

스마트 환경의 주요 정보통신 기술과 정보보호 동향

홍진근*

◆ 목 차 ◆

1. 들어가는 말
2. 스마트 시대의 관련 기술 동향
3. 스마트 환경에서 보안기술 동향
4. 결 론

1. 들어가는 말

스마트 시대의 인터넷 동향과 관련하여, 세계 인터넷 인구는 2000년대의 8배, broadband 보급률이 3.5배 증가한 것으로 나타나고 있다. 또한 국내 통신 서비스 시장은 2012년 43조 7천억원에 이를 것으로 예측되고 있다. 무엇보다도 스마트 시대의 10대 주요 기술 트렌드에는 정보보안을 포함해, 클라우드 서비스, 소셜 네트워크서비스, 모바일 어플, 위치기반 서비스, 스마트워크, 소셜 비즈니스, 오픈 플랫폼, 빅 데이터로 예측된다. 스마트 기술과 관련하여, 기존 연구에서는, 유상근 등이 기고한 스마트 모바일 서비스 -M2M 기술 및 표준 동향)에 따르면, 최근 스마트 모바일 서비스인 M2M 기술(사물통신)과 관련하여, AT&T, Sprint, Orange, Telefonica, Deutsch Telecom 등 통신사를 중심으로 전담조직을 만들어 M2M 서비스를 지원하고 있다고 소개하고 있다.

또한 오픈성 등)은 3GPP LTE 기술 개발 및 서비스 동향에서, 실무적인 모델설계, 성능검정과 시험방법을 살피고 있다.

이승윤 등은 차세대 모바일 웹 플랫폼 표준화 동향)에서, 모바일 웹 표준이 차세대 모바일 어플리케이션

이전 및 플랫폼 실현을 위한 핵심 기능으로 발전하고 있다고 평가한다. 모바일 웹은 단순히 브라우징 수준을 넘어선다는 것이다. 모바일 웹 기술에서 큰 변화가 다양한 어플리케이션을 제공하기 위한 API 기술로 발전에 있다고 말한다. 현재의 스마트 폰과 같은 모바일 단말이 이제 홈 네트워킹, TV, 사물 통신 등 유비쿼터스 환경에서 실현되고 있는 것으로 분석한다. 여기서 모바일 플랫폼은 웹 기반의 공통 API를 기본 인터페이스하며, 모바일 미들웨어에 독립된 플랫폼이라 할 수 있다.

김학영 등은 모바일 클라우드 기술 동향)을 살피고 있다.

이강찬 등은 클라우드 컴퓨팅 표준화 동향 및 전략)에서, 클라우드 표준화 이슈로 플랫폼 간의 독립성 문제, 플랫폼간의 통합 서비스와 이동성 문제, 데이터 서비스의 안전성 문제, 단말 간의 독립적인 서비스 문제에 대해 살피고 있다. 이 연구에 따르면 SC38 SGCC 표준화 대상 항목에는 신뢰성이 있고 안전 보장형인 클라우드 컴퓨팅 프레임워크, 안전한 클라우드 서비스 매커니즘 및 프로토콜이라는 보안 문제가 포함되어 있다. 클라우드 표준화 모델에서 언급되는 보안기술은 프라이버시와 데이터 보안 영역, 신뢰가능한

* 백석대학교 교수

1) 유상근 등이 전자통신동향분석 제26권 제2호(2011. 4)에 기고한 바 있다.
2) 오픈성 등이 전자통신동향분석 제25권 제6호(2010. 12)에 기고한 바 있다.

3) 이승윤 등이 전자통신동향분석 제25권 제3호(2010. 6)에서 차세대 웹 모바일 기술과 동향에 대해 살피고 있다.
4) 김학영 등은 전자통신동향분석 제25권 제3호(2010. 6)에서 모바일 클라우드 기술 동향을 살피고 있다.
5) 이강찬 등이 전자통신동향분석 제25권 제1호(2010. 2)에서 클라우드 컴퓨팅 표준화 이슈를 다룬 적이 있다.

컴퓨팅, 클라우드 싱글사인온, 네트워크 보안 등의 이슈를 포함하고 있다.

본 기고에서는 2장에서 유비쿼터스 네트워킹, 전송 통신 기술, 모바일 클라우드, 스마트 매체, 디바이스, 콘텐츠를 중심으로 하는 스마트 시대의 관련 기술 동향을 기술하였다. 또한 3장에서는 클라우드 서비스에 보안, 개인정보보호, N-스크린 보호, 분산서비스 공격, 스마트디바이스 보안, 모바일 인터넷 보안을 중심으로 스마트 환경에서의 보안 기술 동향을 기술하였고 마지막 4장에서 결론을 맺었다.

2. 스마트 시대의 관련 기술 동향

미국의 모바일 특히 스마트폰 시장은 2012년에는 88억달러에 이르러 전세계 시장의 40%를 점유하고 트래픽 양만해도 1GB가 이를 것으로 추정된다. 미래 IT 산업의 전개는 어떻게 될 것인가라는 물음앞에 차세대 모바일 기술의 변화는 초고속 광대역 저전력화, 지능화와 자율화, 컨버전스화에 초점이 맞추어지고 있다. 2015년이 되면 지능형 맞춤형 모바일 플랫폼 기반으로 발전할 것이고, 대화형 인터페이스에 오감을 기반으로 상황인지형 서비스에 관심을 가지게 될 것이다. 또한 유무선 VoIP서비스 연동과 함께 증강현실, 가상현실 등을 지원하는 실감 서비스가 제공될 것이다. 산업 기간망은 차량, 조선, 교육, 국방, 건설 분야에서 융합 서비스가 제공될 것이다.

이번 장에서는 차세대 네트워킹과 5any를 지원하는 유비쿼터스 네트워킹, MWC2012를 중심으로 전송통신 기술, 스마트 디바이스와 매체, 콘텐츠를 기반으로 하는 스마트 기술, 모바일 클라우드기술을 중심으로 간략하게 살펴볼 것이다.

2.1 유비쿼터스 네트워킹

유비쿼터스 기술의 특징은 차세대 네트워킹 + 5any를 지원하기 위한 능력에 있다. 유비쿼터스 네트워킹 기술에 주요 이슈였던 사물(M2M; 네트워크에 접속된 사용자나 개체로 정보장치 콘텐츠, 디버깅 기계 등 포함) 통신의 경우, 권고안이 현재 나오고 있는 실정이다.

다. 유비쿼터스 네트워킹 기술은 중단 사용자 기능, 전송층, 서비스층과 이를 지원하는 어플리케이션이 주요 특징을 이룬다. 사물통신이 갖는 기본적인 특징에는 최적화된 경량형 프로토콜 설계, 통신거리 내에서 사물에 대한 자동 발견, 유연한 이동성 관리, 복잡한 사물 통신을 지원할 수 있는 동적인 라우팅 능력, 네트워크의 확장성, IP기반의 종단간 연결성, 손쉽게 이식가능하고 사용이 용이한 어플리케이션 능력, 서비스 품질에 대한 요구성, 오류 허용 및 대처 능력 등이 있다. 사물통신은 무엇보다 5any를 만족시키기 위해, 사물에 대한 식별문제, 사물에 대한 위치식별과 추적문제, 연결성 차원에서 naming과 어드레싱 문제가 고려되어야 한다.

2.2 전송 통신 기술

모바일 산업은 어디로 갈 것인가. 2012년 Mobile World Conference에서는 모바일 용어에 대한 재정의가 이루어지고 있다. 'Connected life', 'Connected house'라는 용어가 나오고 있다. AT&T는 헬스 케어와 관련하여 개인 응급 대응 시스템을 시연하였으며, KT는 교육용 로봇이나 자산 도난방지 재고관리 시스템을 전시한 바 있다. 보다는 에너지 관리에 초점을 맞추어 빌딩 에너지 소비의 최적화를 목표로 하며, GSMA는 도난 차량추적을 포함한 스마트 시티의 생활상에 초점을 맞추어 시연한 바 있다. 최대 이슈로는 3G와 공존하는 LTE 기술에 초점을 맞추어 다양한 기술을 시연하는데 있었다. 2,500개의 모바일 기기 사용자들은 4년 동안 4억 2,500만명의 가입자를 자랑하는 페이스북 사용자가 되고 있다. 스마트 모바일 폰의 5대 트렌드에는 쿼드코어 프로세서, 고해상도의 대형 스크린, NFC, LTE, 저가 보급폰가 이슈가 되고 있다. 하드웨어와 소프트웨어 영역에서 경쟁력의 상승 가도를 달리는 중국의 급부상과 함께, 노키아와 윈도우8의 성공 여부가 여전히 이슈가 되고 있다.

1) WIFI

최근 WiFi를 기반으로 하는 P2P 규격- WiFi direct 기술에 대해 이슈화가 있다. 이 규격은 TV, 노트북, 카메라 등과 같은 휴대기기와 모바일 단말이 직접 연

결을 통해 데이터 전송이 가능하기 위한 기술을 특징으로 한다. WiFi P2P 인증제품을 보유한 주요 회사에는 Broadcom, Intel, LG, Pantech, Qualcomm, Realtek, Samsung, Sony 등이 있다.

2) 3G와 4G

현재 LTE는 3.9G 모바일 통신기술이며, 4G 기준에 미치지 못하나 3.5G (HSPA (3.1~14.4Mbps), EV/DO-rA,B (5.8Mbps)) 기술보다 빠르다. 5G에 대한 언급이 현재 진행되는데, 4G의 1Gbps 속도이상(5G는 4G보다 1000 배 이상 빠를 것)을 제공할 것으로 전망하며, 낮은 배터리 소모량과 커버리지, 음영지역, 트래픽 비용이 그 이슈가 될 것이다. 2020년이 되면 5G 서비스는 공간을 초월한 실감 서비스와 맞춤형 정보 서비스, 친환경적이고, 지식 품질 등 차별화된 서비스가 제공될 것으로 예측된다.

(표 1) 3G기술과 4G기술 비교⁶⁾

항 목	WCDMA (UMTS)	HSPA/HSDPA/HSUPA	HSPA+	LTE
최대다운링크 속도	384Kbps	14Mbps	28Mbps	100Mbps
최대업링크 속도	128Kbps	5.7Mbps	11Mbps	50Mbps
지연시간	150msec	100msec	~50msec	~10msec
시 기	2003~4	2005~2008	2008~2009	2009~2010
접속방식	CDMA	CDMA	CDMA	OFDMA/SC-FDMA

LTE는 단순 음성 서비스나 모바일 웹 서비스는 물론이고, e-헬스, 사물통신, 어플리케이션 에코시스템에 이르기 까지, 다양한 융복합 멀티미디어 서비스로 확장되어가고 있다. 그런데 LTE 서비스 확산의 움직임과 함께, 이를 저해하는 요인 몇 가지가 언급되고 있다. 먼저 LTE 과금제나 서비스 패키지 구성에서 상이한 시각과 함께, 비즈니스 모델이나 수익모델이 뚜렷하지 않다는 점, 그리고 멀티 대역 기능 탑재로 인한 단말 제조비용의 상승이나, 지연되는 다양한 디바이스 출시계획, 어려운 주파수 할당문제 등이 지적되고 있다.

2.3 스마트 기술

2011년에 가장 주목 받은 제품군이 스마트 TV이었다. 스마트 매체 가운데 스마트 TV의 특징은 웹브라우저를 통해 컴퓨터와 유사하며 어플리케이션을 자유롭게 활용할 수 있다는 것이다. 이 서비스는 방송융합서비스를 제공한다. 애플이 Mobile Me를 통해 N-스크린 서비스가 가능하도록 하는 클라우드 서비스가 제공되고 있다면, 구글 TV는 웹 기반의 콘텐츠를 TV로 확장하고 있고, 소니는 실시간 프리미엄 스트리밍 비디오 서비스 VOD를 제공하고 있다. 인터넷 기반의 기술을 최적화한 MMT 전송기술이 표준화되고 있는 실정이다. 인터넷 HTTP 적응형 스트리밍 서비스 기술 개발은 마이크로소프트, 애플, 어도비사가 중심이 되고 있다.

스마트 콘텐츠 시장은 종래의 서비스 공급자나 네트워크로부터 소비자와 콘텐츠 중심으로 이동하고 있다. 모바일의 생태계와 관련하여 이상일⁷⁾이 고찰한 바 있는데, 모바일 생태계가 갖추어야 할 조건으로, 개방형 모바일 플랫폼을 스마트 디바이스에 탑재하는 문제, 개방형 개발 환경의 제공으로 누구나 단말기 어플을 개발할 수 있도록 하는 문제, 마켓 공간에서 어플을 유통 판매할 수 있는 환경 조성 문제, 아울러 수익분배 구조 문제 등의 이슈가 초점이 되고 있다고 말한다. 스마트 폰과 스마트TV는 유통시장, 화면크기나 해상도, 이용거리, 교체주기 측면에서 차이를 보이면서 이슈화가 되고 있다.

스마트 네트워크 사업의 경우, 스마트 게이트웨이가 활용되는데, 스마트 노드의 위치정보를 스마트 라우팅 관리자로부터 수신하여 사용자가 접속하고자 하는 스마트 노드로 접속 구성되도록 구한다. 스마트 노드는 콘텐츠 캐싱, 다운로드, 스트리밍 등에 대한 항목들을 대상으로 HTTP 서비스가 제공된다. 스마트 네트워크는 P2P서비스를 제공할 수 있도록 오픈 API를 제공하고 있다. 스마트 디바이스의 경우, 가속도 센서, GPS, 카메라, 터치 센서 등 각종센서를 탑재하고 있으며 2015년 시점이 되면 본격적으로 보급될 것이다.

6) <http://www.nipa.kr>, 정보통신산업진흥원의 최신IT동향, LTE 확산이 가져온 4G와 5G 논쟁

7) 이상일이 스마트 디바이스가 몰고오는 산업지형 변혁에서 모바일 생태계 문제를 소개한 바 있다. 정보통신산업진흥원 IT 기획시리즈

(표 2) 스마트디바이스(SD)와 소셜 매체(SM) 융합 기반의 로드맵

		2010~2012	2013~2014	2015~2016
SD/SM 발전		SD 도입시점 트위터	SD 발전시점 페이스북	SD 보급시점 SD의 웹 프런트
활용	단말, 서비스 진화	모바일 브로드밴드 고속화		모바일 광대역, 고속화, 센싱 정보 확대, 빅 데이터 분석, 단말 안내기능 (매체의 지능화)
	SM 진화	소셜매체 연계 위치정보 도입기		기업 소셜넷 활용 소셜 매체분석
기업에 미치는 영향		스마트 기기 기반 소비자 데이터 수집, 서비스	소셜 넷 기반 서비스 제공, 고객정보 분석	빅 데이터분석, 소셜지능화를 통한 안내 서비스

스마트 디바이스 가운데 카메라는 렌즈를 통해 습득된 정보를 인공지능과 융합되어, 지능적으로 해석·판단·이해하고자 하는 시도가 진행되고 있다. 여기에는 컴퓨터 비전시스템이 임베디드 형태로 개발되고, 특정 이벤트를 검출하거나 의사결정 정보를 생성하는 일을 수행한다. 하드웨어는 ASIP 형태로, 소프트웨어는 지능화된 인식 분석 알고리즘이 재프로그램화가 가능하도록 개발되고 있다. 스마트 카메라의 각 컴포넌트에 대한 연구⁸⁾는 NXP의 WiCa 카메라 시스템, 스탠포드 대학의 MeshEye 무선 아키텍처, Bourgogne 대학 Le2i 연구, 프랑스 LASMEA의 SeeMOS 아키텍처, 카네기 멜론대학의 CMUCam, Graz 공대의 SmartCam 등이 있으며, 하드웨어에 보안기능이 적용된 TrustCam 플랫폼도 있다.

2.4 모바일 클라우드 기술

최근 기업 M&A의 관심은 스마트이동성, 소셜 네트워킹과 함께, 클라우드 컴퓨팅에 초점이 맞추어지고 있다. 클라우드에서 이슈화되는 주요 요건들에는 클라우드 SLA의 체계화와 표준화, 통제시스템과 모니터링 시스템 기능의 개선과 위험 최소화, 그리드 커뮤니티

의 신뢰기반, 운영방식 측면에서 분석, 보안 프로파일 및 테스트 기준, 오류발생 가능성 예측, 서비스 측정 표준의 수립과 표준화 등이 포함된다.

클라우드 컴퓨팅에 공개 SW가 적용되고 있으며, 2015년 이후 시점이 되면 글로벌 기업의 99%가 공개 SW를 사용하게 될 것이다. IaaS 클라우드 환경에 사용되는 공개 SW 내역은 다음과 같다.

- 가상머신 모니터: Xen, KVM, VirtualBox
- 가상머신 모니터 기능제어 : Libvirt, Ovirt, virt-manager
- 스토리지 가상화: LVM, Hadoop, Gfarm, Swift
- 가상 머신 이미지 관리: Glance, Aeolus
- 가상머신 시스템 제어: OpenStack, CludStack, Eucalyptus, Nimbus, OpenNebula, ConVirt
- 사용자 인증: GroundWork, Zabbix, Nagios, Higgins, Shibboleth
- 서비스 품질 관리: Zabbix, Ganglia
- 미터링: Ovirt

클라우드 운영 관리에는 IaaS 환경에 OpenStack 오픈 프로젝트를 관리하는 Nova가 있고, 캘리포니아 산타바바라 대학 프로젝트로 시작된 유칼립투스(Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems), Universidad Complutense de Madrid 프로젝트의 OpenNebula, 사이트릭스와 클라우드닷컴이 개발한 CloudStack이 있다. 또한 다중 클라우드 호환기술에는 Deltcloud, Simple Cloud, Libcloud, Aeolus가 있다.

김학영 등이 연구한 모바일 클라우드 기술 동향에서는 모바일이 클라우드 컴퓨팅을 지향하게 되고, 2014년 시점까지 클라우드가 모바일 컴퓨팅에 주 이슈가 될 것이라는 점이다. 현재 상용화된 모바일 플랫폼을 지원하는 회사(서비스)에는 MS(윈도 모바일, 라이브 미-휴대폰 백업과 동기화 서비스, 위치 찾기), 노키아(심비안), 애플(OS - 모바일 미; 이메일/연락처/캘린더 푸시; 3-스크린), 구글(안드로이드-클라우드 프린트), 림(블랙베리), 팜(웹 OS) 등이 있다.

또한 클라우드 컴퓨팅의 요소 기술에는 가상화, 분산처리, 오픈 인터페이스, 서비스 프로비저닝, 리소스

8) 김무섭 등이 스마트 카메라 기술동향 주제로 전자통신동향분석 제26권 제6호(2011. 12)에 기고한 바 있다.

유틸리티, SLA, 다중 공유, 보안 및 프라이버시가 있다. 그런데 모바일 클라우드 플랫폼에도 한계점이 대두된다. 플랫폼 간의 상호호환성의 문제와, 각 다른 형태로 데이터 저장 관리로 인한 데이터 이동성 문제가 지적되고 있다.

3. 스마트 환경에서 보안기술 동향

이번 장에서는 클라우드 환경에서 고려되는 보안 서비스, 이슈가 되고 있는 개인정보보호, 3-스크린을 넘어서는 N-스크린에서 보안문제, 모바일 환경에서 분산서비스 공격 이슈, 스마트 디바이스 보안, 그리고 모바일 인터넷 보안 등 여러 요소들을 중심으로 간략하게 살필 것이다.

3.1 클라우드 서비스에서 보안

클라우드 환경에서 보안서비스는 웹 방화벽, DRM, DLP 등과 같은 보안솔루션들을 적용하는 영역이 클라우드 서비스 환경으로 이동하고 있다고 분석된다. 많은 기업과 조직들은 사회적 환경이 클라우드 서비스로 이동해 감에 따라 대두되어 왔던 보안과 프라이버시 문제를 고민하고 있다. 정부차원에서 추진되는 클라우드 보안 서비스의 주요 항목에는 보안감사와 법적 수행을 위한 표준, 보안시스템과 평가, 인증 프로세스의 지원, ID 및 접속관리 표준, 기업용 보안 인프라와 안전한 통합 문제 등이다.

또한 클라우드 서비스에서 일어날 수 있는 7가지의 보안 위협으로는 클라우드 오용과 비도덕적인 사용, 불안정한 인터페이스와 응용 프로그래밍 인터페이스, 악의적인 내부자, 기술 공유 문제, 데이터 유실이나 유출, 계정이나 서비스 갈취, 알려지지 않은 위협 프로파일 등이 있으며 이 문제에 대한 관심들이 고조되고 있다.⁹⁾

클라우드 서비스 보안은 클라이언트, 인프라 서비스, 플랫폼 서비스, 소프트웨어 서비스 등의 요소를

중심으로 개발되고 있는 실정이다. 클라우드 컴퓨팅에 관한 보안 프로그래밍 FedRAMP가 제정되었다.¹⁰⁾ 이 프로그램은 사전에 인증한 벤더를 활용하는 방식으로, 정보시스템/서비스에 대한 정보보증, 위험관리의 비용 절감, 연방기관의 정보시스템과 서비스를 제공하여, 보안평가와 인증, 모니터링 절차를 제공하고 있다. FedRAMP 보안 인증 프로세스에서는 보안평가, 운용 허가서 활용, 지속된 모니터링과 인증, 공인된 제3의 평가기관을 운영하고 있다.

클라우드 컴퓨팅 환경에서는 클라우드 서비스의 구조적 특성, 다른 사용자와 정보 공유 여부 등이 기반이 되는 인증 서비스와 ID 관리에 대한 요구가 증가하고 있는 실정이다.¹¹⁾ 클라우드 보안정책은 서비스 허가를 위해, IaaS(주체가 시스템/네트워크 관리자, 객체가 사용자 계정, 파일시스템이나 자원 관리기능), PaaS(주체가 프로그램개발자, 객체가 DB), SaaS(주체가 사용자, 객체가 프로그램)를 중심으로 고려하게 된다. 보안정책의 경우 각 구성요소에 대해 포괄성과 확장성을 지녀야 하며, 프라이버시 문제와 관련하여, 서비스 제공자에 의해 개인정보보호와 암호화, 키 관리 기능이 함께 고려되고 지원되어야 한다.

클라우드 서비스에 대한 법적 규제 문제와 관련하여, 미 연방기관이 FISMA (Federal Information Security Management Act)에서 정보와 시스템 보호를 위한 법적 기준을 마련하여 적용하고 있는 상황이다.

전통적으로 적용되고 있는 주요 보안기능들처럼, 클라우드 서비스에서도 가상환경에서 보안, 기밀성과 무결성에 대한 대책, ID 관리, 접근통제와 프라이버시 문제가 고려되고 있다. 가상화 보안 문제는 NIST가 가이드라인을 제시한 것처럼, 소프트웨어의 실행과 관리통제, 고객을 위한 운영체제와 호스트 운영체제 사이의 자원공유 통제, 고객 운영체제와 소프트웨어 동작에 대한 점검 등이 요구되고 있다.

데이터 기밀성과 무결성이 클라우드 서비스 제공자에게나 소프트웨어에 구현되고 있고, 웹 환경의 경우 보안정책은 XACML (eXtensible Access Control Markup

9) 남기효, 김윤홍이 정보통신산업진흥원 IT기획시리즈에서, 클라우드 서비스 분석 및 보안 이슈에 대해 리뷰한 바 있다.

10) 박춘식이 정보통신산업진흥원 IT 기획시리즈에서, 클라우드 컴퓨팅 보안인증제도에 대해 리뷰한 바 있다.

11) 이형효는 정보통신산업진흥원 IT기획시리즈에서, 클라우드 컴퓨팅 보안 연구에 대한 동향에 대해 기고한 바 있다.

Language)의 사용이 활용될 것으로 예측되고 있다.

3.2 개인정보보호¹²⁾

개정된 정보통신망법에서는 주민등록번호의 수집 이용제한사항(제23조-2), 개인정보 누출시 이용자 통지와 방통위 신고사항(제27조-3), 개인 정보의 유효기간 제(휴면계정 등 개인정보 파기 등에 대한 조치)의 의무화, 제29조), 개인정보의 이용 내역 통지제도(이용자에게 통지하도록 의무화, 제30조-2) 항목이 포함되어 있다. 사업자라면 주민번호를 사용하지 않고 회원 DB를 관리하는 방안이 요구되고 있다.

개인화서비스에 대한 요구와 개인정보보호 사이에 상관관계를 가지고, 어떻게 하면 적합한 고객의 요구를 제공할 수 있을까 하는 개인화서비스 모델(CRM, VRM)에 대한 연구가 시도되고 있다. 그런데 이러한 모델을 적극적으로 서비스하기 위해서는 익명화(그룹서명, 링 서명 등)나 프라이버시(일방적인 개인정보 수집에 제한을 두고 사용자의 자기 정보에 대한 통제권 강화) 기술과 같은 보안서비스에 대한 요구는 반드시 해결되어야 할 과제이다.

3.3 N-스크린 보호¹³⁾

TV, PC, 휴대전화를 인터넷으로 연결하고 콘텐츠를 동기화하는 3 스크린이, 공통된 OS를 탑재한 다양한 단말기에서 공통된 콘텐츠를 이용할 수 있는 서비스인 N 스크린으로 확대되고 있다. N 스크린의 주요 요건은 클라우드 컴퓨팅, 풀 브라우징 인터넷의 접속, 플랫폼과 단말간 OS 통합이 언급되고 있다. 저작권 보호 기술에는 실시간 스트리밍 콘텐츠의 사용 통제, 워터마킹 기반의 콘텐츠 저작권자 통제, 다운로드 되는 콘텐츠 저작권 통제, 불법 업로드/다운로드와 캡처에 대한 통제, 과금기술 통제, 저작권 보호 기술에 대한 API 기술, 구매정보 관리 등이 포함되고 있다.

12) 김정섭이 ICT시장 변화에 따른 개인정보보호 정책에서 개인정보보호 정책동향과 사업자 대응방향에 대해 기고한 바 있다.

13) 임형민이 N-스크린 기반의 저작권 침해대응 기술에 대해 기고한 바 있다.

3.4 분산서비스 공격¹⁴⁾

모바일 환경에서 분산서비스 공격은 모바일 네트워크 서비스와 운영에 요구되는 특정 리소스(페이징 채널이나 트래픽 채널, 신호 메시지 등)를 대상으로 한다. 또한 적은 양의 트래픽으로 공격이 가능하다는 분석이 나오고 있다. 현재까지 대부분의 DDoS 공격은 어플리케이션 서버를 대상으로 대량의 패킷을 전송함으로써 클라이언트들이 정상적인 서비스를 받을 수 없도록 하였다. 그런데 모바일 네트워크에서 DDoS는 수십Kbps~수백Mbps 환경에서 공격이 가능하다는 것이다. 이러한 배경에는 먼저 접속을 위해 단말 IP나 전화번호에 해당하는 ID를 수집하게 되는데, 이때 전화번호는 인터넷 검색을 통해 쉽게 이루어질 수 있다. 샘플링 공격 역시 지동화 공격기술 가운데 유용한 방법으로 알려지고 있다.

모바일 환경에서 DDoS 공격에는 네트워크 운용을 방해할 목적으로 여분의 데이터를 증가시켜 방해하는 네트워크 제어 측면에서 공격형태가 있고, 리소스를 고갈시키는 형태인 문자 메시지(단문메시지를 포화시키기 위해 300-400개(초당)의 메시지 전송)나 페이징 채널 공격(적은 대역폭을 사용하는 이 채널을 고갈), 데이터 채널을 공격하는 형태(공격자가 데이터 전송에 사용하는 데이터 채널의 연결상태를 지속시킴으로써 리소스 고갈)가 분석되고 있다. 제시되는 간접공격의 예로 SNS 서버로 하여금 서비스 거부 공격을 일으키게 유도하여, 모바일 단말이 지속적으로 상태정보의 재전송 요청을 하게하는데, 이 요청처리는 결국 네트워크의 제어채널 리소스를 고갈시키게 된다.

3.5 스마트 디바이스 보안

카메라 시스템을 적용할 경우, 카메라 렌즈를 통해 인식되는 개인 인식정보의 이용이나 저장이라는 측면에서, 역시 프라이버시 문제나 윤리적인 문제의 소지가 언급되고 있다. 그럼에도 불구하고 최근 객체 탐지

14) 이성원 등이 이동통신 네트워크 DDoS 공격 및 대응기술 동향을 전자통신동향분석 제26권 제6호(2011. 12)에 기고한 바 있다.

와 인식, 차량 인식과 침입 탐지 분야를 포함한 관계 시설에 지능화된 카메라 시스템의 도입 계획이 증가하고 있다.

스마트 폰에서 보안 위협요소에는 다양한 인터페이스가 오히려 다양한 공격 경로를 제공함에 따른 개방성의 문제, 분실/도난의 위험성을 야기하는 휴대성 문제, 전력과 성능의 제약사항으로 인한 보안기능 적용에서 문제점 등이 있다. 최근 언급되는 모바일 악성코드 유형에는 단말에 장애를 일으키는 형태, 배터리를 소모하는 형태, 과금을 유발하는 형태, 정보를 유출하는 형태, 플랫폼을 크로스로 감염시키는 공격 형태 등이 있다. 이러한 위협 환경에 대해, 스마트 폰에 적용될 단말 보안, 보안관리, 앱 스토어 보안, 전자결제 기술 등에 대한 연구가 진행되고 있다.

3.6 모바일 인터넷 보안

모바일을 포함하는 미래 인터넷 연구¹⁵⁾는 콘텐츠 중심, 이동성 중심, 클라우드 중심, 보안성 중심의 네트워크 구조 연구라는 측면에서 접근하고 있다. 콘텐츠 중심의 네트워크 연구는 UCLA를 중심으로 하는 9개 기관이 NDN 프로젝트 이름으로 추진하고 있으며, 이동성 중심의 연구는 Rutgers 대학의 7개 기관이 Mobility First 프로젝트 이름으로, 클라우드 중심의 연구는 펜실베이니아 대학의 11개 기관이 NEBULA 프로젝트 이름으로, 보안성 중심의 연구는 카네기 멜론 대학 외 2개 기관이 XIA 프로젝트 이름으로 추진하고 있다. XIA에서 제시되고 있는 요구조건을 살펴보면, 먼저 사용자나 어플리케이션의 경우 패킷 전송에서의 서비스 유형이나 콘텐츠 유형을 명확하게 표현해야 한다는 점이나, 또 다양한 통신 개체(Principal) ID에 보안을 제공해야 하는데, 호스트간 통신에서 상호 인증과 함께, 전송되는 콘텐츠에 대한 무결성에 대한 검증이 요구되고 있다는 점이다.

4. 결 론

이번 기고에서는 전체적으로 스마트 시대의 주요 정보통신기술과 보안기술에서 동향을 중심으로 밀거림을 그리고자 접근하였다. 유비쿼터스 네트워킹, 전송통신, 스마트 디바이스를 포함한 매체, 모바일 클라우드에 대한 기술적인 이슈를 간략하게 기술하였고, 보안기술과 관련하여, 클라우드 서비스 환경, 개인정보, N 스크린, 스마트 디바이스, 모바일 인터넷 등 관련 환경에서 보안문제를 기술하였다. 끝으로 본 기고에 관련된 기술 사항들은 전자통신기술동향과 정보통신산업진흥원 IT기획시리즈 내용들을 중심으로 고찰된 것임을 밝힌다.

참 고 문 헌

- [1] 유상근, 홍용근, 김형준, “스마트모바일 서비스 - M2M기술 및 표준 동향,” 전자통신동향분석 제26권 제2호(2011. 4)
- [2] 오돈성, 이문식, 김일규, 정현규, “3GPP LTE 기술 개발 및 서비스 동향,” 전자통신동향분석 제25권 제6호(2010. 12)
- [3] 이승윤, 정해원, “차세대 모바일 웹 플랫폼 표준화 동향,” 전자통신동향분석 제25권 제3호(2010. 6)
- [4] 김학영, 민옥기, 남궁한, “모바일 클라우드 기술동향,” 전자통신동향분석 제25권 제3호(2010. 6)
- [5] 이강찬, 이승윤, “클라우드 컴퓨팅 표준화 동향 및 전략,” 전자통신동향분석 제25권 제1호(2010. 2)
- [6] <http://www.nipa.kr>, 정보통신산업진흥원 최신IT동향, “LTE 확산이 가져온 4G와 5G 논쟁”
- [7] 이상일, 정보통신산업진흥원 최신IT동향 - “스마트 디바이스가 몰고 오는 산업지형 변혁에서 모바일 생태계”
- [8] 김무섭, 한종욱, “스마트 카메라 기술동향,” 전자통신동향분석 제26권 제6호(2011. 12)
- [9] 남기효, 김운홍, 정보통신산업진흥원 IT기획시리즈 - “클라우드 서비스 분석 및 보안 이슈”
- [10] 박춘식, 정보통신산업진흥원 IT 기획시리즈- “클라우드 컴퓨팅 보안인증제도”
- [11] 이형효, 정보통신산업진흥원 IT기획시리즈- “클라우드 컴퓨팅 보안 연구에 대한 동향”

15) 이상우 등이 미래인터넷 보안기술동향과 관련하여 전자통신동향분석 제26권 제5호(2011. 10)에서 기고한 바 있다.

- [12] 김정섭, 정보통신산업진흥원 최신IT동향, “ICT시장 변화에 따른 개인정보보호 정책에서 개인정보보호 정책동향과 사업자 대응방향”
- [13] 임형민, 정보통신산업진흥원 최신IT동향, “N-스클린 기반의 저작권 침해대응 기술”
- [14] 이성원, 김중현, 서동일, “이동통신 네트워크 DDoS

공격 및 대응기술 동향,” 전자통신동향분석 제26권 제6호(2011. 12)

- [15] 이상우, 서동일, 조현숙, “미래 인터넷 보안 기술동향,” 전자통신동향분석 제26권 제5호(2011. 10)

● 저 자 소 개 ●



홍진근

경력) 국가보안기술연구소 근무
현) 백석대학교 정보통신학부 교수
국가정보원 암호기술 검증위원, 국가암호포럼 안전성평가분과위원,
정보화진흥원CCTV심의/평가/전략발전위원
국가지요기관 심의/전문/기술/평가위원
관심분야 : 클라우드 보안, 보안SLA, 스마트 보안, 금융보안