무 선	n	m	o
Domain Information	유 선	n	m	m
	무 선	n	m	o
Authority Information Access	유 선	n	m	m
	무 선	n	m	o

c : critical n : non-critical b : critical or non-critical
- : not defined m : mandatory o : option x : not recommended

2.2 블루투스 개요

블루투스는 최초 스웨덴의 에릭슨이라는 회사에서 무선 근거리 통신을 위해 저전력, 저비용으로 무선 인터페이스를 가능하게 하기 위한 기술로서 시작된 프로젝트 이름이었다. 후에 이러한 프로젝트명을 바꾸려고 하였으나 프로젝트의 이름이 현재의 이름으로 굳어졌다. 이에 따라 블루투스에 관심을 갖는 회사들은 1998년 5월에 무선 근거리 통신을 위한 하나의 프로젝트 개발을 위해 결성되었다. 이러한 그룹은 기존 케이블로 연결된 셀룰러 전화기를 통해서 셀룰러 망에 연결된 다중 통신을 조사하고자 하였으며 이것이 SIG(Special Interest Group)라는 이름으로 시작된 최초의 모임이다.

블루투스 이전에도 IrDA, IEEE 802.11, SWAP와 같은 무선 근거리 무선통신들이 많이 등장하였다. 그러나 블루투스가 주목받고 있는 이유는 여러 가지 들 수 있는데 우선 기업 측면에서는 대량 출하 수량을 통해 전세계적으로 판매할 수 있다는 점을 들 수 있으며 저가격으로 제조할 수 있다는 장점을 가지고 서로의 상호작용을 일으켜 부품에 대한 저가격화가 가능하고 이에 따라 출하수량이 늘어나는 상승효과를 가져다줄 수 있다. 또한 사용자 측면에서는 적은 소모 전력으로 휴대폰이나 기타 주변장치들의 무선 연결을 통해 선이 없는 인터페이스를 이루므로 보다 간편하고 효율적인 측면에서 사용자에게 다가서고 있다. 전체적으로 살펴보았을 때 정보통신 산업이 무엇을 위해 발전하였는가를 살펴보면 쉽게 알아볼 수 있다. 이는 보다 자유롭고, 안전하며, 신뢰성과 최근 급부상하고 있는 인터넷의 확장과 더불어 발전하고 있는 것이며 이를 만족하기 위해 제안된 기술이 블루투스라 볼 수 있다. 블루투스를 간단히 정의한다면 근거리 무선 통신을 위한 하나의 기술이다. 중요한 것은 사용자의 요구에서 발생한 기술이라는 점이다. 이는 블루투스가 가져야 하는 여러 가

지 특징 중에서 가장 중요한 특징이라고 할 수 있다.

블루투스의 또 다른 특징의 하나는 작은 네트워크의 구성이 가능하다는 것이다. 이는 피코넷(Piconet)이라 불리우며, 하나의 피코넷에는 슬레이브가 2개에서 최대 7개까지 연결이 가능하다. 이러한 피코넷이 여러개가 모여 서로 연결되어 있을 때 이를 스카터넷(Scatternet)이라 한다. 결국 피코넷은 여러 통신장비를 하나의 통신 네트워크로 묶을 수 있다는 장점이 된다[5].

보안적인 측면에서 블루투스는 자체 보안 서비스를 제공해주는 특징이 있으며 블루투스 프로파일에서도 이와 관련되어 다음과 같은 3가지 보안 서비스를 기술하고 있다[4,5].

- 보안 모드 1(non-secure)
  각 디바이스는 어떠한 보안 프로시져도 가지고 있지 않다.
- 보안 모드 2(서비스 레벨 보안)
  각 디바이스는 L2CAP(Logical Link Controller and Adaptation Protocol) 레벨에서의 채널 설정 이전에 보안 프로시져를 획득할 수 없다. 이 모드는 응용을 위한 이질적이고 유동적인 액세스 정책을 허용하는 것으로서, 특히 서로 다른 보안 요구사항을 갖는 응용에서 수용된다.
- 보안 모드 3(link 레벨 보안)
  각 디바이스는 LMP(Link Manager Protocol) 레벨의 link set-up이 완벽하게 이뤄지기 이전에 보안 프로시져를 가질 수 있다.

2.3 무선랜(Wireless LAN)

IEEE(Institute of Electrical and Electronics Engineers)는 사용자들의 랜에 대한 무선 접근의 요구에 발맞추어 모바일 장비, 랩톱, PDA, 네트워크에 선이 없이 통신이 가능한 무선랜을 802.11의 표준으로 발표하고 계속적인 연구를 지속하고 있다.

이 표준안에는 이더넷에서 처리되는 속도처럼 11Mbps의 무선랜 제품에 대한 표준을 포함하고 있다. 이러한 무선랜 장비의 네트워크 처리속도는 기업이나 조직이 무선랜 장비를 도입하기 위한 무선랜 장비의 요구사항이기도 하다.

많은 무선랜 장비들의 호환성 때문에 WECA(Wireless Ethernet Compatibility Alliance)라 불리우는 공동체를 형성하였으며, 이러한 WECA에 대한 지원을 제품에 표현하기 위해 "Wi-Fi"라고 언급 규격문구를 사용하기도 한다. 수십개의 벤더들이 Wi-Fi 제품들에 대한 시장을 형성해 왔으며, 많은 업체 및 조직들이 무선랜의 도입을 고려하고 있다. 랜으로의 무선 접근에 대한 요구는 모바일장비, 랩탑, PDA, 네트워크에 "plug-in" 없이 연결을 하려하는 사용자들의 계속적인 성장에 의하여 가속화 되었으며, 2003년에는 10억개 이상의 모바일 장비들이 사용될 것이며, 무선랜 시장도 2002년에는 20억불 이상으로 성장할 것으로 전문가들은 예상하고 있으며 무선랜 장비의 보안시장도 상당히 성장할 것으로 예상된다. 무선랜의 주요한 관심은 보안이며 이러한 보안 사항은 접근제어(Access Control)와 프라이버시(Privacy) 등이다. 접근제어는 민감한 자료들이 허가된 사용자들에 의해서만 접근되어질 수 있도록 하는 것이며, 프라이버시는 송수신되는 자료들이 의도된 대상들에 의해서만 처리되어 지도록 되는 것이다. 무선랜에서 송·수신되는 자료는 전파(Radio Wave)를 사용하여 공중으로 브로드캐스트(Broadcast)되기 때문에 자료의 송·수신 디바이스에 의해 제공되는 공간에 있는 모든 무선랜 사용자들에게 자료가 전송된다. 그러나 전파는 천장, 바닥, 벽, 공중으로 송신되기 때문에, 전송된 자료는 의도되지 않은 대상들(다른 층, 건물 밖 등)에게 도달 할 수 있다. 비슷하게 무선랜의 송신을 하나의 대상으로만 지시할 수 없기 때문에 자료의 프라이버시는 매우 중요한 고려대상이다. IEEE 802.11b 표준은 접근제어, 프라이버시를 보장하는 요소들에 대한 내용을 포함하고 있다. 이러한 무선랜 장비의 보안요소들은 무선랜 장비의 규격에 반드시 포함되어져야 한다. 이와 더불어 수백, 수천의 무선랜 사용자들을 고용하고 있는 조직들은 중앙집중 및 효율적인 방법으로 관리되어질 수 있는 구체적인 보안 솔루션을 필요로 한다[6-8].

3. 근거리 무선통신의 보안 요구사항

3.1 보안 요구사항

무선 통신의 특수한 환경을 고려해 볼 때 유선에 비해 보안적인 취약점이 더욱 심화되는 것은 당연하다. 즉, 제한된 환경에서 이루어지는 보안 서비스는 유선에 비해 취약할 수 밖에 없으며, 이로인해 사용자의 프라이버시를 침해 할 위험성이 매우 높다. 따라서 사용자 주변에 흩어져 있는 모바일 디바이스의 취약성은 사용자의 프라이버시 침해와 직결된다.

따라서 본 장에서는 근거리 무선 통신인 블루투스와 무선랜을 실제 적용하기 위해서 필요한 보안적 요구사항을 다음과 같이 제시한다[3-5, 7-10].

- 기밀성(Confidentiality) : 근거리 무선 통신인 블루투스와 무선랜에서 제공하는 기밀성 보안 서비스는 PIN(Personal Identification Number)에 근거하거나 기밀성 서비스를 위한 키 생성과정 및 전송 과정에서 취약성을 내포하고 있다. 따라서 랜덤 수에 근거한 동적인 세션키 설정을 통해 사용자의 프라이버시를 제공해야 한다.
- 무결성(Integrity) : 사용자의 데이터가 근거리 무선 통신 기술을 이용해 전송될 때 전송 데이터에 대해 무결성 서비스를 제공해야 한다.
- 인증(Authentication) : 블루투스와 무선랜으로 대표되는 현재의 근거리 무선 통신 기술에서 반드시 필요한 것이 모바일 디바이스를 사용하는 사용자에 대한 인증이다. 현재 인증 서비스는 사용자의 인증이 아니라 모바일 디

바이스 자체에 대한 인증이다. 따라서 사용자 인증 뿐만 아니라 전체 참여 객체들간의 상호인증이 반드시 필요하다.

- 부인봉쇄(Non-repudiation of send/receipt) : 근거리 무선 통신의 모바일 디바이스에 대한 사용자의 비인증은 전송하거나 전송되는 데이터에 대한 부인봉쇄 서비스를 제공할 수 없게 한다. 따라서 사용자 인증과 함께 반드시 제공되어야 할 서비스가 부인봉쇄이다.

3.2 근거리 무선 통신의 비보안적 요구사항

근거리 무선 통신 기술에서 보안적인 요구사항이 아니면서 사용자의 프라이버시와 밀접한 관계가 있어 반드시 고려되어야 할 비보안적 사항은 다음과 같다[5-6, 9-10].

- 전력(Power) : 모바일 환경에서 전력은 매우 중요하며 사용자 주변의 모바일 디바이스에 대한 주기적인 감시가 필요하다.
- 프로세싱(Processing) : 모바일 디바이스의 현재 프로세싱은 전력과도 매우 밀접한 관계가 있으며, 사용자가 의도하지 않은 프로세싱은 사용자의 프라이버시와 밀접한 관계가 된다.
- 관리체계(Management) : 흩어져 있는 모바일 디바이스들은 서로 다른 보안 정책을 유지하며 공격자에 의해 의도된 침해가 있을 경우 이에 대한 실시간적인 감시 및 보안 정책에 대한 변동이 가능해야 한다.

3.3 근거리 무선 통신 기술 보안 분석

사용자 중심으로 흩어져 있는 모바일 디바이스간의 통신은 사용자 프라이버시와 매우 밀접한 관계가 있으며 무선 환경이라는 특수성을 감안하였을 경우 보안적인 사항에 포함되지는 않지만 반드시 고려해야 하는 비보안적인 사항까지 고려해 분석되어야 한다.

3.3.1 블루투스의 보안적 취약점 분석

블루투스는 자체 보안 서비스를 제공하고 있으나 블루투스가 실제 적용되었을 때는 다음과 같은 보안적 취약점을 가지고 있다[3-5].

- 기밀성 : 블루투스는 PIN에 근거한 보안 키를 생성한다. 그러나 PIN 길이의 취약점에 의해 발생되는 보안 키는 사용자의 기밀성을 유지할 만큼의 보안 서비스를 제공해 주지 못한다.
- 무결성 : 블루투스에서 자체 제공되는 보안 서비스는 안전한 무결성 서비스를 제공하고 있지 않는다.
- 인증 : 블루투스는 모바일 디바이스에 대한 인증만이 이루어질 뿐 사용자에 대한 인증은 이루어지지 않는다. 또한 블루투스 무선 통신에 참여하는 각 객체간의 상호인증이 요구된다.
- 부인봉쇄 : 블루투스에서는 디바이스에 대한 인증만을 취하므로 실제 사용자에 대한 부인봉쇄 서비스는 제공하지 못한다.

3.3.2 무선랜의 보안적 취약점 분석

IEEE 802.11b 표준은 WEP(Wired Equivalent Privacy)이라는 부가적인 암호화 기능을 제공하고 있다. WEP은 무선랜의 데이터 스트림을 보호하는 메커니즘을 제공한다. 그러나 다음과 같은 보안적 취약점을 가진다[7-10].

- 기밀성 : 현재 WEP이 선택적인 부가기능이지만 40 비트 암호화 키를 지원한다. 그러나 사용되는 암호 키는 제 3자에 의해 안전성을 가지지 못한다.
- 무결성 : 무선랜에서의 제공하는 무결성 서비스는 CRC (Cyclic Redundency Check) 서비스로서 완전한 무결성 서비스를 제공해 주지 못한다.
- 인증 : 무선랜에서 제공해주는 두가지 인증 매커니즘은 공개키 인증방식과 공유키 인증 방식으로 나뉘며 공개키 인증방식의 경우 올바른 WEP 키 없이도 엑세스포인터에 접속할 수 있는 단점이 있으며 공유키 인증 방식의 경우 WEP키를 가지고 암호화 해서 엑세스포인트로 반환해야만 하는 챌린지 텍스트 패킷을 송신하지만 올바른 키가 없다면 인증이 실패해서 엑세스포인트와 연결할 수 없다.
- 부인봉쇄 : 무선랜에서 제공하는 인증 방법은 카드나 하드웨어 장비의 분실 및 악의적인 사용에 대한 대응이 어려우며, 단방향 인증으로 인해 전송 및 수신 데이터에 대한 부인봉쇄가 어렵다.

3.4 블루투스와 무선랜의 공통된 비보안적 취약점 분석

블루투스와 무선랜이 좀더 보편화되기 위해서는 강화된 보안 서비스와 더불어 다음과 같은 문제점들에 대한 서비스를 제공해야 한다[4, 7-8].

- 전력 : 모바일 환경에서 모바일 디바이스의 전력은 가장 중요한 요소로서 전력을 최소화 하면서 최대의 성능을 발휘해야 한다. 그러나 블루투스와 무선랜의 경우 공격자로 의심되는 제 3자에 의해 지속적인 연결 요청을 인지함으로써 전력에 대한 보안 대책이 없다.
- 프로세싱 : 모바일 디바이스의 현재 진행 프로세스는 사용자의 프라이버시뿐만 아니라 전력과도 밀접한 관계가 있다. 특히 비인가 된 프로세싱을 사용자가 주기적으로 감시할 필요가 있다. 그러나 현재의 근거리 무선통신 서비스에서는 사용자의 감시 기능을 제공해주지 못하고 있다.
- 관리체계 : 사용자 주변에 많은 디바이스들을 계속적인

감시를 위해서는 사용자가 중심이 되는 중앙 집중형 보안 모니터링 기법이 필요하다. 현재의 블루투스와 무선랜은 이러한 관리 기법을 제공해 주지 못해 사용자 주변의 많은 디바이스들을 관리할 수 없다.

4. 제안방식 I

4.1 근거리 무선 통신에 적용 가능한 보안 모니터링 기법

본 논문에서는 WPKI 기반 구조하에서 모바일 디바이스에 고유의 보안 정책을 감시하는 기지 에이전트가 내장되어 있다고 가정한다. 제안 방식의 구성 객체는 크게 모바일 디바이스와 정책 관리 서버로 구성된다.

- 모바일 디바이스 : 사용자의 주변에 흩어져 있는 유동성 디바이스
- 정책 관리 서버 : 정책 관리 서버는 사용자 주변의 모바일 디바이스에 대한 주기적인 감시를 통해 보안 정책을 감시 및 수정하는 객체

4.1.1 일반화 모델 시스템 계수

다음은 근거리 무선 통신에 적용 가능한 안전한 보안 모니터링 기법을 구성하는데 필요한 시스템 계수를 기술한다.

$*$: 참여 개체(모바일 디바이스 : W, 정책 관리서버 : S)를 가리키는 지시자

$*_p$, $*_q$: 공개키 암호 알고리즘 E를 기반으로 한 $*$의 공개키, 개인키

M_W : 모바일 디바이스의 기지 에이전트에서 생성한 이벤트 메시지(모바일 디바이스의 이름, 현재 진행중인 기지 에이전트 ID, 의심되는 시스템 로그가 있을 경우 로그를 남긴 Time Stamp, 해당 다바이스의 이름, 현재 전력상태, 전력 소비율, 정보 수집때의 Time Stamp)

M_{res} : 이벤트 메시지 M_W에 해당하는 정책 관리 서버의 이벤트 응답 메시지

r_* : $*$가 생성한 의사난수

$H()$: 안전한 해쉬 함수

$E()$: 공개키 암호 알고리즘

g, n : 각 객체에 공유된 시스템 계수

T_* : $*$가 생성한 타임 스탬프

$V*\_@$: $*$에서 @p의 공개키로 암호화하여 @으로 전송되는 암호화된 값

Cert$*$: $*$의 공개키 인증서

ID$*$: $*$의 정보

4.1.2 일반화된 보안 모니터링 프로토콜

[단계 1] 이벤트 발생 및 정책 설정단계

모바일 디바이스의 기지 에이전트는 현재 보안 정책에 위배되는 보안적 및 비보안적 위협이 있을 경우 이를 이벤트 메시지로 변환하여 정책 관리 서버와의 통신이 이루어지는 단계이다.

① 모바일 디바이스는 현재 발생된 이벤트 전송을 위해 암호화된 값 V_{W_S}와 상호인증을 위한 X_W, e_W을 타임스탬프 T_W과 함께 정책 관리 서버에 V_{W_S}, X_W, T_W을 전송한다.

$$V_{W\_S} = E_{S_p}(ID_W \| M_W \| g^{r_W})$$
$$e_W = H(ID_W \| M_W)$$
$$X_W = H(ID_W \| g^{r_W}) \oplus H(e_W \| M_W) \bmod n$$

② 정책관리 서버는 전송받은 V_{W_S}를 자신의 개인키로 복호화한 뒤 다음을 계산하여 전송된 값의 무결성과 모바일 디바이스의 인증을 검증한다.

$$e_W' = H(ID_W \| M_W),$$
$$X_W' = H(ID_W \| g^{r_W}) \oplus H(e_W' \| M_W) \bmod n$$

$e_W = e_W'$이고 $X_W = X_W'$이면 모바일 디바이스의 이벤트 메시지 M_W의 응답 메시지 M_{res}를 생성하고 다음을 계산하여 모바일 디바이스에 V_{S_W}, X_S, T_S를 전송한다.

$$V_{S\_W} = E_{W_p}(ID_S \| M_{res} \| g^{r_S})$$
$$e_S = H(ID_S \| M_{res})$$
$$X_S = H(ID_S \| g^{r_S}) \oplus H(e_S \| M_{res}) \bmod n$$

③ 모바일 디바이스는 정책 관리 서버가 전송한 암호화된 값 V_{S_W}를 자신의 개인키로 복호화하여 기밀성을 검증하고 e_S', X_S'를 생성하여 전송된 e_S와 X_S를 비교한 뒤 무결성과 인증 데이터를 검증한다.

이상의 단계를 기반으로 모바일 디바이스는 정책 관리 서버로부터 현재의 보안 이벤트에 대한 응답 메시지를 현재의 보안 정책에 수용함으로써 사용자의 프라이버시 보호를 위한 정책을 수정 및 보완한다.

[단계 2] 세션키 설정 단계

초기 이벤트 발생 후 지속적인 모니터링이 필요한 경우 모바일 디바이스와 정책 관리 서버 사이의 동적 세션키 설정 단계이다.

① 모바일 디바이스는 지속적인 보안 이벤트의 전송을 위한 세션키 생성 정보인 Z_W와 공개키 인증서 $Cert_W$, 타임스탬프 T_W를 정책 관리서버에 전송한다.

$$Z_W = H((r_W \oplus g^{r_S}) \| T_W)$$

② 정책 관리 서버는 모바일 디바이스로부터 전송된 공개

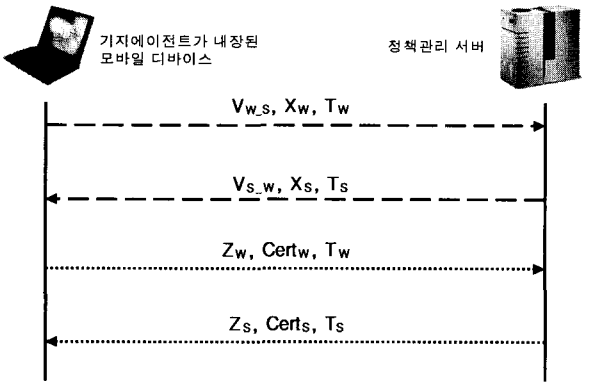
키 인증서를 확인한 뒤 Z_W, T_W를 임시 저장하고, 모바일 디바이스와의 동적 세션키 설정을 위한 정책관리 서버의 세션키 생성 정보인 Z_S, 자신의 공개키 인증서 $Cert_S$, 타임스탬프 T_S를 모바일 디바이스에 전송한다.

$$Z_S = H((r_S \oplus g^{r_W}) \| T_S)$$

모바일 디바이스는 전송된 값에서 정책 관리 서버의 $Cert_S$를 확인한 뒤 정당할 경우 정책 관리 서버와 모바일 디바이스는 세션키 K를 다음과 같이 생성한다.

$$K = H(Z_W \oplus g^{r_S} \| Z_S \oplus g^{r_W})$$

이상의 진행과정을 그림으로 도식화하면 다음과 같은 (그림 1)로 표현할 수 있다.



(그림 1) 근거리 무선통신에 적용 가능한 보안 모니터링 일반화 기법

4.2 무선랜에 적용한 안전한 보안 모니터링 기법

본 논문에서는 WPKI 기반의 무선랜 환경에서 모바일 디바이스에 내장된 기지 에이전트를 이용하여 AP(Access Pointer)와 유선으로 연결된 중앙 서버의 보안 모니터링을 통해 현재 사용자 주변의 모바일 디바이스의 보안 사항을 모니터링 함으로써 공격자로 의심되는 제 3자로부터의 안전한 근거리 통신이 가능한 방식을 제안한다. 제안된 방식이 진행되기 위해 다음과 같은 몇 가지 전제사항을 제시한다.

- 사용자의 PIN 입력은 안전하게 이루어진다.
- 공개키 인증서 $Cert$는 25시간 마다 안전하게 자동 갱신된다.

4.2.1 시스템 계수

무선랜에 적용한 보안 모니터링을 위한 시스템 계수이며, 일반화 모델과 공통된 시스템 계수는 생략한다.

$*$: 참여 개체(중앙서버 : D, AP(Access Pointer) : P, 에이전트 : A, 모바일 디바이스 : W)를 가리키는 지시자

M_* : $*$의 기지 에이전트에서 생성한 이벤트 메시지(모바일 디바이스의 이름, 현재 진행중인 기지 에이전트 ID, 의심되는 시스템 로그가 있을 경우 로그를 남긴 Time Stamp, 해당 다바이스의 이름, 현재 전력상태, 전력 소비율, 정보 수집때의 Time Stamp)

M_{res} : 메시지 M_*에 해당하는 응답 메시지

Sig_* : $*$의 공개키 서명값

r_{*_1}, r_{*_2} : $*$의 개체가 생성한 의사난수들

PIN(Personal Identification Number) : 사용자가 입력하는 사용자 고유번호

4.2.2 프로토콜 진행 단계

모바일 디바이스내에 활성화 된 기지 에이전트에서 보안 정책에 위배된 이벤트가 발생했을 경우 이를 모바일 디바이스에 통보하고 중앙 서버의 이벤트 응답 메시지를 대기하는 단계이다.

[단계 1] 이벤트 발생 및 통보 단계

단계 1은 이벤트 발생 및 통보 단계로써 WLAN을 사용하는 사용자 모바일 디바이스의 기지 에이전트에서 보안적 및 비보안적 위협이 있을 경우 이를 이벤트 메시지로 변환하여 중앙서버에 통보하는 단계이다.

① 모바일 디바이스에 포함된 기지 에이전트는 모바일 디바이스 자체의 보안 정책에 위배되는 이벤트가 발생했을 경우 이를 모바일 디바이스에 전송한다.

② 이벤트 발생을 통보 받은 모바일 디바이스는 전송데이터에 대한 무결성과 인증 데이터에 대한 무결성과 상호인증을 위해 X_W, e_W, C_W를 계산한 뒤 중앙 서버의 공개키로 암호화된 값 V_{W_D}와 자신의 공개키 인증서 $Cert_W$, 타임스탬프 T_W를 $(ID_A \| X_M \| M_M)$, C_W와 함께 AP에 전송한다.

$$X_W = (g^{r_{W_1}} \times r_{W_2} \bmod n)$$
$$e_W = H(X_W \| M_W)$$
$$C_W = H(ID_W \| e_W) \oplus H(g^{r_{W_1}} \times W_p) \bmod n$$
$$V_{W\_D} = E_{D_*}(e_W \| g^{r_{W_1}})$$

[단계 2] 중앙 관리 서버와 통신단계

단계 2는 모바일 디바이스에서 발생한 보안 이벤트에 대한 중앙 관리 서버의 보안 정책의 수정과 이벤트에 대한 보완사항을 모바일 디바이스에게 안전하게 전송하는 단계이다.

① AP는 전송받은 V_{W_D}, $(ID_A \| X_W \| M_W)$, C_W, $Cert_W$, T_W에서 모바일 디바이스의 인증서를 확인한 뒤 $(ID_A \| X_W \| M_W)$, C_W를 중앙 서버의 공개키로 암호화하여 V_{P_D}를 계산한다. AP는 계산된 V_{A_D}를 자신의 공개

키 인증서와 함께 다음을 중앙서버에 전송한다.

$$V_{P\_D} = E_{D_s}(ID_A \| X_W \| M_W \| C_W)$$
$$(V_{W\_D} \| Cert_P),\ V_{P\_D}$$

② 중앙서버는 전송받은 $Cert_P$를 확인한 뒤 V_{W_D}, V_{P_D}를 자신의 개인키로 복호화 하여 다음을 계산하여 무결성을 검증한다.

$$e_W' = H(X_W \| M_W)$$
$$C_W' = H(ID_A \| e_W') \oplus H(g^{r_{W_1}} \times W_p)$$

$C_W' = C_W$이면, 모바일 디바이스의 공개키 인증서를 확인하고 전송된 이벤트 메시지 M_W에 해당되는 응답 메시지 M_{res}를 생성한 후 다음을 계산하여 AP에게 V_{D_W}, $Cert_D$, T_D를 전송한다

$$X_D = (g^{r_{D_1}} \times r_{D_2} \bmod n)$$
$$e_D = H(X_D \| M_{res})$$
$$C_D = H(ID_D \| e_D) \oplus H(g^{r_{D2}} \times D_p) \bmod n$$
$$V_{D\_W} = E_{W_p}(ID_D \| X_D \| M_{res} \| C_D \| g^{r_{D_1}})$$

③ AP는 전송받은 V_{D_W}, $Cert_D$, T_D에서 중앙서버의 공개키 인증서와 타임 스탬프를 확인하고 V_{D_W}와 자신의 공개키 인증서 $Cert_P$를 모바일 디바이스에 전송한다.

$$(V_{D\_W} \| Cert_P)$$

④ 모바일 디바이스는 전송받은 $(V_{D_W} \| Cert_P)$에서 AP의 공개키 인증서를 확인하고 자신의 개인키로 V_{D_W}를 복호화 한 뒤

$$e_D' = H(X_D \| M_{res})$$
$$C_D' = H(ID_D \| e_D') \oplus H(g^{r_{D_1}} \times D_p)$$

$e_D' = e_D$이고 $C_D' = C_D$이면 중앙서버의 M_{res}를 모바일 디바이스의 ID_W와 함께 기지 에이전트에 전송한다.

$$(M_{res},\ ID_W)$$

[단계 3] 세션키 설정 단계

기지 에이전트는 중앙 서버의 이벤트 응답 메시지에 맞는 보안의 재설정과 모바일 디바이스의 계속적인 보안 모니터링을 위한 세션키 설정 단계이다.

① 중앙 서버로부터 전송된 보안 정책에 따라 기지 에이전트는 모바일 디바이스의 보안 업데이트를 통해 보안 정책을 수정하고 계속적인 보안 모니터링을 위해 사용자의 PIN번호를 이용하여 모바일 디바이스의 동적 세션키 정보인 Z를 생성한 뒤 모바일 디바이스에 전송한다.

$$Z = H(PIN \| r_{W_1})$$
$$(r_{W_1} \| Z \| T_A)$$

② 모바일 디바이스는 전송 받은 $(r_{W_1} \| Z \| T_A)$를 자신의 공개키 서명값과 암호화 된 V_{W_D}, T_W를 AP에 전송한다.

$$S_W = Sig_{W_s}(ID_W \| T_W)$$
$$V_{W\_D} = E_{D_p}(r_{M_1} \| Z \| T_A)$$

③ AP는 전송된 정보의 타임스탬프 T_W 확인하고 S_W, V_{W_D}을 자신의 개인키로 서명한 S_P를 계산하여 중앙서버에 전송한다.

$$S_P = Sig_{P_s}(S_W \| V_{W\_D})$$
$$(S_P,\ T_P)$$

④ 중앙 서버는 전송된 (S_P, T_P)에서 AP의 공개키로 S_P의 서명을 확인하고 올바른 경우 S_W를 모바일 디바이스의 공개키로 서명을 확인하여 ID_W를 저장한다.

중앙서버는 ID_W를 저장한 후에 자신의 개인키로 V_{W_D}를 복호화 한 뒤 $(r_{W_1} \| Z \| T_A)$를 확인하고 중앙서버의 세션키 정보인 Z'를 계산하고 공개키 서명값 S_D와 모바일 디바이스의 공개키로 암호화한 값 V_{D_M}를 생성한 후 AP에 V_{D_W}, S_D, T_D를 전송한다.

$$Z' = H(Z \| r_{D_1})$$
$$S_D = Sig_{D_s}(ID_D \| T_D)$$
$$V_{D\_W} = E_{W_p}(r_{D_1} \| Z' \| T_D)$$

⑤ AP는 전송된 S_D를 중앙 서버의 공개키로 복호화 하여 ID_D, T_D를 확인한 뒤 V_{D_W}를 자신의 개인키로 서명하여 S_P, T_P를 모바일 디바이스에 전송한다.

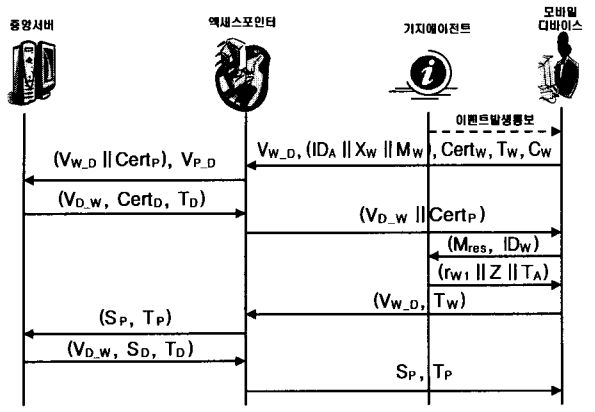
$$S_P = Sig_{P_s}(V_{D\_W})$$

⑥ 모바일 디바이스는 전송된 S_P를 AP의 공개키로 서명을 확인한 뒤 V_{D_W}를 자신의 개인키로 복호화 하여 r_{D_1}, Z'를 확인한다.

⑦ 모바일 디바이스와 중앙관리 서버는 다음을 공통으로 계산하여 새로운 보안 이벤트가 발생하기 전까지 보안 모니터링을 위한 세션키 K를 계산한다.

$$K = H(r_{D_1} \| Z) \oplus H(r_{M_1} \| Z')$$

이상의 내용은 (그림 2)와 같이 요약해 볼 수 있다.



(그림 2) 무선랜에 적용 가능한 보안 모니터링

4.3 블루투스에 적용한 보안 모니터링 기법

일반화된 보안 모니터링 기법을 블루투스에 적용하기 위한 전제사항을 다음과 같이 가정한다.

- 블루투스의 마스터와 슬레이브는 그룹 키에 근거한 그룹 서명값을 기반으로 안전한 피코넷이 형성되었다.
- 안전한 피코넷 기반의 마스터와 슬레이브는 WPKI 기반 구조하에서 25시간 마다 갱신되는 인증서를 내장하고 있으며 고유의 보안 정책을 감시하는 기지 에이전트가 내장되어 있다.

따라서 제안 방식의 구성 객체는 크게 블루투스 마스터와 슬레이브로 구성된다.

- 블루투스 마스터 : 사용자의 주변에 흩어져 있는 유동성 디바이스들이 블루투스 통신을 위해 형성한 피코넷의 마스터 유동 디바이스
- 블루투스 슬레이브 : 블루투스 슬레이브로 정의된 모바일 디바이스로서 기지 에이전트가 내장되어 있으며 자체 보안 정책을 가지고 있는 디바이스

4.3.1 시스템 계수

다음은 블루투스에 적용한 안전한 보안 모니터링을 구성하는데 필요한 시스템 계수를 기술한다(일반화 모델에서와 공통된 시스템 계수는 생략).

$*$: 참여 개체(블루투스 마스터 : W, 블루투스 슬레이브 : S)를 가리키는 지시자

M_S : 블루투스 슬레이브에 내장된 기지 에이전트에서 생성한 이벤트 메시지(블루투스 슬레이브의 이름, 현재 진행중인 기지 에이전트 ID, 의심되는 시스템 로그가 있을 경우 로그를 남긴 Time Stamp, 해당 디바이스의 이름, 현재 전력상태, 전력 소비율, 정보 수집 때의 Time Stamp)

M_{res} : 이벤트 메시지 M_S에 해당하는 블루투스 마스터의 이벤트 응답 메시지

S_i : 안전한 피코넷 형성에 따른 블루투스 슬레이브의 그룹키 서명값

$EB(\,)$: 대칭키 암호 알고리즘

$V*@$: 대칭키로 암호화되여 $*$에서 @으로 전송되는 암호화된 값

4.3.2 블루투스에 적용한 보안 모니터링 프로토콜 진행 단계

[단계 1] 이벤트 발생 및 정책 설정단계

[단계 1]에서 블루투스 마스터와 슬레이브는 안전한 피코넷 형성 후 피코넷의 마스터는 해당 슬레이브에 내장된 기지 에이전트에서 현재 보안 정책에 위배되는 보안적 및 비보안적 위협이 있을 경우 이에 대한 메시지를 전달받고 그에 해당하는 응답 메시지를 전송하는 단계이다.

① 블루투스 슬레이브는 현재 보안 정책에 위배되는 보안적 및 비보안적인 이벤트가 발생하였을 경우, 블루투스 슬레이브의 ID_S, 그룹키 서명값 S_j, 이벤트 메시지 M_S를 블루투스 마스터의 공개키로 암호화하고, 세션 정보의 무결성과 상호 인증을 위한 e_S, X_S를 계산한 뒤 타임 스탬프 T_S와 함께 V_{S_W}, e_S, X_S, g^{r_S}, T_S를 블루투스 마스터에 전송한다.

$$V_{S\_W} = E_{W_p}(ID_S \| S_j \| M_S),\quad e_S = H(S_j \| g^{r_S})$$
$$X_S = H(ID_S \| g^{r_S}) \oplus H(e_S \| T_S) \bmod n$$

② 해당 피코넷의 블루투스 마스터는 전송받은 V_{S_W}를 자신의 개인키로 복호화 하고 전송된 e_S, X_S의 검증을 통해 세션 정보의 무결성과 인증정보를 검증한다.

$$e_S' = H(S_j \| g^{r_S}),$$
$$X_S' = H(ID_S \| g^{r_S}) \oplus H(e_S' \| T_S) \bmod n,$$
$$e_S = e_S' \text{이고 } X_S = X_S'$$

이상의 내용이 올바른 경우 블루투스 마스터는 블루투스 슬레이브의 이벤트 메시지 M_M의 응답 메시지에 해당되는 M_{res}를 생성하고 자신의 ID_W와 동적 세션키 설정정보로 계산된 Z'를 블루투스 슬레이브의 공개키로 암호화한 뒤 전송데이터의 무결성과 인증정보를 위한 e_W, X_W를 계산하여 타임스탬프 T_W와 V_{W_S}, e_W, X_W, g^{r_W}, Z'를 전송한다.

$$V_{W\_S} = E_{S_p}(ID_W \| M_{res} \| Z'),\quad e_W = H(g^{r_W} \| T_W)$$
$$X_W = H(ID_W \| g^{r_W}) \oplus H(e_W \| M_{res}) \bmod n$$
$$Z' = H(r_W \oplus g^{r_S} \| T_W)$$

③ 블루투스 슬레이브는 해당 피코넷의 마스터가 전송한 V_{M_S}를 자신의 개인키로 복호화 한 뒤 e_W'와 X_W'를 생성하여 전송된 e_W와 X_W를 비교함으로써 세션정보의 무결성과 인증정보를 검증한다.

$$e_W' = H(g^{r_W} \| T_W),$$
$$X_W' = H(ID_W \| g^{r_W'}) \oplus H(e_W' \| M_{res}) \bmod n$$

블루투스 슬레이브는 $e_W = e_W'$ 이고 $X_W = X_W'$ 이면 Z' 를 임시 저장하고 해당 피코넷 마스터로부터 현재의 보안이벤트에 대한 응답 메시지를 현재의 보안 정책에 수용함으로써 사용자의 프라이버시 보호를 위한 정책을 수정 및 보완한다.

[단계 2] 지속적인 모니터링을 위한 세션키 설정 단계

초기 이벤트 발생 후 지속적인 모니터링이 필요한 경우 블루투스 마스터와 슬레이브 사이의 동적 세션키의 설정 단계이다.

① 블루투스 슬레이브는 지속적인 보안 이벤트의 전송을 위해 다음을 계산하여 V_{SW}, T_S를 해당 피코넷의 마스터에 전송한다.

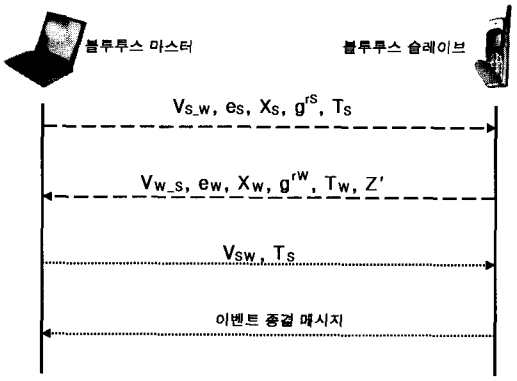
$$Z'' = H((r_S \oplus g^{r_W}) \| T_S),\ V_{SW} = EB_{Z'}(Z'')$$

② 해당 피코넷 마스터는 모바일 디바이스로부터 전송된 자신이 전송했던 Z'로 복호화 한 뒤 Z''를 저장한다.

이상의 단계를 거쳐 블루투스 마스터와 슬레이브는 다음과 같이 세션키 K를 생성한다.

$$K = H(Z' \oplus M_S \| Z'' \oplus M_{res}) \bmod n$$

이상의 진행과정을 그림으로 도식화 하면 다음과 같은 (그림 3)으로 표현할 수 있다.



(그림 3) 블루투스에 적용한 보안 모니터링 기법

5. 제안 방식 고찰

본 논문에서의 일반화된 보안 모니터링 기법은 블루투스와 무선랜으로 대표되는 근거리 무선통신의 보안적, 비보안적인 사항을 고려할 경우, 다음과 같은 특징이 있다.

5.1 보안 요구사항에 대한 고찰

- **기밀성** : 블루투스와 무선랜에서 취약한 기밀성을 공개키 암호 알고리즘과 동적 세션키를 생성하여 보안 이벤트 전송으로 안전한 기밀성을 유지할 수 있다.
- **무결성** : 제안 방식은 안전한 해쉬 함수를 이용한 X, e의 해쉬 값과 타임 스탬프를 이용한 안전한 무결성 서비스를 획득할 수 있다.
- **인증** : 기존 근거리 무선 통신에서 제공하는 단방향 인증으로 발생하는 취약점을 공개키 인증서와 안전한 그룹 서명값을 이용한 상호인증으로 보안적 취약점을 보완하였다..
- **부인봉쇄** : 제안 방식은 상호 인증으로 객체의 상호인증을 기반으로 타임스탬프와 공개키 서명을 이용한 부인봉쇄 방식으로 부인봉쇄 서비스를 제공한다.

5.2 비보안적 요구사항에 대한 고찰

근거리 무선 통신 기술에서 보안적인 요구사항이 아니면서 사용자의 프라이버시와 밀접한 관계가 있어 보안적인 요소 뿐만 아니라 반드시 고려되어야 할 비보안적 사항에 대해 제안 방식은 다음과 같은 특징을 갖는다. 다음과 같다.

- **전력** : 모바일 디바이스에 내장된 기지 에이전트의 주기적인 전력 감시를 통해 중앙정책서버 혹은 중앙 서버의 정책을 모바일 디바이스의 보안정책에 포함시킴으로써 안전한 전력관리 서비스를 제공할 수 있다.
- **프로세싱** : 기지 에이전트에 생성되는 이벤트 메시지에 포함되어 있는 현재 프로세싱의 상태에 대한 주기적인 모니터링을 통한 감시체제를 확립할 수 있다.
- **관리체계** : 사용자 주변에 흩어져 있는 디바이스들이 서로 다른 보안 정책을 유지하지만, 공격자에 의해 의도된 침해가 있을 경우 이에 대한 이벤트 메시지를 생성하고 이를 중앙 정책서버 혹은 중앙 서버로 전송하여 그에 해당하는 실시간적인 감시 및 보안 정책에 대한 변동이 가능하다는 특징을 갖는다.
- **기존 WPKI 정책서버와의 차별성** : 근거리 무선 통신 단말기 사용자만에 각기 다른 보안정책 수립과 디바이스 감시를 위해서는 사용자만의 보안 서비스를 보장하여야 한다. 따라서 기존 WPKI에서 서비스되는 데이터 보안 서비스와는 별도로 사용자 중심의 보안 체계가 필요하며 이는 WPKI 보안 서비스와는 차별화된 서비스라 할 수 있다

〈표 2〉 제안방식 분석

	블루투스 spec v1.1	무선랜의 WEP	제안된 일반화된 보안 모니터링	제안된 블루투스 보안 모니터링	제안된 무선랜 보안 모니터링
기 밀 성	△	△	○	○	○
무 결 성	△	△	○	○	○
인 증	△	△	○	○	○
부인봉쇄	×	×	○	○	○
전력 감시	×	×	○	○	○
프로세싱감시	×	×	○	○	○
관리 체계	없 음	없 음	중 앙	중 앙	중 앙

주) × : 위험, △ : 취약, ○ : 안전

<표 2>는 기존의 방식과 제안 방식을 비교 분석한 결과이다.

6. 결 론

최근 정보통신의 급속한 발전으로 개인 정보통신의 수요는 날로 증가하고 있다. 이에 따라 사용자의 요구에 의해 많은 근거리 무선 통신에 대한 연구가 진행되고 있으며 블루투스와 무선랜의 경우에는 국내 무선국에서 국내 근거리 무선 통신 기술의 표준으로 정착시키기 위한 노력이 계속되고 있다.

본 논문에서는 근거리 무선통신의 특수한 환경에서 요구되는 보안적 요구사항 뿐만 아니라 기존의 기술에서는 고려되지 않았던 비보안적인 사항까지 고려안 안전한 보안 모니터링 기법을 제안하였다. 제안 방식은 실제 무선이라는 환경을 기반으로 사용자 중심으로 흩어져 있는 모바일 디바이스들을 안전하게 관리하면서 사용자의 프라이버시를 유지시킬 수 있는 사항까지를 고려하였다. 이는 기존의 보안적 요구사항만을 만족시키려는 연구와는 차별화된 연구라 할 수 있으며, 근거리 무선 통신의 기술을 실제 환경에 적용시켰을 때 고려되어야 하는 비보안적인 사항까지 고려함으로써 가장 일반화되고 현실성 있는 보안 응용 프로토콜을 제시하였다.

현재 무선 인터넷 사용자의 정보 취득에 대한 욕구는 일반화되고 있는 무선 통신 환경에서 모바일 디바이스의 사용인구의 급증과 모바일 기기의 대중화로 나타나고 있으나, 보안에 관련된 연구는 한정된 보안 환경에서 이루어지고 있는 실정이다. 이에 본 연구는 무선 환경에서 사용자 중심으로 흩어져 있는 모바일 디바이스들간의 통신인 근거리 무선통신 기술을 기반으로 하여 사용자의 프라이버시를 안전하게 유지하면서도 다양한 응용 서비스에 대한 활용이 가능한 방식을 제안하였다.

제안 방식은 현재의 무선 환경에 적용이 가능할 뿐만 아니라 안전하면서도 효율적인 보안 서비스를 제공함으로써 사용자가 중심이 되면서 신뢰할 수 있는 정보 제공 서비스를 받을 수 있으리라 사료된다.

참 고 문 헌

[1] Bluetooth White Paper, http://www.bluetooth.com.

[2] Bluetooth Sepcification v1.1, http://www.bluetooth.or.kr.

[3] Juha T. Vainio, "Bluetooth Security," jssmd, 2000, http://niksula.cs.hut.fi/~jiitv/bluesec.html.

[4] Ullgren T, "Security in Bluetooth Key management in Bluetooth," 2001, http://www.cs.hut.fi/Opinnot/Tik-86.174/sectopics.html.

[5] Jakobsson M. and Wetzel S, "Security Weakness in Bluetooth," RSA, 2001, http://www.bell-labs.com/user/markusj/bt.html.

[6] http://www.hldp.org.

[7] http://www.infoworld.com/articles/hn/xml/02/02/14/020214hnwifispec.xml.

[8] http://www.drizzle.com/~aboba/IEEE/wireless.pdf.

[9] Borisov, Goldberg and Wagner, "Intercepting Mobile Communications : The Insecurity of 802.11," The proceedings of the Seventh Annual International Conference on Mobile Computing and Networking, July, 2001.

[10] Stubblefield, Ioannidis and Rubin, "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP," AT & T Labs Technical Report TD-4ZCPZZ, Aug, 2001.

[11] CISCO System, http://www.cisco.com.

[12] CISCO Systems, Managing Cisco Network Security, Version 2.0, 2001.

[13] Univ. of Maryland, http://www.cs.umd.edu/~waa/wireless.pdf.

[14] 서대희, 이임영, 김해숙 "홈 네트워크에 적용한 블루투스 Security에 관한 연구", 한국통신학회 하계종합학술발표회 논문집(상), 제23권 제2호, pp.36-39, 2001.

[15] 서대희, 이임영, 김영백, 김해숙 "ECC를 이용한 안전한 피코넷에 관한 연구", 정보처리학회 2001년도 추계학술발표 논문집, 제8권 제2호, pp.911-914, 2001.

[16] 최용락, 소우영, 이재광, 이임영 "컴퓨터 통신보안", 도서출판 그린, 2001.

[17] Alfred J. Menezes, Paul C. Van Oorschot and Scott A. Vanstone "HANDBOOK of APPLIED CRYPTOGRAPHY," CRC.

서 대 희

e-mail : patima@hanmir.com

2001년 동신대학교 전기전자공학과

2001년~현재 순천향대학교 전산학과 석사과정

관심분야 : 암호이론, 정보이론, 컴퓨터 보안

이 임 영

e-mail : imylee@sch.ac.kr

1981년 홍익대학교 전자공학과

1986년 오사카대학 통신공학전공 석사

1989년 오사카대학 통신공학전공 박사

1989년~1994년 한국전자통신연구원 선임연구원

1994년~현재 순천향대학교 정보기술공학부 부교수

관심분야 : 암호이론, 정보이론, 컴퓨터 보안