情 報 保 護 學 會 誌
第18卷 第6號, 2008. 12

모바일 USN 기술 및 보안 취약성 사례 분석

이 해 동*, 박 남 제*, 최 두 호*, 정 교 일*

요 약

현재 널리 쓰이고 있는 다양한 형태의 모바일 디바이스들을 무선 센서 네트워크 환경에 접목하여 보다 편리하고 효율적으로 센서 네트워크 서비스를 제공 받을 수 있는 모바일 USN(Ubiquitous Sensor Network) 서비스 기술을 소개하고, 그 응용 서비스 모델인 Nike 플러스 i-Pod 스포츠 키트 플랫폼에 대해 살펴본다. 그리고, 해당 서비스의 보안취약성을 분석하여 모바일 USN에서의 보안 및 프라이버시 문제를 제시하고, 향후 제공되어질 다양한 모바일 USN 보안 응용 서비스들에 대해 고찰해본다.

Ⅰ. 서 론

기업무선 센서 네트워크는 현재 유비쿼터스 환경을 구현하기 위한 핵심 기술로서 초경량, 저전력 센서들을 사용하여 우리 거주공간 속에서의 다양한 편의 정보, 주변 환경 정보, 교통 정보 등을 센싱하여 사용자에게 전달 할 수 있다. 실제로 센서 네트워크는 센싱 기능과 정보 처리 능력, 그리고 통신 능력을 가진 다수의 센서 노드들로 구성되며, 특히 사용자가 원하는 서비스 영역에 배치된 후 자동적으로 Ad-hoc 네트워크를 형성한 후 필요한 정보를 수집하여 서비스를 제공하는 역할을 한다. 모바일 WSN(Wireless Sensor Networks) 기술은 싱크나 센서노드가 이동성을 가진 모바일폰 기반 센서 네트워크이다. 기본의 센서네트워크가 고정적이였다면, 모바일 WSN은 모바일폰이 싱크와 센서노드의 역할을 가짐으로 인해 이동성을 제공한다. 또한 WiFi-UMTS, WiMax/WiBro-UTMS, Bluetooth-UMTS, Zigbee-UMTS를 모바일폰, PDA, 스마트폰과 같은 멀티 단말기를 통해 제공해 줄 수 있으며 이를 통해 폐쇄적인 센서네트워크의 한계를 극복할 수 있을 것으로 기대하고 있다. 본 고에서는 모바일 USN 기술에 대한 개념을 살펴보고, 현재 상용화된 응용 서비스 모델인 Nike 플러스 i-Pod 스포츠 키트 플랫폼과 그 보안 취약점을 분석하여 모바일 USN에서의 보안 및 프라이버시 문제점을 제시한다. 그리고, 향후 제공되어질 다양한 모바일 USN 보안 응용 서비스들에 대해 고찰해본다.

Ⅱ. 모바일 USN 서비스

USN 기술은 RFID와 함께 유비쿼터스 시대를 열어갈 최첨단 미래 기술로서, 센싱 기술과 무선 네트워크 기술을 혼용하여 인간은 컴퓨팅 기기의 존재를 인식하지 못하는 사이에 센서네트워크를 통하여 데이터를 유통시켜 다양한 서비스를 제공한다. USN 센싱 기기들은 우리 주변에 다양하게 존재할 수 있다. 이처럼 RFID, USN과 같은 유비쿼터스 시대의 기술이 진보해감에 따라, 더 많은 컴퓨팅 장비들이 우리의 일상생활에 파고들고 있다. 지난 세대의 컴퓨터 혁신은 대부분의 사람들에게 하나의 컴퓨터를 보급시키는 효과를 가져왔다. 다음 세대의 혁신은 다수의 컴퓨터를 개개인에게 제공하게 된다. 일대다 컴퓨팅 변혁은 많은 긍정적인 효과를 가져오는 반면, 우리의 개인 프라이버시에 대한 위협은 증가일로에 놓일 것이다.

모바일 USN은 일반 USN과 달리, USN 노드를 구성하는 센서 기기 및 데이터 중계 기능을 담당하는 중간 노드들이 모두 이동성을 가지고, 시간과 장소에 구애 받

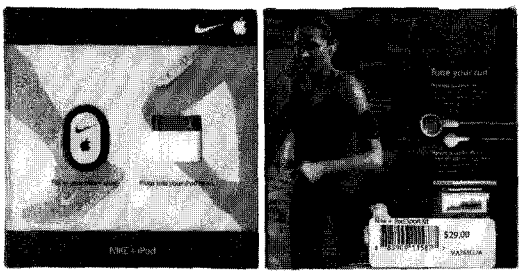
* 한국전자통신연구원 정보보호연구본부 ({haenamu, namjepark, dhchoi, kyoil}@etri.re.kr)
* 본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업[2005-S-088-04, 안전한 RFID/USN을 위한 정보보호 기술] 사업의 일환으로 수행하였음

지 않고 더욱 다양한 서비스를 제공할 수 있는 기술이다. 본 절에서는 모바일 USN 서비스를 구현하는 최신 상품으로서 애플과 나이키의 합작품인 Nike+iPod 스포츠 키트를 소개하고 이와 관련된 정보보호 요소를 논하고자 한다.

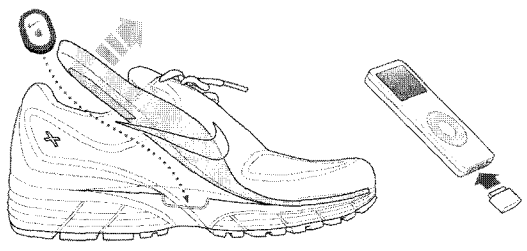
2.1 모바일 USN에서의 프라이버시 문제

본 절에서는 모바일 USN의 최신 응용 서비스인 애플의 Nike+iPod 스포츠 키트의 정보보호 제반 사항의 제반 문제를 다룬다. Nike+iPod 스포츠 키트는 시중가 $29 로 구입 가능하며, 센서와 수신기로 두개의 모듈로 구성된다. 센서는 사람의(편의상 앨리스로 명명) 신발 내에 삽입 장착되며, 수신기는 iPod Nano와 연결된다 (그림 1, 2 참조). 앨리스가 걷거나 달릴 때, 앨리스의 신발에 장착된 센서는 그녀의 움직임에 대한 정보를 센싱하고 수신기를 통해 iPod Nano에 무선으로 전달한다. iPod은 앨리스에게 전체 운동 거리, 소비 칼로리와 같은 정보를 iPod에 연결된 헤드폰을 통해서 피드백한다.

비록 센서는 온-오프 버튼 기능이 있음에도 Nike+iPod 스포츠 키트의 온라인 설명서[9]는 센서를 켜진(온) 상태를 유지하도록 권고하며, 대부분의 경우, 사람들은 센서를 켜진 상태로 방치될 것으로 예측된다. 온



〔그림 1〕 Nike+iPod 스포츠 키트 구성



〔그림 2〕 Nike+iPod 센서(Nike+슈즈에 부착), Nike+iPod 수신기(iPod Nano와 연결)

라인 설명서의 4번째 구절에서 설명하였듯이, 애플은 추적 가능성을 염려하고 있다. 즉, 센서를 통해서 사용자를 추적할 수 있음을 알 수 있다. 이러한 권고는 애플과 나이키가 그들의 기기를 이용하여 악의적인 목적으로 사용할 의도를 가졌다고 볼 수는 없을 것이다. 또한 애플과 나이키 모두 이러한 공격을 찬성하지도 않고 있다.

질레트 레이저[3], 도서관 서적[8] 속의 RFID 태그에서 나타난 우려와 같이, 기존 기술에서의 잠재적 프라이버시 위협을 인식하고 있고 추적성이 바람직하지 않은 결과를 가져올 것이라는 애플의 명백한 인식에도 불구하고, Nike+iPod 스포츠 키트는 가장 기초적인 수준의 사용자 프라이버시조차도 제공하지 못하고 있다. 사용자가 키트를 사용 중일 때 뿐만 아니라, iPod가 없을 때도 Nike+iPod 센서는 고유 식별 정보를 지속적으로 브로트캐스팅하는 장치이다. 게다가 수동형 RFID와 비교해서 Nike+iPod 스포츠 키트는 다음과 같은 이유로 공격자에게 무방비로 노출될 수 있다. (1)Nike+iPod 센서는 어떤 종류의 수동형 RFID보다도 판독 거리가 넓고, (2) 쉬운 공격 방법 및 저렴한 비용으로 공격이 가능하여 결코 안전하지 못하다. 예를 들어 Nike+iPod 수신기를 사용하는 3세대 iPod을 감시 장치로 사용할 수도 있다.

공격 형태를 구체적으로 논하기 위해서, 공격자가 악의적인 목적으로 Nike+iPod을 사용하는 여러 시나리오를 살펴본다. 시나리오들은 충분한 프라이버시 대책이 없을 때 개인의 안전에 심대한 위협을 야기할 수 있음을 보여준다.

스토킹(Stalking). 스토킹 목적을 가진 사람은 Nike+iPod 센서의 브로드캐스팅 반경을 이용할 수 있다. 우리는 다음과 같은 시나리오를 생각해 볼 수 있다. 앨리스는 집, 강의실, 도서관, 학생회관, 체육관 친구의 집을 오갈 때, 나이키 신발을 신고 다니는 대학생이다. 그녀의 전 남자친구인 마빈은 여전히 그녀를 잊지 못하고 다시 만나길 원한다. 만약 마빈이 위에서 언급한 장소에 감시 장치(Nike+iPod 도청기) 설치한다면, 마빈은 Alice의 Nike+iPod 센서에서 브로드캐스팅되는 고유 식별 정보를 도청함으로써, 특정 장소에 대한 앨리스의 출입 상황을 원거리에서 감시할 수 있다. 이러한 감시 정보는 앨리스의 프라이버시에 대한 잠재적 위협일 뿐 아니라, 마빈은 감시 데이터를 이용하여 다음 행동을 취할 수 있다. 최소한, 마빈은 우연을 가장해서 그녀와 우연히 마주친 척할 수 있다.

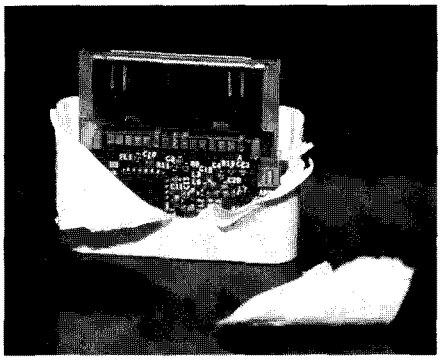
상기 시나리오에서 마빈이 개발한 기기와 비슷하게, 프로토타입 감시 시스템을 만들 수 있다. 앨리스가 이동할 때, 마빈은 자신에게 SMS 문자 메시지 혹은 이메일을 전송하게 할 수 있다. 그러므로 해서 마빈은 앨리스의 현재 위치를 지속적으로 파악할 수 있다. 또한 마빈은 앨리스의 위치 정보와 다른 사람의 위치 정보를 결합하여, 앨리스가 어떤 사람과 접촉하는지, 새로운 남자 친구가 있는지 추측할 수 있다. 만약 앨리스가 Nike+iPod 키트를 구입하지 않더라도, 마빈은 몰래 그녀의 신발에 센서를 장착하고 상기와 같은 공격을 수행할 수 있다.

동시에 다수의 사람들을 추적하고, 범죄 대상을 물색하는데 감시시스템을 사용할 수도 있다. 예를 들어, 범죄자는 특정 시간에 특정 경로로 혼자서 조깅하는 사람을 찾고자 한다. 스토커는 범죄 대상자를 선택한 후, 감시 시스템에 저장된 로그 데이터베이스를 이용하여 특정 인물의 행동 습관에 대한 정보를 취득하여, 특정 인물이 다음 시간에 갈 위치를 예측한 후 범죄 희생자를 납치할 수 있다.

개인의 전자 기기에 기반을 둔 추적가능성은 새로운 것은 아니다. 제 3자는 수동형 RFID, 블루투스 장비, WiFi 기기와 같은 전자 기기를 소지한 개인을 트래킹할 수 있음은 널리 알려진 사실이다. 또한, 여전히 새로운 전자 기기들은 강한 프라이버시 보호 대책없이 소개되고 있는 실정이다. 산업계 및 연구 커뮤니티는 기존 기술의 프라이버시를 향상시킬 뿐만 아니라 미래의 기기의 프라이버시 문제를 더욱 잘 이해하고 해결해야 한다.

2.2 NIKE + IPOD 프로토콜

Nike+iPod 스포츠 키트는 사용자에게 아이팟 나노를 통해서 실시간으로 운동 진행 상황을 보고하고, 웹사이트 http://www.nike.com/nikeplus/에 그들의 정보를 온라인으로 게시할 수 있게 한다. Nike+iPod 스포츠 키트에 포함된 센서는 3.5cm × 2.5cm × 0.75cm 크기의 플라스틱 속에 내장된 장치이며, 수신기는 2.5cm × 2cm × 0.5cm 플라스틱 구조물에 내장된 장치이다. 사람이 달리거나 도보시, 센서는 iPod Nano의 존재와 별개로 센싱 데이터를 브로드캐스팅하기 시작한다. 사람이 10초 동안 멈출 때, 감지기는 sleep 상태에 놓이게 된다. iPod Nano가 운행 모드이고 수신기는 센서로부터 센싱 데이터를 수신할 때, 수신기는 센싱 데이터를 iPod Nano에 데이터를 중계할 것이다. iPod Nano는 운동중인 사람에게 피드백을 준다.

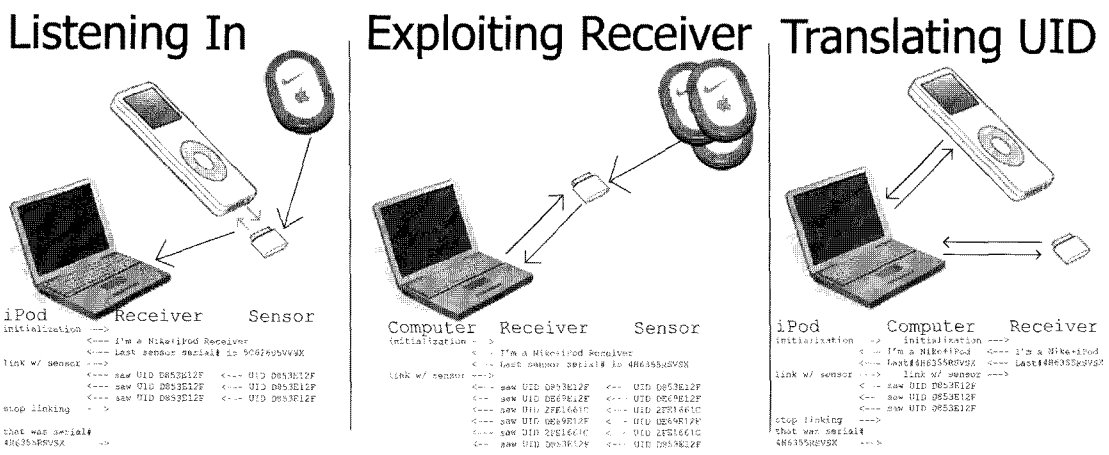


[그림 3] Nike+iPod 수신기

iPod 소프트웨어는 Basic, Time, Distance, Calories로 구성된 다양한 운동 모드를 제공한다. Basic 모드에서는 운동 중 듣고자 하는 음악을 선곡하고 운동 거리, 운동 속도, 소비된 열량을 모니터링할 수 있다. 사용자는 운동 중 언제든지 iPod의 중앙 버튼을 누르면, 헤드폰으로부터 운동 시작 후 경과 시간, 운동 거리, 운동 속도와 같은 음성 피드백을 들을 수 있다. Time, Distance, Calories 모드는 Basic 모드와 유사하다. 단지 각각의 모드에서는 사용자가 운동 목표 시간, 운동 거리, 목표 소비 열량을 설정할 수 있다. 운동 종료 후, 사용자는 iTunes을 이용하여 iPod와 웹사이트 Nike Plus.com을 동기화시켜서 운동 정보를 웹사이트로 전송한다. NikePlus.com는 사용자에게 그들의 운동 정보를 시각화하여 제공한다.

Nike+iPod 센서가 수신기는 다음과 같은 방법으로 서로 통신한다. Nike+iPod 설명서에 따르면, 센서와 수신기는 사용에 앞서 서로 연결(link)될 필요가 있다. 사용자가 직접 연결 과정을 수행해야 한다. 한번 연결되면, 수신기는 연결된 특정 센서로부터 데이터를 보고받고 다른 사용자의 센서로부터 수신 트래픽은 제거한다. 수신기는 마지막으로 연결된 센서를 기억하고 있으므로 사용자가 iPod를 동작시킬 때 마다 연결 단계를 수행할 필요는 없다. 또한 수신기는 나중에 다른 센서와 연결될 수도 있다. 표준 사용자 인터페이스를 적용할 경우, 수신기는 언제든지 하나의 센서와 연결될 수 있다.

하나의 센서는 동시에 2개의 수신기와 연결될 수 있다. 즉, 두 사람이 각자 iPod Nano를 소유하고, 동시에 단일 Nike+iPod 센서로부터 데이터를 판독하는 표준 사용자 인터페이스를 사용하는 경우를 의미한다. 센서

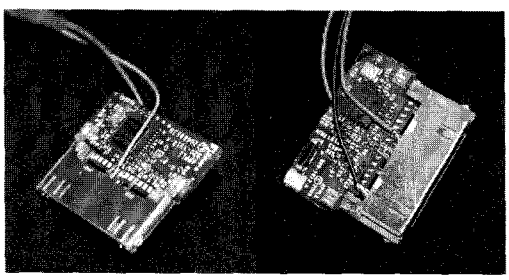


〔그림 4〕 좌측그림은 아이팟과 나이키+아이팟 수신기사이에 시리얼 통신을 수동적으로 모니터링하는 기법을 설명; 아이팟과 수신기간 통신은 시리얼 연결, 센서와 수신기간 통신은 무선통신. 중앙그림은 Nike+iPod 수신기 제어 접근 방법 설명; 컴퓨터와 수신기간 통신은 시리얼 연결. 우측그림은 센서 UID와 센서 시리얼 번호간 변환 방법 설명

는 전송 기능만 가지고 있다. 즉 센서는 어느 iPod(혹은 수신기)이 자신과 연결되어 있는지 알 수 없다. Nike+iPod 스포츠 키트에서는 센서와 수신기간의 강력한, 배타적 일대일 바인딩을 제공하지 않음을 보여주는 것이다.

하드웨어. Nike+iPod 수신기는 표준 iPod 커넥터를 통해서 iPod Nano와 통신한다. 수신기의 커넥터의 핀과 온라인 핀 설명서에 나와 있는 핀 구성을 비교함으로써, 이들간 통신이 시리얼 연결을 통해서 수행됨을 알 수 있다.

수신기의 흰색 플라스틱 케이스를 벗겨보면, iPod 커넥터에 연결되는 수신기의 컴포넌트 보드와 핀 구성을 볼 수 있다. 10개의 핀이 사용되고 있으며, 이중에서 접지(ground), iPod 전송(iTXD), iPod 수신(iRXD)을 담당하는 3개의 핀이 시리얼 통신에 사용된다(그림 3, 4 참조). iRXD와 접지선을 오실로스코프에 연결하면 시리얼 연결을 통한 디지털 신호의 전송 상태를 검증할 수 있다. 오실로스코프를 이용하면 비트 폭, 데이터 레이트(57,6 Kbps로 확인됨)을 측정할 수 있다. 수신기의 접지, iTXD, iRXD 신호선을 컴퓨터의 시리얼 포트에 납땜하여 연결하면, 수신기와 iPod 사이의 데이터를 도청할 수 있다.



〔그림 5〕 Nike+iPod 수신기

수신기를 iPod에 연결한 후, iPod를 구동시킨 상태에서, 시리얼 연결 상의 양방향 데이터를 도청할 수 있다. iPod에서 송출되는 신호를 분석하면, iPod의 기기 시리얼 번호가 ASCII 문자형태로 전송됨을 확인할 수 있다. 또한 수신기에서 송출되는 신호를 분석하면, 수신기의 시리얼 번호와 수신기에 마지막으로 연결된 센서의 시리얼 번호가 ASCII 문자형태로 전송됨을 확인할 수 있다.

시리얼 통신. 위에서 언급된 바와 같이, 수신기와 센서가 함께 사용하기 전에 센서는 수신기에 연결되어야 한다. 사용자는 iPod 인터페이스에서 제공되는 메뉴를 이용하여 상기 초기화를 수행한다. 사용자는 신발을 신은 상태로 걸어서 센서가 자신의 정보를 브로드캐스팅하면, 수신기는 센서를 인식하게 된다. 연결 단계가 시작될 때, iPod는 수신기에 어떤 데이터를 송출한다. 그리고 나면, 수신기는 새로운 센서가 발견되고, 수신기와 연결될 때까지 데이터 전송을 계속한다. 최종적으로, iPod은 수신기에 더 많은 정보를 돌려보낸다. iPod의 마지막 데이터에서 새로운 센서의 시리얼 번호가 ASCII 형태로 전송된다. 그림 5는 시리얼 통신을 표현하고 있다.

iPod 액세서리 시리얼 패킷 포맷은 3 바이트 헤더,

페이로드와 1 바이트 체크섬(checksum)으로 구성되어 있다. 헤더의 상위 2 바이트는 "FF55"이며, 하위 1 바이트는 페이로드의 길이를 바이트 수로 표현한다. 헤더의 "FF"와 "55" 바이트사이에 "00" 바이트가 추가되기도 한다.

여러 개의 다른 센서를 대상으로 링크단계의 트래픽을 분석해보면, 수신기로부터 나오는 어떤 패킷의 세번째 출현이후 연결단계는 완성되는 것을 알 수 있다. 상기 패킷의 페이로드는 4 바이트의 "090D0D01"로 시작한다. 다음 4 바이트는 센서에 따라 다른 데이터가 전송된다(예를 들어 "37625122"). 이러한 데이터를 센서마다 다른 고유의 식별 정보로 가정할 수 있다. iPod Nano 소프트웨어는 고유 식별정보를 링크단계후 수신기에 시리얼 번호를 돌려보내기 위해서, 센서의 ASCII 시리얼 번호와 맵핑한다. 상기 4 바이트 데이터는 센서의 UID이다.

Nike+iPod 스포츠 키트의 설명서에 따르면, 센서가 구동중일때도, 전원을 절약하기 위해서 sleeping 모드로 전환되기도 한다. 사용자가 걷기시작하면, 센서는 데이터 전송을 시작한다. 또한 신발 속에 센서를 넣지 않더라도 센서의 데이터 전송을 시작시킬 수 있다. 예를 들어, 판매점에서 봉인된 채로 팔리지 않은 패키지라도 흔들면, 패키지 속의 센서는 UID를 전송하기 시작한다. 또한 센서를 딱딱한 표면에 톡톡 치거나, 급격하게 흔들면 센서는 동작을 시작한다. 센서는 바지주머니, 가방, 지갑 등에 있다면, 때때로 깨어날 것이다. 걷거나, 달리거나, 흔드는 것을 중단하면, 센서는 대략 10초 후에 sleep 모드로 진행된다.

센서가 깨어있을 때, 센서는 UID를 포함하여 매초에 1개의 패킷을 전송한다. 센서가 멀어지거나 길모퉁이에 있을 때, 수신기는 간헐적으로 패킷을 수신하게 된다. 여러 개의 센서가 서로 인접하여 위치할 때, 어떤 패킷은 변조되어 오류를 일으킨다(체크섬이 일치하지 않음). 깨어있는 센서가 증가할 때, 변조되는 패킷의 개수가 증가한다. 그러나 7개의 센서를 이용한 실험에서는 수신기가 모든 센서의 UID를 적어도 10초에 한번 꼴로 청취 가능하였다.

그림 4에서 보여준 Nike+iPod 수신기의 컴포넌트를 조사하면, Nike+iPod 스포츠 키트는 ANT 무선 라디오 프로토콜을 사용하고 있음을 짐작할 수 있다. ANT 라디오는 1-30 미터 범위의 전송 거리를 가진다[1]. Nike+iPod 센서의 실험에서 10미터 실내에서, 10-20 미터 실외 동작범위를 관찰할 수 있다. 또한 센서는 빠르게 이동하더라도 탐지가 가능하다. 대략 10 MPH 속도로 달리면, 센서는 신뢰할 정도로 수신이 가능하다. 신발에 센서를 장착하고 걸으면, 30 MPH 속도에서도 관찰될 수 있다.

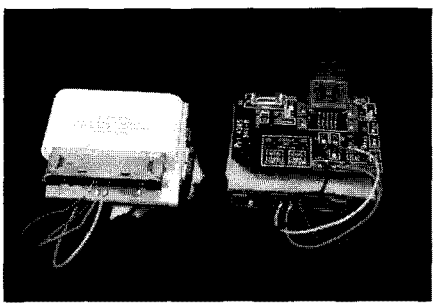
아이팟에 장착된 수신기와 통신하는 센서를 부착하고 있다면, 상기 수신기이외 다른 수신기도 UID를 브로드캐스팅하는 센서를 감지할 수 있다. 이러한 상황은 센서는 단지 정보만 전송할 뿐, 수신 기능은 없다는 점에서 자연스러운 것이다.

Ⅲ. 모바일 USN에서의 공격 도구

본 절에서는 Nike+iPod 스포츠 키트를 사용하는 사람에 대해서, 공격을 위해 필요한 도구를 어떻게 만들 수 있는지 자세히 소개한다.

3.1 Nike+iPod receiver to USB adaptor

Nike+iPod 센서 UID를 검출하기 위한 소형 USB 수신기 모듈을 제작할 수 있다. USB 수신기 모듈의 제작에서는 Nike+iPod 수신기의 변경이 필요하지 않으며, USB 모듈은 iPod 암커넥터와 FTDI FT2232C 칩셋 내장 serial-to-USB 보드로 구성된다.(그림 6 참조). iPod 커넥터의 3개의 시리얼 핀과 3.3V 전원 핀을 FT2232C에 적절한 핀에 연결하기만 하면된다. 상기 USB 모듈이 USB 포트를 통해서 컴퓨터와 연결될 때, 수신기는 전원이 들어오고, 컴퓨터 소프트웨어와 수신기간의 통신을 위한 USB 시리얼 포트가 사용 가능해진다. 패키지 크기는 수신기를 포함하여 3cm × 3cm × 2cm 길이정도 된다.



[그림 6] Nike+iPod receiver to USB adaptor

3.2 Nike+iPod Serial Communication Tool

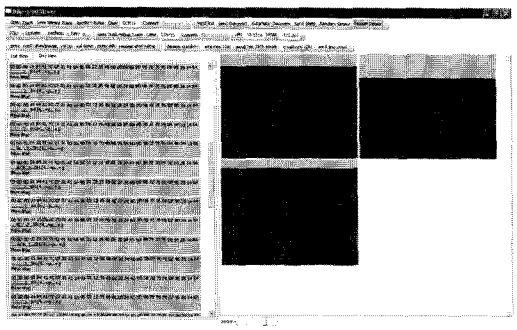
Nike+iPod 시리얼 통신 툴은 2개 시리얼 포트에 대한 동시 트래픽 로깅, Nike+iPod 수신기 초기화, 링크 커맨드 송신, Nike+iPod 수신기 시리얼 데이터의 패킷 로깅(checksum 포함), 동작중인 센서와 동작 시간 로깅 기능을 제공한다(그림 7 참조). 여러 개의 시리얼 포트상의 트래픽 로그가 중첩되면서 iPod과 수신기사이의 프로토콜 및 교환되는 데이터를 엿들을 수 있다.

Nike+iPod 시리얼 통신 툴은 2개의 시리얼 포트까지 헥사타입으로 송수신되는 바이너리 데이터, 패킷의 헥사 및 ASCII 표현, 동작중인 센서 구분, 센서로부터 도착한 새 패킷의 시점에 대한 그래픽 인터페이스를 제공한다. 화면 인터페이스는 UID로 표시되는 검출 센서, 센서의 검출 시간을 담고 있는 청색 사각박스로 구성된다. 센서가 감지될 때마다 사각박스는 적색으로 표시되고, 서서히 청색으로 표시된다. 이를 통해서 어떤 센서가 감청 범위 내에서 깨어있고, 얼마나 많은 패킷이 도착하는지 파악할 수 있다. 또한 Nike+iPod 시리얼 통신 툴은 UID, 사진, 시간정보, 위도, 경도를 포함하는 센서 이벤트를 SQL 서버에 업로드할 수 있다.

Nike+iPod 시리얼 통신 툴은 사용자에게 SMS 혹은 이메일을 이용하여 센싱 정보를 전달할 수 있다. 마이크로소프트 윈도우 XP 혹은 그 이후 버전을 위한 마이크로소프트 .Net 3.0 상에서 실행되며, C#과 XAML로 대략 2000 라인으로 구현될 수 있다.

3.3 Intel Motes

인텔의 iMote2를 이용하여 Nike+iPod 센서에 대한 로깅 및 트래킹을 제공하는 임베디드 모듈을 개발할 수 있다. 임베디드 모듈은 iMote2, Nike+iPod 수신기, iPod 암커넥터, 블루투스 기능이 탑재된 iMote2 유틸리티 보드로 구성된다. 모듈의 조립 패키지의 크기는 5cm × 3.8cm × 2.5 cm 크기, 무게는 2.3온스이며, 2GB의 미니 SD 카드를 포함한다.

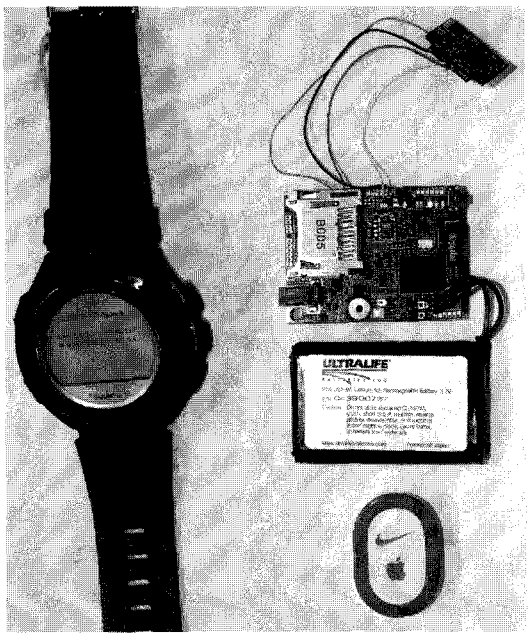


(그림 7) Nike+iPod Serial Communication Tool

iMote2 리눅스 운영체제에서 동작하며, 공격 소프트웨어는 C 언어로 구현된다. iMote2는 시리얼 포트로 Nike+iPod 수신기와 통신한다. 부팅시, iMote2는 초기화 및 링크 명령을 수신기에 송신하며, 센서 관련 이벤트를 파일에 로깅하기 시작한다. 선택적으로, 소프트웨어는 iMote2가 센서를 발견할 때, LED를 On시킬 수 있다. 타켓 센서 목록은 구성 파일에 명시되어 있다. LED 기반의 알람은 목표물의 센서가 근접하고 있다는 시각적인 신호로 사용되는 구체적인 방법일 것이다. LED이외에도 부저와 같은 오디오 장치, 진동기와 같은 물리적 장치를 이용할 수도 있다.

iMote2는 블루투스 기반으로 센서의 UID를 마이크로소프트의 SPOT 손목시계와 통신하도록 구성할 수 있다. 공격자는 상기 iMote2와 수신기를 자신의 배낭, 주머니, 핸드백 등에 넣고, 손목시계에 있는 근접한 센서에 대한 정보를 지속적으로 모니터할 수 있다(그림 8 참조).

파일에 로그된 센서 이벤트는 시리얼 통신 툴으로부터 수집된 센서 정보의 취합을 위해서 수동으로 중앙



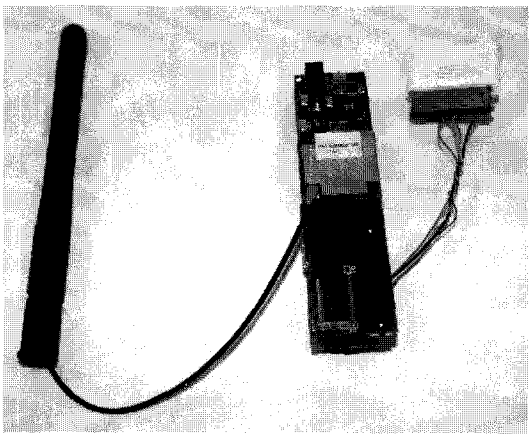
(그림 8) 마이크로소프트 SPOT 손목시계와 iMote2

서버에 업로드될 수 있다. 상기 장치에 대한 확장으로 iMote2가 블루투스 GPS 센서로부터 실시간 위치 정보를 수집하게 할 수 있다. 이것은 공격자로 하여금 공격자가 이동중일 때도 정확한 센서 위치 정보를 수집할 수 있게 한다. 다른 확장 방법으로는 다수의 iMote2 노드로 구성된 대규모의 분산 감시 센서 네트워크를 만들어서, 중앙의 SQL 서버에 실시간으로 감시 데이터를 업로드할 수 있다.

3.4 Gumstixs

리눅스 기반의 gumstix 컴퓨터를 이용하여 저렴한 비용으로 Nike+iPod 감시 장치를 개발할 수 있다. 본 장치 모듈은 $29의 Nike+iPod 수신기 1대, $109의 gumstix connex 200xm 마더보드, $79의 wifistix, $27.50 gumstix breakout 보드, $2.95의 iPod 암커넥터로 구성된다. 조립된 모듈의 크기는 8cm × 2.1cm × 1.3cm이며, 무게는 1.1 온스이다(그림 9 참조).

Gumstix 기반 감시 모듈은 다음 두 가지 사항을 제외하고는 iMote2에서 실행되는 것과 동일한 감시 소프트웨어를 사용한다. 1) gumstix 모듈에서 운용되는 소프트웨어는 중앙 백-엔드 서버로 실시간 감시 데이터를 무선으로 전송하기 위해 WiFi를 사용한다. (2) gumstix 기반 감시 모듈은 마이크로소프트의 SPOT 손목시계를 필요로 하지 않는다. 실시간 리포팅 기능은 gumstix 모듈을 더 큰 규모의 실시간 감시 시스템의 일부분으로 만들어 준다. 만약 공격자가 실시간 리포팅 기능을 필요로 하지 않는다면, 공격자는 전체 모듈에서 wifistix 부품을 빼고 제작하면 모듈 비용을 절감할 수 있다.



(그림 9) Gumstix 기반 Nike+iPod 감시 장비(WiFi 무선 기능 탑재)

3.5 기존 iPod 활용

기존이 iPd을 사용하고, iPod에 연결되는 하드웨어를 간단히 수정하면, Nike+iPod 센서에서 송출되는 센서 데이터를 감시할 수 있다. 3세대 iPod에 iPod 리눅스를 설치하기 위해서 데스크탑 컴퓨터를 사용한다. iPod 리눅스 툴체인을 사용하여 iMote2 로깅 소프트웨어를 재컴파일한다. 유일한 하드웨어 수정은 iPod 상단에 위치한 원격 제어 포트의 시리얼 송수신 라인을 도크(dock) 커넥터의 iPod 하단 시리얼 포트와 연결시키는 것이다. breakout 보드를 이용하여 iPod와 Nike+iPod 수신기를 연결한다.

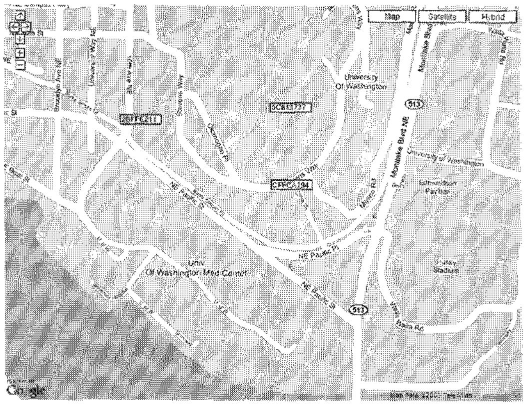
iPod에 Nike+iPod 수신기와 iPod에 플러긴된 Pod 리눅스 애플리케이션을 실행하면 iPod 화면에 어떤 센서가 근접해 있는지 표시할 수 있고 중앙 서버와의 동기작업을 위해 iPod의 하드드라이브에 센서 이벤트(UID, 타임스템프)를 저장할 수 있다. 이러한 기능은 공격자가 3세대 이전 iPod 기기를 감시 장비로 활용할 수 있음을 의미한다. 이전 버전의 iPod은 이베이 등에서 할인된 가격으로 구입가능하다. 택스트-음성 변환 소프트웨어를 사용하면, 어떤 Nike+iPod 센서 혹은 어떤 사람이 근접했는지를 iPod에 연결된 헤드폰을 이용하여 음성으로 알릴 수 있다.

만약 iPod 리눅스 커뮤너티는 3세대 iPod의 도크 커넥터에서 시리얼 포트를 사용하는 방법을 찾는다면, 공격자는 하드웨어 변경없이 Nike+iPod 센서를 추적할 수 있다.

3.6 분산 감시 시스템

구글맵스 기반의 웹 애플리케이션은 여러 장소에서 수신된 센서 정보를 수집하는 강력한 기능을 보여준다. 웹 애플리케이션은 여러 데이터 소스로부터 중앙 SQL 서버로 업로드되는 센서 이벤트를 웹사이트에 시각적으로 디스플레이한다. 데이터 소스로는 시리얼 통신 툴, iMote2 애플리케이션, gumstix 애플리케이션, iPod 리눅스 애플리케이션이 있다.

그림 10와 같이, 웹 애플리케이션은 센서 발견 위치에 해당하는 구글맵스 지도상에 센서의 UID를 실시간으로 출력한다. 센서가 더 이상 존재하지 않으면, UID



〔그림 10〕 구글맵스 기반 감시 웹 애플리케이션

는 사라진다. 또한, UID 대신에 랩탑 컴퓨터로 촬영한 디지털 사진을 업로드할 수 있다. 또한 웹 애플리케이션은 사용자에게 열람하고자 하는 감시 시간대를 지정하게 하여, 지정된 시간대에 기록된 모든 센서 정보를 열람할 수 있게 한다.

공격자는 구글맵스 기반 감시 웹 애플리케이션을 이용하여 사람들의 동선 패턴을 구축할 수 있다. 만약 Nike+iPod 수신 장비를 갖춘 다수의 공격자들이 협력한다면, 감시 소프트웨어와 웹 사이트만으로 센서를 소지한 다수의 사람들을 추적할 수 있게 된다.

Ⅳ. 모바일 USN에서의 공격 유형

본 절에서는 모바일 USN 서비스의 대표적 상품인 나이키+아이팟 스포츠 키트에서 발생가능 한 다양한 공격 형태를 소개하고자 한다. 또한 공격 도구들이 특정 감시 및 공격 애플리케이션에 어떻게 사용되는지를 기술한다. 이후, 공격 도구로 사용되는 시리얼 통신 툴 운용 랩탑 컴퓨터, iMote2, gumstix, 3세대 iPod을 Nike+iPod 디텍터(detector)로 통칭한다.

• 남자친구의 의심

마빈은 여자 친구인 앨리스가 자신의 절친한 친구인 밥과 외도를 하고 있다고 생각하는 질투심이 많은 남자친구라고 하자. 앨리스는 Nike+신발을 신으며, Nike+iPod 스포츠 키트를 사용한다. 마빈은 앨리스의 신발에 있는 Nike+iPod 센서의 UID를 알고 있다. 예를 들어, Nike+iPod 디텍터앞에 앨리스의 신발을 흔들거나, 앨리스가 그의 차로 걸어올 때 Nike+iPod 디텍터를 작동시키면, 센서의 UID는 쉽게 취득할 수 있다. 마빈은 앨리스가 눈치채지 못하게 앨리스의 신발 한쪽에 Nike+iPod 센서를 숨겨둘 수도 있다. 아니면, 앨리스의 자켓이나 핸드백에 센서를 숨길 수도 있다. 만약 마빈이 밥의 집 근처에 Nike+iPod 디텍터를 숨겨 놓으면, 그는 앨리스가 밥과 만나는지, 얼마나 오래 함께 시간을 보내는지를 유추할 수 있다. 이런 경우는 감시 시스템의 풀 세트를 사용하는 대신, 단지 시리얼 통신 툴을 탑재한 윈도우 XP 랩탑 컴퓨터, 인텔 모트, gumstix, 혹은 3세대 iPod만으로 공격이 가능한 공격 유형이다. 만약 마빈은 밥이 Nike+신발을 신고 다니며, 밥의 Nike+iPod 센서의 UID를 알고 있다면, 그는 앨리스의 집 근처에 Nike+iPod 디텍터를 몰래 숨겨 둘 수 있다. 결국 마빈은 밥이 얼마나 자주 앨리스의 집을 방문하는지 유추할 수 있게 된다. 또한 마빈은 앨리스가 새로운 조깅 파트너를 찾고 있는지 추론하기 위해서 그녀의 예상 조깅 경로에 Nike+iPod 센서를 숨겨 둘 수도 있다. 이러한 공격들은 앨리스의 사생활을 침해하는 수단이 될 것이다.

• 옛 남자친구의 미행

만약 둘 사이가 나빠져서, 앨리스가 헤어지기를 선택했다고 가정한다. 그러나 마빈은 이별을 받아들이지 못하고, 앨리스와 우연히 만날 방법을 찾고 있다고 가정한다. 앨리스를 추적하기 위해서, 그는 분산 감시 시스템을 사용하고자 한다. 그는 도서관, 기숙사, 학생회관과 같은 캠퍼스 내의 중요 장소와 앨리스의 일터, 집과 같은 캠퍼스외의 장소에 Nike+iPod 디텍터를 설치한다. 구글맵스 기반의 웹사이트를 통해서, 마빈은 앨리스가 머물렀던 장소를 파악할 수 있다. 마빈은 우연을 가장해서 특정 장소에서 앨리스와 우연히 마주친 척할 수 있다. 구글맵스 기반 웹사이트에서 그녀의 위치를 찾는 방법외에 감시 시스템이 앨리스가 감시 지역내로 들어올 경우 그에게 이메일이나 SMS 문자메시지를 송출하게 할 수 있다. 마빈은 앨리스 주변에 항상 있는 Nike+iPod 센서의 UID를 수집하기 위해서 구글맵스 기반 감시 시스템을 사용할 수 있다. 앨리스가 만나는 사람들에 대한 정보를 취득할 수도 있다. 마빈은 감시 시스템의 기능을 이용하여 지도에 이동 경로를 표시하여 앨리스의 일상 스케줄에 대해 좀 더 자세하게 구체적으로 파악할 수 있다.

• 전문 절도범

특정인을 목표로 하는 마빈과 달리, 전문 절도범은 특정시간대에 집을 비우는 어떤 사람을 타켓으로 삼는다. 범인은 절도의 대상이 될 집을 물색해야 하며, 이런 일은 많은 시간이 필요하며, 타인의 눈에 잘 띌 수 있다. 불행하게도, Nike+iPod 기반의 분산 감시 시스템은 전문 절도범으로 하여금 동시에 많은 사람들을 모니터링 할 수 있게 한다.

• 비윤리적 조직

윤리적이지 못한 조직이 조직내의 구성원을 추적하거나 경쟁조직의 구성원을 추적하기 위해서 분산 Nike+iPod 기반 감시 시스템을 사용할 수 있다. 전자의 경우, 조직이 자신의 구성원이 다른 조직의 이벤트, 사무실에 출입하는지 조사하기 위해서 Nike+iPod 기반 감시 시스템을 사용하는 것이다. 후자의 예를 들자면, 많은 사설탐정을 고용하기보다는 경쟁자의 가정에 Nike+iPod 디텍터를 은밀히 설치한다. 이렇게 함으로써, 비윤리적 조직은 저렴한 비용으로 기초적인 감시 단계를 수행한 후 의심되는 인물을 추려서, 이들을 조사할 한 두 명의 사설탐정을 고용하면 된다.

• 고객 트래킹

회사는 그들의 매장을 방문하는 고객을 트래킹하기 위해 Nike+iPod 센서를 사용할 수 있다. 예를 들어, 상점은 고객의 Nike+iPod 센서 UID와 고객의 구매 이력 사이의 연관 관계를 만들 수 있다. 고객이 다음에 매장을 방문하면, 점원은 즉시, 고객의 소비취향을 파악하여 그에 따른 판매 전략을 구사한다. 상품에 RFID 태그를 삽입하고 고객이 소지한 물품을 은밀히 관찰함으로써, 고객의 사생활을 침해하는 사례들도 있다 [3, 4].

• 강도

iPod Nano는 절도의 매력적인 대상이며, iPod Nano의 소유자는 다른 매력적인 물품을 가지고 있을 수 있기 때문에, 강도들은 잠재적 범행 대상이 iPod Nano을 소지하고 있는지 파악할 필요가 있다. 실제로도 맨하탄에서 iPod 소유자를 목표로 하는 일련의 절도사건으로 인하여 뉴욕 대학생들은 iPod에 사용되는 흰색의 이어버드(ear-bud)를 착용하지 말도록 권유받았었다[2, 5]. 그 사람이 이어버드를 착용하지 않더라도, 강도는 Nike+iPod 디텍터를 이용하여 iPod의 소유 유무를 파악할 수 있다. 만약 사람이 Nike+iPod 센서가 장착된 신발을 신고 있다면, iPod를 사용하고 있지 않더라도 기기의 소지 유무는 파악될 수 있기 때문이다. 강도는 Nike+iPod 센서가 근처에 있는지 파악하기 위해서 Nike+iPod 디텍터를 사용한다. 만약 근처에 많은 사람들이 있다면, 강도는 방향 안테나를 사용함으로써, 특정 범죄 대상의 위치를 파악할 수 있다.

Nike+iPod 디텍터와 같은 도구를 이용한 공격 방식는 대부분의 강도들의 기술적 능력 밖이라고 하지만, 다음과 같은 이유로 우리는 동의할 수 없다. 첫째로, 강도범은 번거롭더라도 Nike+iPod 센서가 근처에 있는지 파악하기 위해서, 표준 iPod Nano, 표준 Nike+iPod 수신기, 표준 사용자 인터페이스, 링크 프로세스를 이용하여 상기 공격의 조잡한 버전을 실제로 만들 수 있다. 둘째로, 누군가가 인터넷에 공격 소프트웨어를 만들어 게시한다면 최소한의 기술적 지식만으로도 자동화된 공격 방법을 사용할 수 있다. 게다가, 범죄 조직은 상기 공격을 수행하기 위해서 공격 기술을 보유한 최소한의 기술자를 필요로 하거나 그러한 공격기능을 가진 도구만 구입하면, 모든 공격은 가능하다. 결국, 강한 프라이버시 보호 기능을 갖추지 않은, Nike+iPod과 같은 기기들이 범람할 때, 탐지 기술을 사용하는 범죄의 유혹을 증가시킬 수 있다.

• 트래킹 기술의 접목

Nike+iPod 기반 감시 기술과 다른 기술을 접목할 경우, 사람들에 대한 더욱 자세한 프로파일을 생성하여 프라이버시를 손상시킬 수 있다. 예를 들어, 우리는 블루투스 기기를 프로토타입 감시 시스템과 접목시킨다. Nike+iPod 센서와 블루투스 기기를 결합함으로써, 비록 개인 휴대 기기를 소지한 사람들에 한해서 가능하더라도 공격자는 개개인의 일상생활을 추적 할 수 있다. 아마도, 더욱 나쁜 경우는 블루투스 기기들이 Nike+iPod 센서에 의미있는 이름을 부여하는 것이다. 센서가 감청범위 내에 진입할 때, 사진 촬영을 한다. 그리고 나서 안면, 걸음걸이 혹은 면허증 인식 기술과 같은 정교한 컴퓨터 비젼 기술을 활용하여 촬영된 사진으로부터 정보를 추출한다. 공격자는 이러한 정보를 이용하여 개인에 대한 폭넓은 프로파일을 만들 수 있다. 만약 공격자가 공격 도구를 범죄 대상에게 충분히 근접시킨다면,

그는 Nike+iPod 센서 데이터와 개인의 RFID 신용 카드 정보[6], 여권 정보[7] 혹은 도서관 서고정보[8]를 연결시킬 수 있다.

V. 모바일 USN 보안 서비스 방안

RFID 태그와 블루투스 장비와 관련한 프라이버시에 대해 공공의 광범위한 인식에도 불구하고, 또한 산업계에서 불추적성의 중요성을 인식하고 있음에도 불구하고, 아직도 유명 회사들조차도 강한 프라이버시 보호 대책이 없이 새로운 기술 및 상품들을 출시하고 있다. 많은 경우에 고객의 프라이버시를 기술적으로 크게 향상시키는 것이 가능함에도 불구하고, 강한 프라이버시 보호 대책이 보장되지 못하는 현실이 우려스럽다.

본 절에서는 모바일 USN 서비스의 대표적 상품인 Nike+iPod 스포츠 키트에 적용 가능한 보안 방법을 소개하고, 그 의미를 살펴본다.

5.1 암호시스템 적용

Nike+iPod 스포츠 키트에 대한 전형적인 사용 시나리오를 생각해보자. 일반적인 경우에, 사용자가 Nike+iPod 스포츠 키트를 구입할 때, 구입한 키트의 센서와 다른 키트의 수신기와 함께 사용하지 않는다. 이것은 공장의 생산단계에서 센서와 수신기는 비밀하게 공유된 암호키로 프로그램된다는 의미한다. 프로그램된 비밀키로 브로트캐스팅 메시지를 암호화함으로써, Nike+iPod 설계자는 Nike+iPod 응용 프로토콜과 관련된 대부분의 프라이버시 문제를 해결할 수 있다. 물론 여전히 하부 하드웨어를 통한 정보 유출 가능성은 존재한다. 만약 애플과 나이키에서 하나의 센서는 다른 키트의 수신기와 함께 사용되게 설계한다면 암호화 키 설정방법이 필요하다. 예를 들어, 서로 다른 키트의 센서와 수신기를 사용하고자 하는 경우는 극히 드문 것이며, 암호키가 센서의 뒷면에 인쇄되어 있을 수 있고, 사용자는 새로운 센서를 사용하기 전에 암호키를 iPod에 직접 입력할 수 있다. 또한 센서는 특별한 버튼을 가지고 있을 수 있다. 즉, 버튼을 누르면, 센서는 짧은 시간동안 암호키를 브로트캐스팅한다.

좀 더 세부적으로 기술을 살펴보면, 키트의 센서와 수신기는 128비트 암호키 K로 사전 프로그램 되어 있다. 센서는 브로드캐스팅중 새로운 난수인 128비트 X를 재생성한다. 이때, X는 공유되지 않은 128비트 AES 키 K'로 AES-CTR을 사용하여 생성되기를 권고한다. 센서는 초기카운터 X와 공유키 K로 AES-CTR을 사용하여 키스트림 S를 사전 생성한다. 최종적으로 센서는 특정 수신기에 메시지 M을 전송하기를 원할 때, 센서는 (X,M⊙S)를 계산하여 전송한다. "⊙"는 배타적 or(exclusive-or) 연산을 의미한다. 수신기는 메시지 (X, Y)를 수신하면, X와 K로부터 S를 생성하고, Y⊙S을 연산하여 M을 복원한다. 수신기는 메시지 M에서 해당 UID를 포함하면 M을 인가된 센서로부터 수신한 메시지로 수락한다. 이러한 방법은 도청과 같은 수동적인 공격에 대해 애플리케이션 수준에서 프라이버시를 제공하는 간단한 기법이다. 해킹과 같은 능동적 공격에 대해서는 모든 보안 요구사항을 만족시키지는 못할 것이다. 상기 접근 방식은 최적화될 것이지만, 배터리 수명, 제조단가, Nike+iPod 스포츠 키트의 사용편리성에 영향을 줄 것이다. 그럼에도 불구하고, 상기 기법은 현재의 Nike+iPod 스포츠 키트의 프라이버시에 대한 안전성을 향상시켜 줄 것이다.

5.2 On-Off 스위치

Nike+iPod 스포츠 키트 센서와 같은 모든 모바일 개인 기기에서 on-off 스위치를 장착하는 것이 충분한 프라이버시 보호 대책이 될 수 있는지에 대한 질문이 제기되고 있다. On-Off 스위치 적용은 몇 가지 이유로 프라이버시 보호에 충분한 대책이 될 수 없다. 첫째로, On-Off 스위치는 기기가 동작중일 때는 고객의 프라이버시를 보호하지 못한다. 둘째, 대부분의 사용자들은 사용하지 않을 경우에도 기기를 끄지 않는다. 특히 소유하고 있는 개인기기의 수가 증가할수록 더욱 그러하다. Nike+iPod 온라인 설명서에 따르면, "대부분의 Nike+iPod 사용자들은 Nike+신발에 센서를 삽입한 후 그 존재를 망각한 채로 지낸다.[9]"라는 문구가 들어있다. 즉, 애플과 나이키는 이미 단순함(on-off 스위치를 사용안함)과 비용(동작중이지 않을 때 배터리 전원을 소모하지 않음)사이의 선택의 기로에서 고객은 단순함을 선택한다는 점을 인지하고 있다. 불행이도 이러한 권고사항을 만들고 따르는 것에도 프라이버시와 개인 안전 측면보다 단순함을 선호한다.

VI. 결론

RFID/USN 기술은 유비쿼터스 시대를 열어갈 최첨단 미래 기술로서 각광을 받고 있다. 특히, 모바일 USN, 모바일 RFID 기술을 채용하는 다양한 서비스 및 개인 휴대 기기는 사람들의 일상생활 공간에서 점차 보편화되고 있다. 그러나, 상기 기기의 라디오 신호 출력은 주의 깊이 설계되지 않는다면, 예기치 않은 사생활 문제를 야기할 수 있다. 본 고에서는 모바일 USN 서비스를 구현하는 상용제품인 Nike+iPod 스포츠 키트의 보안 위협 및 대응 보안 기술에 대해서 살펴보았다.

잠재적 프라이버시 문제에 대한 그동안의 일반의 관심과 연구 및 산업계의 이전 논란에도 불구하고, 제조사들은 강한 프라이버시 보호하지 못하는 제품들을 계속해서 출시하고 있다. Nike+iPod 스포츠 키트와 같은 전자기기의 프라이버시 문제는 개인 안전에 대한 위협을 포함하는 심각한 결과를 초래할 수 있다. 향후 지속적으로 산업 및 연구 관련자들은 고객의 프라이버시 보호를 위한 대책을 마련해야 한다.

참고문헌

[1] ANT comparison sheet. http://www.thisisant.com/index.php?section=36.

[2] AppleInsider. NYU Warns Students Against Wearing iPod Earbuds, 2005. http://www.appleinsider.com/article.php?id=930.

[3] A. McCue. Privacy Groups Protest RFID Tagging of Razors, ZDNet.co.uk, 2003. http://news.zdnet.co.uk/emergingtech/0,1000000183, 39115718,00.htm.

[4] A. Gilbert. 'ecret'RFID test draws consumer ire, ZDNet.co.uk, 2003. http://news.zdnet.co.uk/emergingtech/0,1000000183,39117924,00.htm.

[5] gothamist. Gang of iPod Thieves Arrested, 2005. http://www.gothamist.com/archives/2005/09/09/gang of ipod thieves arrested.php.

[6] T. S. Heydt-Benjamin, D. V. Bailey, K. Fu, A. Juels, and T. O'are. Vulnerabilities in first-generation RFID-enabled credit cards, 2006. Manuscript.

[7] A. Juels, D. Molnar, and D. Wagner. Security and privacy issues in e-passports. In IEEE SecureComm, 2005.

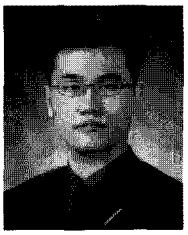
[8] D. Molnar and D. Wagner. Privacy and security in library RFID issues, practices, and architectures. In 11th ACM Conference on Computer and Communications Security (CCS 2004), 2004.

[9] Nike + iPod Frequently Asked Questions (Technical). http://docs.info.apple.com/article.html?artnum=303934.

[10] T. Scott Saponas, Jonathan Lester, Carl Hartung, Tadayoshi Kohno, Devices That Tell On You: The Nike+iPod Sport Kit, November 30, 2006.

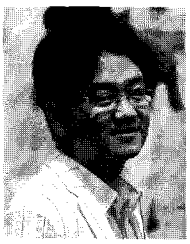
〈著者紹介〉

이 해 동 (Haedong Lee)
1999년 : 경북대학교 컴퓨터과학과 졸업
2001년 : 경북대학교 컴퓨터과학과 석사
2001년~현재 : 한국전자통신연구원 정보보호연구본부 선임연구원
관심분야 : 정보보호, RFID/USN, 암호 하드웨어 설계



박 남 제 (Namje Park)
종신회원
2000년 : 동국대학교 정보산업학과 졸업
2003년 : 성균관대학교 정보보호학과 석사
2008년 : 성균관대학교 컴퓨터공학과 박사
2003년 04월~현재 : 한국전자통신연구원 정보보호연구본부 선임연구원
현재) 관세청 사이버밀수단속 세관원
한국산업기술평가원 평가위원
지식경제부 핵심애로기술지원 기술 지도전문가
한국정보통신인력개발센터 자격검정 전문위원
모바일RFID포럼 표준분과위원, 정보보호분과 간사

미국인명연구소(ABI) 자문연구위원회 전문위원
영국캠브리지국제인명센터(IBC) Vice President
한국인터넷정보학회 편집위원
ITU-T SG17 Q.9 Co-Editor
한국과학기술자네트워크(KOSEN) 전문위원
관심분야 : 정보보호, 암호이론, 모바일 컴퓨팅, 센서네트워크



최 두 호 (Dooho Choi)
정회원

1994년 2월: 성균관대학교 수학과 졸업
1996년 2월 : 한국과학기술원 수학과 석사
2002년 2월 : 한국과학기술원 수학과 박사
2002년~2007년 : 한국전자통신연원 선임연구원, 팀장
2006년 09월~현재 : ITU-T X.1171(X.nidsec-1) 에디터
관심분야 : 정보보호, 암호이론, RFID/USN, 위상수학

정 교 일 (Kyoil Chung)
종신회원

1981년 한양대학교 전자공학과 졸업
1983년 한양대학교 전자공학과 석사
1997년 한양대학교 전자공학과 박사
1982년-현재 한국전자통신연구원 책임연구원, 마케팅기술위원
현재) 국가정보원 정보보호시스템 인증위원
ITU-T(국제전기통신연합) SG17 연구위원
TTA(한국정보통신기술협회) 국제표준화전문가
한국전자지불산업협회 IC카드포럼 의장
Asia IC Forum 표준화위원장
행정자치부 전자주민증 자문위원
ISO TC215 전문위원
TTA(한국정보통신기술협회) TC1 의장
IC카드연구센터 전자여권표준기술 개발단 단장
모바일RFID포럼 정보보호분과위원장
홈네트워크시큐리티포럼 의장
대검찰청 디지털수사 자문위원
대한전자공학회 상임이사
한국정보보호학회 부회장
한국디지털포렌식학회 부회장
한국인터넷정보학회 이사
관심분야 : 정보보호, Biometrics, 국가기반보호, 신호처리