ETRI

2013
Electronics and
Telecommunications
Trends

스마트 유무선 네트워크 특집

세이프 네트워크 기술

Safe Network Technologies

송종태 (J.T. Song) 넷컴퓨팅융합연구실 책임연구원
노성기 (S.K. Noh) 넷컴퓨팅융합연구실 책임연구원
박혜숙 (H.S. Park) 넷컴퓨팅융합연구실 책임연구원
박종대 (J.D. Park) 넷컴퓨팅융합연구실 실장
김상기 (S.G. Kim) 스마트네트워크연구부 부장

사이버 테러의 급증으로 인해 사이버 공간에서의 네트워크 역할이 중요해 지고 있다. 이러한 사이버 공격, 정보 유출 등에 의한 국가적 차원의 사이버 안보 위협에 적극적으로 대처하고자 세이프 네트워크기술 개발을 추진 중 이다. 본고에서는 ① IP 주소 은닉기반 라우팅 기술, ② 전역적 제어 관리 시스템 기술 ③ 폐쇄망용 프로텍티드 WiFi시스템기술, ④ 보안을 강화한 네트워크 SW 기술을 주축으로 하는 세이프 네트워크의 핵심기술 및 주요 시스템의 기술개발 동향에 대해 알아본다.

© 2013한국전자통신연구원

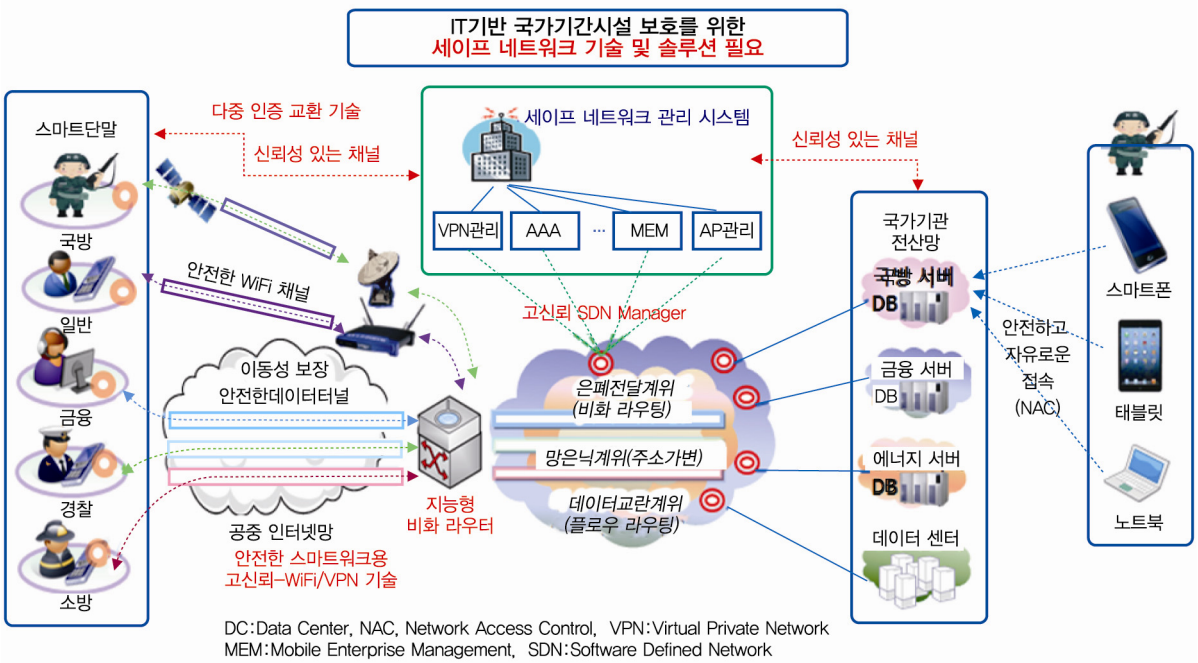
Ⅰ. 세이프 네트워크 개념 및 정의

사이버 테러의 급증으로 인해 사이버 공간에서의 네트워크 역할이 중요해 지고 있다. 특히 폐쇄망인 국가기간망을 효율적으로 사용하면서도, IP 네트워크의 구조적인 취약점을 해결할 수 있는 네트워크 구조 및 장비 개발 필요성이 증대하고 있다[1]. 이에 따라 최근 세계 각국은 사이버 공격, 정보 유출 등에 의한 국가적 차원의 사이버 안보 위협을 미연에 방지하기 위해 적대국, 경쟁국이 생산한 네트워크 장비의 구매를 꺼리는 경향을 나타내고 있다. 2012년10월 미국 하원 정보위원회에서 국가 안보를 이유로 중국산 통신 장비 구매 불가를 선언한 것이 좋은 예이다. 또한 미국에서는 2000년 초부터 국방망/정부망의 세이프 네트워크를 위해 GIG (Global Information Grid)라는 이름으로 신기술 개발 및 구축을 추진 중이다[2]

특히 IoT(Internet of Things)를 비롯한 초연결 시대에 세이프 네트워크 핵심기술 자립이 중요해지고 있으며 가까운 미래에 예상되는 기업, 정부, 공공기관에서 모바일 단말을 활용한 스마트워크 수요 증가 및 클라우드, u-Health, Smart Grid 등 융합형 인프라를 통한 다양한 mission-critical 서비스 증가에 따라 네트워크의 신뢰성은 매우 중요시 되고 있다.

특히 1) 자료의 개방 2) 문제의 개방, 3) 의사 결정의 개방, 4) 예산의 개방, 5) 조직의 개방을 주 내용으로 하고 있는 정부 3.0[3]을 지원하고 창조 경제 실현을 위해 부처별 네트워크 제공은 물론, 서비스 융합 트렌드에 따른 스마트워크 요구를 수용하고 부처 간에 인프라와 정보를 효율적으로 공유하기 위한 세이프 네트워크 기술 개발이 필요성이 매우 높아지고 있다[4].

이러한 필요성으로 인해 세이프 네트워크의 기술개발이 시작되었으며 세이프 네트워크 핵심기술 개발을 통해 국내 기업, 정부, 공공기관의 세이프 네트워크 구축에 활용함은 물론 이를 레퍼런스로 삼아 해외 수출 전략 품목으로 육성하여 국가전략 ICT(Information Communication Technology) 품목으로 발전시킬 계획이다.



(그림 1) 세이프 네트워크 개념도

세이프 네트워크 기술[1]은 ① 외부의 비신뢰적인 통신망으로부터 내부의 신뢰적인 통신망을 보호하기 위한 IP 주소 은닉(비공개) 기반 라우팅 기술, ② 네트워크 접속을 위한 단말/사용자 인증부터 네트워크에 대한 동적인 정책 설정을 통한 지능적 제어 관리를 수행하는 전역적 제어 관리 시스템 기술 ③ 사설망 내부 또는 비신뢰적인(Untrusted) 통신망을 경유하여 상호 연결된 원격에서 기관의 정보 시스템에 대한 접근 및 정보 공유/전달을 위한 폐쇄망용 프로텍티드 WiFi 시스템(단말, AP, 게이트웨이) 기술, ④ 안전한 모바일 OS, 차세대 암호화 SW, 가상화 기반 공격분석/탐지 SW등 보안을 강화한 네트워크 SW 기술로 이루어져 있다.

본고에서는 세이프 네트워크 핵심기술에 대해 알아보고 세이프 네트워크의 핵심 시스템인 전역적 제어관리 시스템과 고신뢰 WiFi 시스템에 대한 국내외 주요 기술 동향을 알아본다.

Ⅱ. 세이프 네트워크 핵심기술

세이프 네트워크 핵심기술은 망은닉 기술, 고신뢰 VPN(Virtual Private Network, 터널링) 기술, 지능형 네트워크 기술로 크게 구분된다.

1. 망은닉 기술

현재 미국 정부는 전세계 네트워크를 미국방성의 가용 네트워크로 만들 수 있어야 하므로 Future Internet이라는 새로운 네트워크 대신에 기존 네트워크상에서 Black Core Network이라는 오버레이 방식을 사용하여 기존 인터넷 인프라를 그대로 활용하면서, 오버레이 기반의 네트워크 보안 장치 및 보안통신 시그널링 기술을 이용하여, 보안성을 요구하는 연결에 네트워크 자원의 배타적 할당과 암호화를 통한폐쇄적 연결 서비스를 제공하고 있다. 망은닉 기술은 이를 더욱 발전 시키는 개념으로 외부의 비신뢰적인 통신망으로부터 내부의 신뢰적인 통신망을 보호하기 위한 IP 주소(서버주소) 은닉하는 기술로써, 고신뢰의 안전한 국가망을 구축할 수 있는 독창적인 기술이다.

이와 유사한 기술로는 TOR(The Onion Routing)[5]기술이 있으며 TOR의 경우 프록시 서버 기반의 가상 네트워크를 구성하여, End-to-End 연결성을 제공하여, 사용자 IP나 개인 정보 등을 남기지 않고 접속할 수 있는 기술로써, 양파(onion) 라우팅이라는 이름처럼 여러 네트워크를 거치면서 자신이 보내는 정보를 겹겹이 암호화하는 방식으로 통신을 한다.

2. 고신뢰 VPN(터널링) 기술

VPN은 인터넷 또는 공용 네트워크를 논리적인 독립 네트워크를 구성하는 기술로써, 모바일 단말을 이용한 스마트워크의 활성화에 따라 보안성을 강화하는 안전한 VPN 기술에 대한 요구가 확산되고 있다.

특히, VPN은 사용자에게 이동 환경을 제공하기 위해서 이동성, 확장성, 관리 용이성, 다중 도메인 지원 기능들이 요구되고 있으나 단일 기술(IPSec, SSL(Secure Socket Layer), GRE, L2TP, MPLS(Multi-Protocol Label Switch), VPN 등)로는 사용자 요구사항을 충족하지 어렵다. 이에 따라 사용자 요구사항을 충족하기 위해 실시간 이용자/서비스 인식 및 이에 따른 트래픽 분리

〈표 1〉 기존 VPN과 본 과제에서 개발하고자 하는 고신뢰 VPN 기술의 비교

기술	기밀성	보안 레벨	사설주소사용	QoS	확장성
암호화기반 VPN	패킷레벨	상	○	중	중
터널기반 VPN	터널레벨	중	○	중	중
정책라우팅 기반VPN	지원하지 않음	하	×	중	하
MPLS VPN	지원하지 않음	중	○	중	상
세이프VPN	패킷레벨	상	○	상	상

및 전달 기술 등 추가적인 기술로 세이프 VPN 기술의 개발이 필요하다. 〈표 1〉은 기존 VPN 기술과 고신뢰 VPN 기술을 비교한 표이다.

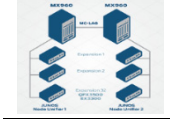
세이프 VPN 기술은 기존 VPN의 취약성을 보완하기 위해서 보안 채널을 통하여 데이터의 기밀성을 보장할 뿐 아니라 서비스 망에 대한 보호가 가능하며 동적으로 다중 도메인을 지원하고, 확장성 제공이 가능한 기술이다.

3. 지능형 네트워크(Intelligent Network) 기술

안정적인 인터넷 사용을 제공하기 위해 멀티미디어 컨텐츠 기반 새로운 응용 및 서비스 증가에 따른 응용별 세밀한 제어 필요성이 증대되고 있다.

특히, 단말 및 서버 중심의 다양한 네트워크 보안 대응 방법이 제시되고 있으나 네트워크 관점의 원천적인 보안 위협을 경감할 수 있는 지능화된 네트워크 장비에 대한 요구가 증대되고 있다. 따라서 지능형 네트워크 장치는 DPI(Deep Packet Inspection)를 이용한 응용 인지 기능, 플로우 기반 QoS 기능, 플로우 단위 통계/패킷 전수 수집 기능, 국가 기관 기밀 데이터의 신뢰성 있는 데이터 전송이 가능한 암호화/복호화 기능을 활용하여 통합 제어 관리와 연계한 솔루션 제공이 필요하다. 〈표 2〉는 주요 장비 제조사의 지능형 네트워크 솔루션을 정리한 내용이다.

〈표 2〉네트워크 장비 제조사의 지능형 네트워크 솔루션의 특징

지능형 네트워크 솔루션	특징
Cloud Intelligent Network (Cisco) 	사설/하이브리드클라우드 서비스 또는 상업적인 엔터프라이즈급 공용 클라우드 서비스 제공 시 사용자의 모든 서비스에 “best effort"보다 높은 수준의 서비스 보장 – 높은 보안 수준 – 예측 가능한 네트워크 및 서비스 관리
MX Series 3D Universal Edge Router (Juniper Networks) 	3D-scaling capability 서비스 제공 – 대역 제어 – 가입자 관리(subscriber management) – 서비스 관리 및 제어 다양한 분야에 대한 고품질의 전송 서비스 제공 – 기업망, 서비스 제공자의 가입자망, 케이블 네트워크, 모바일망 등에 적용
Alcatel Lucent 7750 Service Router	다양한 서비스(mobile, residential, enterprise)를 효율적으로 지원하는 지능적 서비스 라우터 

4. IAM(Identification and Authority Management) 기술

IAM은 아이디와 권한에 대한 관리 기술로, 시스템 내에서 직원, 고객, 계약자 등 사용자를 구분하고 설정된 권한에 따라 권리와 제한 사항을 적용하여 시스템 내 자원에 접근을 제어하는 기술로, 기업 모바일 보안 기술의 주요 항목이다. 최근의 개인 단말의 지능화 및 이동성 지원 요구의 증가, 클라우드의 확산 등에 따라 IAM 기술은 모바일 단말로 엔터프라이즈 클라우드 서버에 접속하는 스마트워크 환경을 안전하게 운용하기 위해서 필수 요구사항이 되고 있다.

이에 따라 IBM, CA Technology, RSA, EMC 등과 Oracle이 안정적인 솔루션과 모바일 기기 회사들과의 파트너십으로 IAM 시장을 주도하고 있으며, RSA/EMC, SafeNet, Gemalto, Symantec 등은 각각 디지털 증명, PKI(Public Key Interchange), 강력한 인증, 하드

〈표 3〉제조사별 IAM 기술의 특징

제조사	기술명	특징
IBM	Tivoli	– 사용자 프로비저닝 – WSSO, ESSO, FSSO – 다중(multi-factor) 인증
CATech-nologies	CA Arcot ID	– 이중(two-factor) 인증 – VPN 인증
SafeNet	SafeNet Authentica-tion Manager	– 컨텍스트 기반 인증 – 모바일망 보안접속 – 확장성 용이
Entrust	IdentityGuard	– 기업망 보안 접속 – 모바일 단말 인증

웨어 토큰 디바이스와 같은 서로 다른 시장에 주도권을 갖고 있다(〈표 3〉 참고).

Ⅲ. 세이프 네트워크 전역적 제어 관리 시스템

전역적 제어 관리 시스템은 기존의 네트워크 제어 관리 기능과 보안 제어 관리 기능을 통합하여 사이버 테러 등의 각종 위협에 능동적 대응을 목표로 구성 장비들을 통합 운용하여 네트워크, 서버 및 서비스를 체계적으로 보호할 수 있는 시스템이다.

네트워크 제어 관리 시스템은 라우터, 스위치 등 네트워크 장비에 대한 구성, 장애, 성능을 모니터링하여, 문제 발생 시 즉각 대응으로 네트워크 문제를 해결하는 시스템으로 EMS(Element Management System), NMS(Network Management System) 등 목적에 맞게 구성하여 계층적으로 관리한다. 네트워크 제어 관리 시스템과 관련된 주요 벤더의 기술동향은 다음과 같다.

IN-SOFT에서는 서버, 네트워크 장비의 전반적인 상태를 모니터링(설정, 버전 정보, CPU, Mem, Disk)하고 장애 발생 시 신속한 장애 처리 프로세스를 가동하여 최적화된 관리가 가능한 Service&System Manager 솔루션을 제공하고 있으며, SECUI.COM의 경우보안 및 네트워크 제어 관리 솔루션으로 UTM(Unified Threat Management) 기능과 IPv6 및 IPTV 등 최신 보안 적용 솔루션 기능을 제공(MF2)하고 있다.

Cisco의 경우 유선, 무선 및 보안 정책을 시각적으로 관리할 수 있는 통합 제어 관리 시스템으로 Cisco사의 스위치, 무선 AP, MSE(Mobility Service Engine) 및 WIPS(Wireless Intrusion Prevention System) 관리가 가능한 통합 솔루션을 제공한다.

Tail-f는 Network-wide 인터페이스(REST, Java, JavaScript, XML)를 통한 네트워크 장비 및 서비스의 접근을 허용하고 있으며, SDN 및 OpenFlow 기반 네트워크 제어 관리가 가능한 솔루션을 제공한다.

IBM은 네트워크 관리 기능을 기존 서버 및 스토리지 관리 기능과 함께 통합해, 하나의 관리 도구를 사용하여 컴퓨팅 환경을 효과적으로 제어할 수 있는 솔루션을 제공한다.

보안 제어 관리 시스템은 기업에서 보안 장비(방화벽, IDS(Intrusion Detection System), IPS(Intrusion Protection System)등을 설치하고, 원격지에서 최적의 보안 시스템 정책 설정, 로그 분석 등을 통해 문제 발생 시 즉각 대응하여 문제를 해결하는 시스템으로 보안의 위협의 증가 및 지능화에 따라 개별 시스템 관리에서 방화벽, IDS, IPS 등 보안 장비들과 로그 관리, 보안성 분석, 접근 통제, 백신 제어 시스템 등을 통합하여, 위험 분석과 위험 관리 기능을 제공하는 시스템으로 발전하고 있다.

JANUS사는 ETRI가 개발한 이상 트래픽 탐지 및 대응 기능이 포함된 플로우 기반의 스마트 라우터와 연동하여 보호 대상 서버의 자원 및 공격 이력 정보 · 공격자에 대한 세부 정보를 제공하는 솔루션을 제공 하고 있으며, A3 Security는 사용자별 자원 접근 정책을 정의하고 예외 상황에 대한 탐지 및 보고 기능이 강화된 솔루션으로 SIEM(Security Information and Event Management)을 제공 하고 있다.

이러한 움직임에 따라 SK텔레콤의 Enterprise Mobility는 적합하고 다양한 보안 기능을 제공하며, 대용량 처리와 높은 보안 수준 제공을 위한 솔루션으로 스마트 디바이스 보안과 관리의 통합적인 제공을 통해 분실 도난 대비, 매체 기능 제어, 애플리케이션 관리가 가능한 솔루션으로 SSM(Smart device Security Management)을 제공하고 있다. 코닉글로리의 경우유무선 위협 데이터를 신속하게 통합해 실시간 탐지/차단 및 경보 기능, 위협 분석 기능, 이벤트 분석 기능, 보안 감사 조회 및 대응 기능, 식별 및 인증 기능, 무결성 검사 기능, 암호화 통신 기능 등을 제공하는 아이에스티엠에

스 v1.0 시스템을 보유하고 있다.

이러한 보안 제어 관리시스템은 방화벽, IDS, IPS, VPN 등과 같은 전통적인 보안 장비들은 특별한 기술발전 이슈 없이 UTM 장비로 통합되는 경향을 보이고 있으며 특히 방화벽의 경우, 서비스 제공자나 데이터센터를 제외하고는 적용 범위가 지속적으로 줄어들면서 단독 장비로 존재하기보다는 UTM 장비에 통합되는 경향을 보이고 있다.

UTM 시장의 선두 기업인 Check Point는 방화벽, VPN, 침입 탐지 및 방지, antivirus 등과 같은 보안 응용들을 통합적으로 제공하는 UTM 장비를 출시하고 있으며, Cisco도 VPN, 방화벽, IPS 와 함께 지능형 라우팅 기능을 통합적으로 제공하고 있다.

Ⅳ. 세이프 WiFi 기술

WiFi는 IEEE에서 802 위원회의 하부 그룹인 802.11 그룹에서 표준화를 주도하고 있으며 WiFi alliance가 802.11 표준에 대한 적합성 인증을 부여하고 있다. 스마트 단말 급증에 따른 모바일 트래픽이 급격히 증가하였으며, 이러한 변화에 대처 방안으로 WiFi 관련 기술이 주목받고 있으며, 일상생활뿐 아니라, 기업의 업무 환경에서도 WiFi가 차지하는 비중이 증가하고 있다.

하지만 WiFi는 전파 수집, 불법 접속, 중간자 공격 등을 통한 사용자 주요 정보 유출과 전파 교란(jamming), 다량의 패킷 전송을 이용한 서비스 거부 공격 등 기술적 보안 위협이 있으며, 취약한 보안 설정을 해킹해 불법 접속 및 내부망으로 침투하는 등 다양한 공격 유형이 가능하여 기술적 보안 취약점을 가지고 있어 중요 업무 데이터 전달 시 기밀 누출에 대한 위험성을 내포하고 있다.

또한 WiFi는 무선랜 장비 및 단말 관리 미흡, 사용자 보안 의식 결여로 인한 침입 허용, 전파 관리 미흡에 따른 외부자의 내부 AP 접속 및 내부자의 외부 AP 접속 허용 등과 같은 관리적 보안 위협이 상존하고 있다. 실제로 2010년, Air Tight Networks사에서 전 세계 27개 공항 대상 무선랜 취약성 조사 결과, 80% 이상이 보안에 취약한 것으로 나타났다. 또한 국내의 경우 전국의 무선 AP 42,997대에 대한 보안 현황 조사 결과, 약 44.8%가 보안이 설정되지 않고 운영되고 있음이 파악되었다[6].

WiFi 보안 취약점에 대처하기 위해 RF 관리, DPI 등을 수행하는 무선랜 제어기, 무선 구간의 신호를 수집, 분석, 대응을 수행하여 불법 AP 및 단말 탐지/차단하는 WIPS 등의 방어 기술이 있다. 하지만 이러한 대응 기술은 무선 구간의 보안 문제점에 주안점을 두기 때문에 유/무선 네트워크 통합 보안 체계에 의한 근본적인 WiFi 보안 대책에 대한 필요성이 대두되고 있다. 구체적으로는 통합 제어 관리를 통한 사용자 인증, CC(Component Compliance)인증 기준에 적합한 암호화 알고리즘 적용, VPN GW(Gateway)와 연동한 AP에서의 화이트리스트를 통한 접근 차단 기술 등이 필요하다.

1. 스마트 워크

세이프 WiFi 기술의 가장 큰 목적 중 하나는 스마트워크 지원이다. 스마트워크는 ICT 기술을 이용하여 언제 어디서나 편리하게 네트워크 상에서 함께 효율적으로 일할 수 있는 근무 형태를 의미한다.

안전한 스마트워크 서비스 제공을 위해 모바일 단말기의 확대에 따른 무선 네트워크 활용도가 증가함에 따라 이와 관련된 보안 관리 기술 요구가 급증하고 있다. 이에 따라 무선 네트워크 접속 구간 보안 대책을 위하여 AP 제어 관리, VPN 등 관련 기술 적용이 필요하며, 서버 접속 구간에 대한 침입 차단/방지 및 보안 제어 관리 등이 필요하다.

2. 스마트 단말 관리

업무 환경 변화(분산화, 모바일화)로 인해 단말을 보호하는 모바일 단말 관리(MDM: Mobile Device Mana-

gement) 솔루션이 스마트워크 도입의 필수 요소로 부상하고 있으며 스마트 단말 관리 기술 특히, 스마트(모바일) 단말은 intelligence, 측위, 다중 센서, 다중 무선 정합 등을 제공함으로써, 업무 생산성 향상을 위한 편의성을 제공하는 스마트워크 핵심 장비로 이에 대한 보안 제어 관리 기술이 요구되고 있다. 기존의 경우 기기 관리와 모바일 보안은 전통적으로 분리 개발되어 쉽게 데이터 보안 침해 및 운영의 비효율성이 발생할 가능성 있다.

스마트 단말 관리 기술은 단말기 기능에 대한 관리/제어를 수행하는 MDM 기능으로부터 어플리케이션 통합 관리/제어(MAM: Mobile Application Management) 및 단말기가 접속하는 데이터/컨텐츠에 대한 관리/제어를 포함하는 MEM(Mobile Enterprise Management) 형태로 발전하고 있다.

전 세계 40여 개 이상의 스마트 단말 관리 솔루션 벤더들은 다양한 플랫폼 지원, 서비스 관리 통합, 비용 관리 및 세계 어디서나 사용 가능한 솔루션 측면에서 차별화를 진행하고 있으며 특히 북미의 경우, 블랙베리 기기와 블랙베리엔트프라이즈(BES)의 조합은 기기 관리 및 보안과 관련된 최적의 표준으로 인정받고 있다.

스마트 단말 관리 시장은 소규모 MDM 벤더들이 난립하고 있으나, 전세계 모든 지역에서 이용 가능한 솔루션은 소수이다. 최근에는 출입 통제 시스템과 연계된 위치 기반 서비스와 주변 기기 지원과 같은 기능들이 차별화 요소로 부각되고 있다.

국내의 경우, 지란지교 소프트는 기존 MDM 기능에 출입 통제 기능을 추가하여 출입 지역에 따라서 스마트폰 일부 기능을 사용하지 못하도록 하는 기기 통제 기능 제공하고 있으며, 인포섹에서는 보안 제어 관리, 보안 컨설팅을 통해 집약된 모바일 보안 기술을 MDM에 결합하여 모바일 오피스용 통합 모바일 보안 솔루션을 제공하고 있다. 안랩은 MDM 에이전트와 관리 서버 외에도 단말기 보안 프로그램인 'V3 모바일엔터프라이즈' 까지 포괄하는 AMC(AhnLab Mobile Center)를 제공하고 있다.

세계시장에서는 마이크로소프트, RIM, Citrix, Good Technology 등이 모바일 단말 관리 솔루션 시장을 주도하고 있다. RIM의 경우 대형 기업의 블랙베리 기기 관리를 위한 사실상의 표준인 BES와 35개 이상의 정책 실행이 가능한 중소기업용 솔루션인 BES Express를 제공하고 있으며 마이크로소프트는 안드로이드, iOS, 팜 OS, 심비안, 윈도 임베디드CE, 윈도 모바일에 대한 기본적인 관리를 위한 EAS(Exchange ActiveSync)를 제공하고있다. Good Technology는 이메일 시스템에서 플랫폼 독립적인 암호화와 특정 어플리케이션을 허가하고 권한을 부여하는 GFE(Good For Enterprise)를 제공하고 있으며, Microsoft Exchange와 Lotus Notes와의 호환성 제공하고 있다. Citrix는 최근 젠트라이즈를 인수하여 XenMobile MDM을 출시하였으며, 2013년 6월 XenMobile MDM과 XenMobile Enterprise의 일부 기능들을 탑재한 XNC(XenMobileNetscaler Connector)와 Netscaler MPX 22000을 출시했다.

3. 복합단말(BYOD: By Your Own Device)기술

스마트 단말 관리 기술을 지원하는 전용 단말에서 스마트 기기 단말 출현으로 인해 개인용과 업무용 기능을 한개 단말기로 수행하는 복합 단말기 형태로 발전하고 있다. 복합 단말기는 한 개의 단말기에 개인용 및 업무용 기능을 동시에 수행하기 때문에 단말기 보안, 개인용/업무용 데이터 분리 관리, 이종 운영체계 사용에 따른 최적화 기술 등이 요구된다.

스마트 단말 솔루션 제공 업체 단위의 데이터 보호 및 암호화가 이루어져 관련 서비스 및 기술이 특정 업체에 종속될 가능성이 있으며 나아가 국가 공공 기관 정보 유출 가능성도 있다. 실재 사례로 모바일아이언사는 관련 제품이 높은 가격임에도 불구하고 고객사의 커스터마이

징 이슈에 유연하게 대응하지 못하는 등 국내에서 요구하는 보안 기능에 대해 충족하지 못하였다. 또한 복합 단말기의 원격 점검으로 인해 업무용 이외에 개인용 데이터 열람이 가능하여 프라이버시 침해 가능이 있다.

VMware는 Horizon Mobile은 가상 드라이브 기술을 통하여 한 개 단말기에 두 개의 운영체계를 두어 개인용과 업무용 운영체계를 분리하는 사용하는 방식을 제공하고 있으며 삼성은 2013년 MWC에서 데이터 센터의 보안 솔루션을 제공하는 centrify사의 기술을 도입한 단말기 보안 솔루션으로 녹스(KNOX)를 발표하였다. 녹스는 Dual Persona의 콘셉트를 적용해 한 개 단말기를 개인용과 업무용 영역으로 구분하고 아이콘 터치로 단말기를 개인용과 업무용으로 전환시킬 수 있는 MDM 솔루션으로 하나의 단말기에 암호화된 'Container'라는 별도 저장 공간을 마련하여 AES 256bit key로 암호화하여 업무용 데이터를 저장하고 있다. 하지만 녹스, VMware Horizon Mobile의 솔루션의 경우 협력업체에 한해서만 API를 제공하여 기능 구현 및 기술 지원에 한계가 있다.

기업망을 중심으로 개발된 현재의 스마트 단말기 관리의 국가 공공망에 적용을 위해서는 네트워크와 연계된 강화된 보안 기술이 추가되어야 하며 데이터 보안 등급에 따른 차별화된 보안 알고리즘(ARIA, SEED)을 적용한 데이터 암호화 및 관리 기술, 서비스 구역 내의 보안 등급 지역에 따른 차별화된 접속 인증/허가 기술, MAC, IP 어드레스, IMEI(International Mobile Equipment Identity)/IMSI(International Mobile Subscriber Identity), USIM(Universal Subscriber Identity Module)정보 등 다양한 정보를 활용하는 mPAK인증 기반 등이 통합적으로 이루어져야 한다.

V. 결론

앞에서 살펴본 바와 같이 세이프 네트워크 기술은 네트워크뿐 아니라 단말, 무선, 서버 등의 다양한 기술이 결합되어 이루어지는 기술로 IoT를 비롯한 초연결 시대로 발전함에 따라 사이버 위협으로부터 방어를 위한 네트워크의 역할이 증가하고 있으며 이에 따라 세이프 네트워크 기술의 중요성이 커지고 있다.

용어해설

세이프 네트워크 기술 기밀성, 가용성, 품질, 이동성 등의 관점에서 비신뢰적인(untrusted) 통신망을 통해 단말, 서버 및 네트워크 기기 간에 신뢰적인 (trusted) 통신을 가능하게 하는 네트워크 기술을 의미하며, 세이프 네트워크 기술 개발을 통해서 ① 동적 은닉 기술을 통한 국가 기간 시설을 보호하고, ② 조직/응용별 안전한 동적 네트워크 구성으로 네트워크 간 실시간 정보 유통이 가능하며 ③「퍼스널 모바일 원격 오피스」 환경 제공이 가능함.

약어 정리

BYOD	By Your Own Device
CC	Component Compliance
DPI	Deep Packet Inspection
EMS	Element Management System
GIG	Global Information Grid
GRE	Generic Routing Encapsulation
GW	Gateway
IAM	Identification and Authority Management
ICT	Information Communication Technology
IDS	Intrusion Detection System
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IPS	Intrusion Protection System
MAM	Mobile Application Management
MDM	Mobile Device Management
MEM	Mobile Enterprise Management
MPLS	Multi-Protocol Label Switch
MSE	Mobility Service Engine
NMS	Network Management System
PKI	Public Key Interchange
SSL	Secure Socket Layer
SSO	Single Sign On

TOR	The Onion Router
USIM	Universal Subscriber Identity Module
UTM	Unified Threat Management
VPN	Virtual Private Network
WIPS	Wireless Intrusion Prevention System

참고문헌

[1] KEIT PD Issue Report, "세이프네트워크 기술", 2013.4.

[2] R.Cieslak, "GIG 3.0 Design Factors," Public Intelligence, http://info.publicintelligence.net/USPACOM-GIG.pdf

[3] 관계부처 합동, "정부 3.0 추진 기본계획," 2013.6.19

[4] 한국인터넷 진흥원 보고서, "2012 국내 지식정보보안산업실태조사," 2012.11.

[5] TOR Project Site, https://www.torproject.org

[6] 한국 인터넷 진흥원 보고서, "2010 해킹. 바이러스 현황 및 대응," 2010.10.