웨어러블 컴퓨팅 시대의 정보보호 위협

서두옥
Clickseo Insight 대표이사
clickseo@gmail.com
이동호
광운대학교 컴퓨터소프트웨어학과 교수

1. 서론

사물인터넷(Internet of Things: IoT)은 사물에 센서 등을 부착하여 데이터를 수집하고, 수집된 정보를 실시간으로 유무선 통신망을 통해 서로 주고 받는 기술이나 환경을 말한다. 즉, 사람의 도움 없이 정보를 주고 받는 것으로 사물지능통신(Machine-To-Machine: M2M)이 확장된 개념이다. 웨어러블 컴퓨팅(Wearable Computing)은 컴퓨팅이 가능한 기기를 몸이나 의류 등에 PC 기능을 부착하여 사용하는 컴퓨팅 환경으로, 웨어러블 기기 간에 통신이 일어날 경우 사물인터넷의 범주로 볼 수 있다. 이처럼 초고밀도 집적회로(Very Large Scale Integration: VLSI)와 정보통신기술(Information and Communication Technology: ICT)의 발전으로 소형 경량화를 더더욱 발전시켜 컴퓨팅 기기의 크기를 몸에 부착할 정도로 작고 편리하게 만들었으며, 이러한 기기들 간의 통신을 통해 정보를 주고 받을 수 있는 환경을 만들어 주고 있다. 사물인터넷이 활성화 되면 수 많은 사물들이 서로를 스스로 식별하고 인식하여 상호간 정보교환을 통해 우리의 삶을 편하게 해줄 수 있는 다양한 서비스 제공이 가능하다[1]. 최근 가장 주목 받는 정보통신기술로 웨어러블 디바이스는 신체에 착용하여 이동 중에도 편리하게 사용할 수 있도록 제작된 것으로 소형화 및 경량화하여 의복 등의 일부분으로 신체에 착용할 수 있도록 제작되었다. 이러한 웨어러블 디바이

* 본 내용과 관련된 사항은 Clickseo Insight 서두옥 대표이사 (☎ 02-940-5216)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP 의 공식적인 입장이 아님을 밝힙니다.

Samsung Gear S

LG G Watch R

Smarth Ring

Jawbone Up

<자료>: 인터넷 참조

(그림 1) 머리부터 발끝까지... 그 밖의 다양한 웨어러블 제품들

스는 피트니스(Fitness)와 웰빙(Well-Being), 헬스케어(Health Care) 및 의료 분야 그리고 제조업 및 군사장비 등 다양한 산업 분야에 적용 가능하다.

특히, 웨어러블 컴퓨팅은 의료 및 U-헬스케어 분야와 결합될 경우 환자의 몸 상태에 대한 빠른 측정을 통해 신속한 진료를 가능하게 하고, 몸이 불편한 노인들이나 아이들에게도 아주 훌륭한 도우미 역할을 할 수 있다. 하지만 이처럼 우리 삶을 좀 더 편안하게 해줄 수 있는 사물인터넷과 웨어러블 컴퓨팅 기술은 사생활 침해와 같은 개인정보에 대한 보안 위협에도 함께 노출될 수 있다. 만약 사물인터넷이나 웨어러블 컴퓨팅을 통해 정보를 수집할 경우 개인정보에 해당된다면 '개인정보보호법'에 의해 반드시 정보주체로부터 동의를 받은 후에 정보를 수집해야 한다. 하지만 구글글래스와 같은 웨어러블 컴퓨팅 기기를 통해 수집되는 정보는 별도의 동의절차 없이 간단하게 타인을 촬영할 수 있으며, 웨어러블 컴퓨팅 기기 자체에 별도의 촬영여부를 알려주는 기능이 제공되지 않는다면 상대방은 자신이 촬영되고 있는지 조차 인지하기 어려울 수밖에 없는 상황이 발생하게 될 것이다[1]. 또한 의료 및 U-헬스케어 분야에서 웨어러블 디바이스는 개인의 생명과 관련된 민감한 정보를 다룰 수 있다는 점에서 특히 주의를 기울여야 할 것이다. 실제로 2012 년에 개최된 블랙햇 보안 컨퍼런스에서 해커가 특정인의 인슐린 펌프를 조작하여 개인의 생명에 치명적인 복용량을 주입할 수 있도록 조작할 수 있음이 증명된 바 있다[2].

이처럼 웨어러블 컴퓨팅의 다양한 서비스를 통해 편리한 삶을 누릴 수 있음에도 불구하고 센서 정보 혹은 개인 정보 노출, 비정상적인 패킷의 유통 그리고 메시지의 재사용, 데이터 위변조 문제 등과 같은 다양한 위협에 노출되어 있다. '제 3 의 IT 혁명' 기술의 한 축을 담당하게 될 웨어러블 컴퓨팅의 활용은 개인정보보호가 선행되어야 하며, 공공 목적이나 군사용으로 사용되는 경우 보안 기능은 더욱 필수적이다[3].

본 고에서는 이러한 웨어러블 컴퓨팅 환경에서의 보안 위협과 이에 대처하기 위해 필요한 보안 요구사항을 살펴보고자 한다. 본 고의 2 장에서는 웨어러블 컴퓨팅 개요 및 기술 분류, 3 장에서는 시장 현황 및 기술 발전 전망, 4 장에서는 정보보호위협과 대응 기술의 진화, 5 장에서는 결론을 맺는다.

2. 웨어러블 컴퓨팅 개요 및 기술 분류

1950 년대에 MIT 에서 그 개념이 정립된 웨어러블 컴퓨팅은 1981 년 고등학생이었던 스티브 만(Steve Mann)이 웨어러블 컴퓨터 시스템을 제시한 이후, 미국 제록스사의 마크 와이저(Mark Weiser)가 제안한 유비쿼터스 컴퓨팅과 함께 차세대 컴퓨팅 분야의 핵심 개념이다. 일반 사용자를 위한 범용 웨어러블 컴퓨터는 우리가 일반적으로 입고 다니는 옷이나 액세서리와 같은 형태로 자연스럽게 착용할 수 있고, 사용자의 요구에 즉각 반응하며, 또한 기기 사용에 따른 안정성을 보장하여 착용에 따른 문화적 이질감을 극복할 수 있도록 장치를 사용하는 것보다는 장치와 융합할 수 있는 사용자 인터페이스 기능을 지원해야 한다(<표 1> 참조)[4].

<표 1> 웨어러블 컴퓨터의 기본 기능[4]

기능	내용
착용감	일상생활에서 사용하는 의복, 액세서리와 같이 착용을 의식하지 않을 정도의 무게감과 자연스러운 착용감 제공
항시성	사용자 요구에 즉각적인 반응을 제공하기 위하여 컴퓨터와 사용자간 끊임없는 통신을 지원할 수 있는 채널 존재
사용자 인터페이스	인간의 신체적, 지적 능력의 연장선상에 있어야 하므로 사용자와의 자연스러운 일체감과 통합감 제공
안정성	장시간 착용에 따른 불쾌감과 신체적 피로감을 최소화하고 전원 및 전자파 등에 대한 안정성 보장
사회성	착용에 따른 문화적 이질감을 배제하고 사회 문화적 통념에 부합되는 형태와 개인의 프라이버시 보호

<표 2> 웨어러블 디바이스 기술 분류[5]

1 세대	2 세대	3 세대
웨어러블 디바이스	착용형 플랫폼	Reconfigurable SoC 초소형 대용량 배터리 저장장치 Smart fabrics(입는 컴퓨터) 액세서리(손목, 손가락, 팔 착용형 등)
	근거리 통신 기술	SAN, PAN, LAN, WAN Sensor Network Ad-hoc Network U-ID
	웨어러블 스마트 I/O	반지형, 장갑형 입력장치 안경형 디스플레이(머리착용형) 오감/BIO 센서
	경량 내장형 소프트웨어	소형 저전력 RTOS 분산 미들웨어 응용 SW 개발 도구
	감성 중심 에이전트	상황/위치 인식 에이전트 Security, 프라이버시, 생체인식 멀티모달 UI(제스처, 음성 등)
	오감 인터페이스	오감 인식 및 표현 오감 정보 융합 전송 및 재현(증강현실) 생체신호 인터페이스

이러한 웨어러블 컴퓨팅 기본 기능을 구현하기 위한 웨어러블 디바이스 기술의 세부적인 기술 분류와 발전 단계를 살펴보도록 한다. 웨어러블 컴퓨터 개발자인 스티브 만은 웨어러블 컴퓨터를 1, 2, 3 세대로 구분하고 있다. 1 세대와 2 세대를 구분하는 요소는 컴퓨터 모듈의 분리이며, 2 세대 웨어러블 디바이스는 분산된 컴퓨터 모듈을 선으로 연결하고 사용된 선은 의복에 넣고 꿰메어 자연스러움을 유도한다. 마지막으로 3 세대 웨어러블 디바이스의 특징은 “최대한 자연스럽게, 보이지 않는 디바이스”를 기술 목표로 하고 있다(<표 2> 참조)[5].

웨어러블 디바이스 기술 분류에서 살펴보았듯이 기능을 구현하기 위한 웨어러블 컴퓨팅에는 하드웨어 플랫폼, 사용자 인터페이스, 상황인지, 저전력, 근거리 통신 기술 등이 포함된다. 특히, 사용자 인터페이스 기술과 하드웨어 플랫폼 기술은 양손에 자유를 부여하고 간편하게 기기를 조작할 수 있도록 하며(hands-free), 사용자의 집중을 덜 요구하는(distraction-free) 웨어러블 특성을 보다 잘 반영해야 한다. 뿐만 아니라, 사용자가 직접 착용함으로써 안정성・편안함・패션과 같은 외적인 사항이 기술 수용에 큰 영향을 미칠 수 있기 때문에 의류・인간공학・디자인 등 IT 이외의 다양한 분야와 기술 협력 또한 중요하다고 할 수 있다[4].

3. 시장 현황 및 기술 발전 전망

웨어러블 디바이스 시장의 성장에 대해서는 주요 조사기관들이 긍정적인 전망을 제시하고 있다. IMS Research 는 전 세계 웨어러블 디바이스 단말의 출하량이 2016 년 기준 최소 3,920 만 대에서 최대 1 억 7,100 만 대까지 증가할 것으로 전망하였다. 다만 웨어러블 디바이스 시장이 초기단계이고 다양한 부분이 영향을 줄 수 있어 성장 시나리오를 나누어 전망을 제시하였다. 지역별로는 현재 착용형 디바이스 시장을 주도하고 있는 미국이 2016 년까지 글로벌 시장 주도권 및 가장 큰 시장규모를 유지하는 한편 유럽이 다음으로 큰 시장을 이룰 것으로 전망하였고, 일본 역시 인포테인먼트 분야에서 강점을 드러내며 웨어러블 디바이스의 메이저 시장을 형성할 것으로 예측하였다. 가트너도 헬스케어, 피트니스 분야의 웨어러블 시장규모가 2013 년 16 억 달러에서 2016 년 50 억 달러에 근접할 것으로 전망하였고, Juniper Research 도 최근 웨어러블 디바이스가 연이어 출시되면서 관련 시장도 2012 년 8 억 달러 규모에서 2014 년에는 15 억 달러 이상으로 증가할 것이다. 특히 헬스케어 및 피트니스용 단말과 멀티 기능 단말 등 소비자 시장을 직접 겨냥한 수요가 대폭 증가할 것으로 전망하였다. 이처럼, 현재 시장이 급격히 성장하는 단계이기 때문에 시장조사 기관마다 예측하는 시장규모에서 일부 차이가 있으나 급격한 성장을 보일 것이라는 부분에는 이견이 없는 것을 확인할 수 있다[6].

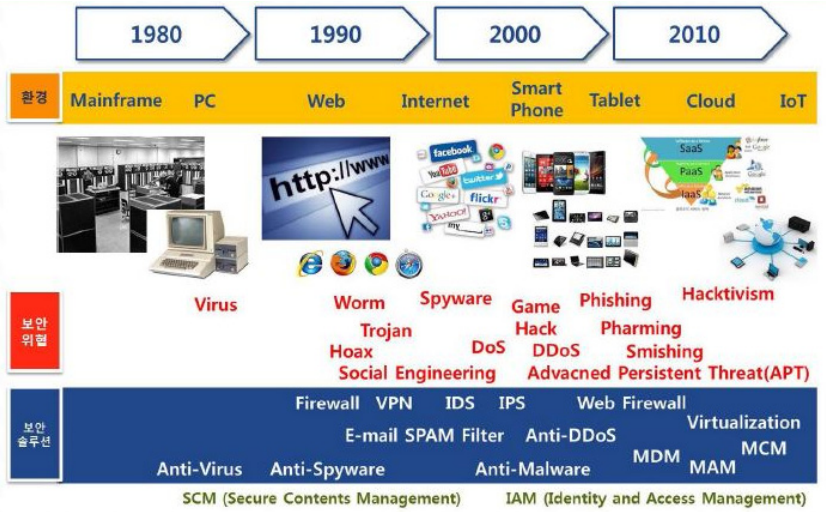
웨어러블 컴퓨터의 초기 발전 단계에는 시계, 안경, 목걸이와 같은 액세서리 형태에서 출발하여 직물 또는 의류에 일체화된 의복형 컴퓨터로 발전하고 있으며, 인간의 몸에 더 근접하여 신체 부착형, 신체 이식형으로 발전할 것으로 전망하고 있다((그림 3) 참조)[7].

(그림 2) 전세계 웨어러블 디바이스 출하량 전망[7]

(그림 3) 웨어러블 컴퓨터의 발전 방향[8]

4. 웨어러블 컴퓨팅 환경의 정보보호 위협과 보안 요구 사항

IT 보안 위협은 PC 의 발전과 궤를 같이한다고 해도 과언이 아니다. PC 의 시대에는 바이러스라는 것이 등장하였다. 인터넷이 발전되면서 웜(worm)이 등장하고 인터넷 네트워크를 통해 빠르게 유포되기 시작하였으며, 그 이후에 다양한 형태의 보안 위협이 끊임없이 등장하였다. 이처럼 환경, 즉 플랫폼의 발전과 보안 위협의 발전이 함께 진행되면 보안 산업 또한 이러한 흐름을 따라가기 마련이다. 스팸 메일이 쏟아지자 이메일 필터링 기술이 각광을 받았다. 이후 침입 탐지를 위한 IDS(Intrusion Detection System) 기술이 등장했지만 곧 방지의 관점인 IPS(Intrusion Prevention System)로 넘어간다. 점차 보안 위협이 복잡해지면서 단순히 '막는다'는 수동적인 개념을 넘어 악의적인 행위, 이상한 행위를 하는 소프트웨어를 탐지하고 차단해야 한다는 개념에서 안티멀웨어(Anti-malware) 기술로 보안의 중심이 이동하게 된다. 이제는 모바일 환경으로 변화함에 따라 다양한 디바



(그림 4) 컴퓨터 환경과 보안의 발전[2]

이스를 어떻게 관리할 것인가, 또 네트워크를 통해 이동하는 콘텐츠를 어떻게 보호할 것인가 하는 관점으로 보안 기술이 다변화하고 있다[2].

웨어러블 컴퓨팅 장치들이 의사 소통할 수 있는 웨어러블 컴퓨팅 환경에서는 정보화의 영역이 사람 중심에서 사물로 확대됨에 따라 기존의 인터넷 기반의 정보통신 환경과는 다른 환경의 변화가 있을 것으로 예상되며, (그림 4)와 같이 이에 따른 정보보호의 위협도 지금과는 달라 많이 다양해질 것으로 예상되고 있다. 즉, 인터넷에서 발생된 위협이 전체 위협 요소로 이어질 수 있어 불법적 공격으로 인한 폐해는 상상을 초월할 정도로 증가할 것이다[4]. 이처럼 우려하던 개인정보 침해에 대한 사례로 2014 년 2 월 구글글래스를 착

(그림 5) 사진 및 동영상 촬영 시 구글글래스의 모습과 타임스퀘어 촬영 사진[9]

용한 여성이 폭행당한 사건이 발생하였다. 웨어러블 디바이스에 대한 일반인의 개인정보 침해가 얼마나 위험한지를 보여주는 단적인 사례이다[8].

웨어러블 컴퓨팅 환경에서 사용자는 보안 시스템이 어떻게 동작하는지 관여하지 않아도 될 뿐만 아니라, 보안시스템에 의해 방해 받지 않아야 한다. 웨어러블 컴퓨팅 환경의 초점은 사용자가 더 이상 컴퓨터 기기에 신경을 쓰지 않아도 될 수 있도록 하는 것이다. 그 결과로 보안시스템은 환경과 조화되어 사용자를 방해하지 않고 서비스를 제공해야 한다[10]. 웨어러블 컴퓨팅 환경은 기존 컴퓨터 환경에서 고려되지 않았던 보안의 기술적인 기본 요구사항을 몇 가지 살펴보도록 하자. 첫 번째로 웨어러블 컴퓨팅의 환경에서 단말은 초경량으로 밀집된 상태로 구성될 것이므로 확장성(Scalability)을 고려해야 한다. 즉, 웨어러블 컴퓨터 네트워크에 적용할 라우팅과 보안 알고리즘들을 포함하는 미들웨어는 단말들이 밀집된 형태로 배치된다는 사실을 고려하여 설계되어야 한다. 또한 노드의 손실이나 배터리의 소모와 같은 물리적인 원인에 의한 웨어러블 노드의 손실에 대해 네트워크 내에서 삭제뿐만 아니라, 안정적이고 효율적인 데이터 전송을 위해 새로운 노드의 추가 등을 할 수 있도록 설계되어야 한다. 두 번째로 웨어러블 컴퓨팅 환경에서 노드들은 가용성(Availability)을 제공하기 위해서는 네트워크가 예정된 수명이 끝날 때까지 본래의 기능을 수행해야 한다. 만약 웨어러블 컴퓨팅 분야에서 가용성을 고려하지 않으면 잠재적인 사고를 감지하는데 실패하게 되어 재정적인 손해 등을 가져올 수 있기 때문이다. 세 번째로 악의적인 공격자에 의해 위협이 될 수 있는 보안상의 다양한 시도들에 대해서 유연하게 대처하기 위해 노드의 추가 및 삭제가 유연하게 이루어질 수 있도록 유연성(Flexibility) 또한 기술적으로 만족해야 한다. 마지막으로 웨어러블 컴퓨팅 환경에서 단말들은 자가 구성(Self-organizing) 능력을 갖추어야 한다[10].

좀 더 안전한 웨어러블 컴퓨팅 환경을 위하여 외부 공격자에 대한 보안 요구사항을 몇 가지 추가적으로 살펴보도록 하자. 정보를 서로 주고 받는 단말들끼리 공유되는 정보가 악의적인 공격자로부터 도청 또는 트래픽 분석 등을 통해 노출되지 않도록 기밀성(Confidentiality)이 요구된다. 또한 서로 통신하고 있는 송수신자가 서로 정당한지를 인지할 수 있어야 하고, 데이터가 악의적인 공격자의 불법적인 위변조 과정이 일어나지 않도록 인증(Authenticity)/무결성(Integrity)을 충족시켜야 할 것이다[10].

마지막으로 외부공격자가 아닌 내부 공격자에 대한 보안 요구사항을 몇 가지 살펴보도

록 하자. 수 많은 노드들로 구성되는 웨어러블 컴퓨팅 환경에서 공격자가 포획한 노드를 탐지하는 것은 어려운 문제이다. 그러므로 보안 프로토콜을 설계할 때 포획된 노드로 인해 발생할 수 있는 문제점을 고려하여 노드에 대한 탄력성(Resilience to node capture)을 고려해야 한다. 또한 시스템의 일부가 파괴되었을 경우 원래 제공받던 데이터 전송 속도에 비해 전송 속도가 많이 저하되더라도 지속적인 데이터를 받을 수 있도록 급격한 성능저하 방지(Graceful degradation) 기능을 제공해야 한다[10].

웨어러블 컴퓨팅 환경에서 다양한 보안위협에 대한 기술적인 요구사항을 만족하는 것도 중요하지만 사회적 합의와 법적인 제도의 정비 또한 수반되어야 한다. 기존의 개인정보보호 프레임은 모바일 디바이스를 통해 “개인의 동의 없는 개인정보 수집금지” 등 기존의 제도적인 방법으로는 무의미하다. 또한 업무 목적의 웨어러블 장비를 통해 수집된 직원의 건강정보가 보험회사나 고용주에게 제공되거나, 누군가의 기분, 체력, 건강상태에 대한 실시간 정보가 다른 사람에게 전해질 가능성도 충분한 상황이다. 그러므로 사회적 합의에 의한 현행 개인정보보호제도의 문제점을 개선하고 웨어러블 디바이스 설계 시 개인정보보호를 위한 고려사항 등을 검토해야 할 것이다[8].

미국의 언어학자인 MIT 의 노암 촘스키 교수는 구글글래스는 사생활 침해로 인해 인간의 삶을 파괴할 것이라고 강도 높게 비판하였다. 이용자들의 모든 시청각 정보를 저장 및 전송할 수 있는 구글글래스의 특성으로 인해 주변에서 일어나는 모든 일들이 무분별하게 인터넷에 올려질 것이어서 사생활 침해가 심각할 것이라고 강조했다. 구글글래스는 전체주의적 사고의 결과이며 마치 조지 오웰의 ‘1984’를 보는 듯하다고 지적하면서 사회적, 윤리적 이슈에 대한 대안 마련이 시급함을 역설했다. 결국 기술적인 요소와 제도적인 방법의 도입과 함께 윤리적인 대안도 함께 수반되어야 할 것이다[9].

5. 결론

향후 웨어러블 컴퓨팅 기술은 가정, 물류/유통, 교통, 행정, 복지 그리고 환경 등의 다양한 분야에 적용될 것으로 예상된다. 또한 미래 사회의 기반 인프라로 자리잡게 될 것이다. 웨어러블 컴퓨팅 환경이 구축된 사회에서는 모든 사물들의 지능화로 자율적으로 주변 환경을 센싱하여 주변 상황을 인식하고 이들을 제어할 수 있는 정보 네트워크가 형성될 것이다. 이처럼 다양한 응용 분야에서 활용되는 웨어러블 노드는 대부분 소형이기 때문에,

일반적으로 배터리로 동작하며 그 크기가 작고 전력 소모가 작아야 한다. 그리고 외부의 환경 변화에도 가능한 영향을 받지 않고, 웨어러블 노드에 탑재되는 임베디드 운영체제 및 협업을 위한 미들웨어는 제한된 메모리와 CPU 자원을 최대한 활용할 수 있어야 하며, 노드에 할당된 작업들을 처리하고 네트워크 내에서의 통신이 원활하게 수행될 수 있도록 보장되어야 한다. 또한, 웨어러블 컴퓨팅 환경에서 다양한 보안위협에 대처하기 위해서 통신, 에너지, 메모리 등의 요구 조건을 전체적으로 고려해 물리적으로 노출될 수 있는 환경에서 발생할 수 있는 다양한 공격 가능성을 예측하여 다양한 기술적 보안 요구사항을 만족할 수 있도록 해야 한다. 또한 제도적인 대안 마련과 함께 윤리적인 사회적 합의가 수반되어야 할 것이다[10].

<참 고 문 헌>

[1] 권현준, “사물인터넷과 웨어러블 컴퓨팅 시대의 개인정보보호”, 보안뉴스, July 24, 2014.

[2] “상상이 현실이 된다, IoT”, AhnLab, 보안 이슈 & 이슈, June 27, 2014.

[3] 김준래, “정보보안을 창조경제 중심으로”, The Science Times, September 2014. 4.

[4] 손용기, 김지은, 조일연, “웨어러블 컴퓨터 기술 및 개발 동향”, 한국전자통신연구원(ETRI), 전자통신동향분석 제 23 권 제 5 호, Oct. 2008.

[5] “차세대 스마트 기기, 웨어러블 디바이스 시장 현황 및 전망”, 한국방송통신전파진흥원(KCA), Market & Issue 분석 Report, December 10. 2012..

[6] “웨어러블 디바이스 동향과 전망”, 한국방송통신전파진흥원(KCA), 방송통신기술 이슈&전망 제 29 호, Dec. 27. 2013.

[7] “웨어러블 컴퓨터 제품 및 기술 개발 현황”, 한국광학기기협회, 광학세계, Nov. 1. 2013.

[8] “개인정보보호 주간동향”, NIA(한국정보화진흥원), July 18. 2014.

[9] 이영석, 유용덕, 박상현, 최훈, “웨어러블 컴퓨터 보안”, 한국차세대컴퓨팅학회 논문지, June 2006..

[10] 박현수, “웨어러블 컴퓨터를 둘러싼 개인정보보호 이슈와 시사점”, 한국산업기술진흥협회, Oct. 2013.