情 報 保 護 學 會 誌
第21卷 第3號, 2011. 5

안전한 스마트워크 향상을 위한 Mobile Security 대응모델에 관한 연구

황 해 수*, 이 기 혁**

요 약

최근 정보통신의 발달은 기업의 업무환경을 기존의 PC기반에서 스마트폰을 이용한 모바일오피스 환경으로 변화 되고 있다. 스마트폰을 이용한 스마트오피스(Smart Office)는 언제 어디서든 기업 인트라넷에 접속하여 업무를 처리할 수 있는 반면 그로 인한 보안위협에 노출되는 보안위협도 가지고 있다. 개인사용자 대상의 보안사고와 달리 기업의 보안 사고는 상당한 비용적인 피해를 발생시킬 수 있고, 사회적 피해의 범위 또한 광범위하다. 이러한 스마트 오피스 환경에서 보안 피해를 최소화 하기위해 정책과 기술, 그리고 운영에 이르는 서비스 전반적인 관점에서 대응 가능한 모바일 보안모델을 제안한다. 본 논문에서는 기업고객을 대상으로 하는 B2B 비즈니스에서 스마트오피스 도입 시 예상되는 보안위협과 이를 해결하기 위한 모바일보안 대응모델을 연구하여, 안전한 Smart work 환경에서 업무의 향상을 제공할 수 있을 것으로 기대한다.

Ⅰ. 서 론

최근 스마트폰[1]의 급속한 보급으로 인해 기업의 업무 형태가 바뀌고 있다. 스마트폰은 기존 폐쇄적인 WIPI플랫폼기반[2]의 휴대폰과 많은 점에서 차이가 있다. 스마트폰은 운영체제(GPOS, General Purpose OS)의 개방성, 어플리케이션 개발을 위한 공개 API(Application Programming Interface) 제공, 다양한 네트워크 인터페이스 및 신규 모바일서비스와의 융합, PC급 수준의 H/W 사양과 이동성(Mobility)이 우선적으로 고려된 손안의 PC라고 정의할 수 있다. 일반 PC에서 가능한 인터넷 접속, 일정관리, 전자메일, 문서작성, 전자상거래 등의 서비스는 물론 소셜 네트워크(SNS, Social Network Service)와 증강현실(AR, Augmented Reality)같은 신규서비스도 스마트폰에서 편리하게 제공되고 있다.

기업에서도 스마트폰을 이용하여 업무효율성을 높이려는 시도가 증가하고 있다. 언제 어디서든 사내 인트라넷에 접속할 수 있는 환경을 제공하여 회사업무를 처리하기위해 스마트오피스(Smart Office)를 도입하는 회사나 공공기관 및 단체 등이 증가하고 있다. 하지만 스마트폰에서 발생할 수 있는 보안 문제는 스마트오피스 도입 이전에 충분히 고려해야 할 필요가 있다. PC기반에서 처리하던 주요업무가 스마트폰으로 확장되므로, 기존 PC 기반에서 발생 가능한 보안위협이 스마트폰에서도 재현될 수 있기 때문이다. 또한, 스마트폰만의 특징을 이용한 신규 보안위협이 존재할 수 있다. 예를 들면, 기존의 PC기반에서 노트북 분실로 인한 정보유출 위험도 대비 스마트폰은 작고 가벼운 이동성으로 인해 분실위험[3]이 상대적으로 더 큰 것으로 볼 수 있다. 그리고 PC기반에서는 데이터 도청 시 반드시 회사 내부 망에 접속하고 있어야 하나, 스마트폰의 경우는 Wi-Fi, 3G (WCDMA), Bluetooth, PC동기화를 이용한 다양한 유/무선통신 기능을 지원하므로 음성 및 데이터 도청으로 인한 정보유출의 위험 범위가 더 확대된 것으로 볼 수 있다.

스마트 오피스에서 주요 보안위협은 다음과 같이 다섯 가지 이슈를 언급할 수 있다. 첫 번째는 스마트폰 악성코드를 들 수 있다. Open-market에서 악성코드에 감염된 컨텐츠를 소비자가 구매하여 스마트폰에 설치 및

* 인포섹(주) 컨설팅사업본부 수석컨설턴트
** SK Telecom 정보기술원 IT보안팀 팀장

실행 하였을 경우 악성코드는 스마트폰에 저장된 개인정보 및 기업 내부 정보가 변조 및 유출될 수 있으며, 이로 인해 기업은 정보자산의 금전적 손실과 브랜드가치 저하 등의 피해를 입게 된다. 두 번째는 기업 내부의 인트라넷 시스템에 대한 침입이다. 기밀정보의 유출이나 내부 시스템의 가용성을 침해하여 기업에 직접적인 피해를 발생시킬 수 있다. 기존 IT인프라 시스템과 연동을 제공하는 스마트 오피스는 다양한 네트워크(WCDMA, Wi-Fi, WiBro)를 통해 언제, 어디서든 기업내부 인트라넷까지 접속할 수 있는 위협에 노출되어 있다. 세 번째는 스마트폰을 통한 분산서비스거부(DDoS, Distributed Denial of Service)[4]공격이 발생할 수 있다. 기존 PC기반의 DDoS 공격은 기업의 네트워크에 가용성 피해만을 발생시킨 반면, 스마트폰을 이용한 DDoS 공격은 네트워크 가용성 피해와 더불어 원하지 않은 트래픽 발생으로 인해 스마트폰 사용자에게 요금부담을 발생시킬 수 있다. 또한, 통신사업자 입장에서는 WCDMA망에 DDoS로 인한 가용성이 저해되는 경우 음성서비스와 데이터서비스에 치명적인 피해를 발생시킬 수 있다. 네 번째는 스마트폰 분실, 도난으로 인한 위협으로 스마트폰에 저장 된 개인정보와 기업 내부정보의 외부유출 이 발생 될 수 있으며, 실 사례로 현재까지 분실 및 도난 위험이 가장 많은 비중을 차지하고 있다. 스마트폰에 저장된 데이터를 보호할 수 있는 보호대책이 제공되지 않은 상태에서 도난 및 분실은 기업에 직접적인 비용손실을 발생시키는 보안위협으로 볼 수 있다. 마지막 다섯 번째는 도청으로 인한 보안위협이다. 기업에 적용되는 스마트오피스 서비스에서 음성통화는 대부분 업무적인 내용이 많다. 이러한 업무전화 내역이 도청되어 악용되는 경우 기업의 정보자산 유출과 프라이버시 침해 까지 확산될 수 있다.

이러한 이유로 스마트폰을 중앙에서 통합관리가 가능한 MDM(Mobile Device Management)[3]과 같은 단말 보안관리 솔루션이 스마트폰 보안시장에 지속적으로 출시되고 있다. 하지만, 서비스 전 영역에서 발생할 수 있는 다양한 보안위협을 대응하기에는 분명한 한계가 있다. 이와 같이 산재해 있는 모바일 위험으로부터 안전한 스마트 오피스 환경을 제공하기 위해 서비스 전반에서 발생할 수 있는 보안위협에 대한 대응전략이 필요하다. 본 논문에서는 기업 입장에서 스마트 오피스 환경에 존재하는 보안위협을 대응하기 위한 모바일보안 대응모델을 제안하여 모바일 보안사고를 능동적으로 대응하고자 한다.

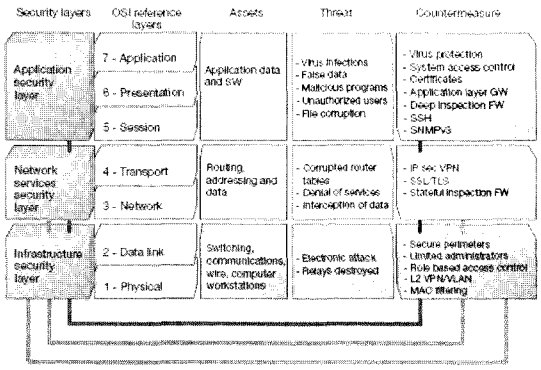
보안위협은 스마트폰 단말에서 발생하므로 스마트폰 보안위협으로 볼 수 있으나, 본 논문에서 제시하는 모델은 스마트폰과 모바일생태계(Mobile Ecosystem)[5]에 해당하는 다양한 복합단말(Compound Terminal, All-in-one Mobile Device), Tablet PC 등을 대상으로 한 서비스 전 영역 관점에서 보안을 고려하므로 스마트폰 보안을 포함하는 모바일보안 모델로 정의하였다. 또한, 스마트오피스는 Smrt work, Connected Workforce 등으로 기업에 적용되고 있다. 개념정의 측면에서 스마트오피스는 기업차원에서 광의적인 업무연장개념이며, Connected Workforce는 특정기업에서 부여한 개념적인 측면이 강하다. 본 논문에서는 기업의 이동성업무에 선제적인 보안기능을 적용할 수 있는 보안모델을 제시하기 위하여 Smart work를 스마트오피스와 Connected Workforce의 개념으로 선정하였다.

Ⅱ. 선행연구

Yin Zhiyu[6]는 기업내에서 무선 Smrt work 시스템의 보안 문제를 SSL VPN, AES(Advanced Encryption Standard), ECC(Elliptic Curve Cryptography)를 사용하여 해결할 수 있는 모델을 제안하였다. 이 연구는 SSL-VPN 게이트웨이를 이용하여 안전한 인증, 보안탐지 및 인가를 제어하고 안전한 데이터 전송을 위해 ECC, AES 암호화 알고리즘을 사용하여 RF통신상의 보안위협을 해결 할 수 있다고 제안하였다. 하지만, 이러한 표준프로토콜 기반의 암호화 전송은 무선통신에서 발생하는 보안위협에만 치중 된 것으로, 단말의 서비스 종류에 따른 보안수준을 정의하여 적용할 필요가 있다. 기업 및 공공기관에서 중요한 내부 네트워크 접속을 위해 PKI(Public Key Infrastructure)와 같은 공인인증서를 사용하는 경우가 대표적인 예로 볼 수 있다.

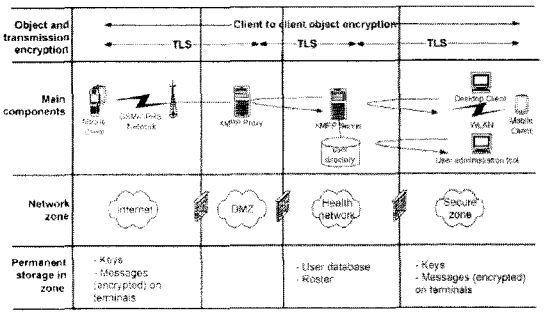
IBM[7]은 모바일에서 발생할 수 있는 보안위협에 대비하기 위해 다음과 같은 11개의 보안프로세스 필요성을 강조하였다. 위험관리(Risk Management)는 위험 발생 이전, 발생 인지, 발생 후의 3단계 측면에서 효과적인 대응을 위한 관리를 의미한다. 사고관리(Incident Management)는 보안사고 발생 시 조직적이고 체계적인 대응을 의미하며, 보안검증(Security Validation Assurance)은 다양한 업무 프로세스에 보안 등급을 부여하는 작업을 의미한다. 이 외에 모니터링(Security Mo-

nitoring), 변화관리(Change Management), 기업보안정책(Corporate Security Policy), 보안아키텍처(Security Architecture), 기술표준 및 정책(Technical Standards and Policies) 개인정보정책(Privacy Policy), 사용자 정책 적용 룰(User Rules), 기업보안조직(Corporate Security Organization), 사고대응팀(Incident Response Team) 프로세스가 있다. 이러한 보안 프로세스는 보다 효과적으로 보안을 업무에 적용하여 보안위협으로부터 안전한 업무를 진행하기 위한 것으로, 기업 업무 프로세스의 대부분에 적용되어야 할 필요가 있음을 강조하고 있다. 하지만, 이러한 프로세스 중심의 보안적용 방안은 많은 시도가 있었으며, 각 프로세스 영역 별 상세화 된 기술 및 수행방법을 기업의 다양한 요구에 적용하는데 한계가 있다.



〔그림 1〕 Ericsson의 네트워크 레이어 기반 보안모델

Ericsson[8]은 모바일 보안을 OSI Reference Layer 관점에서 접근하고 있다. 기본 전략은 OSI 7 layer를 3개의 Security layer로 분류한다. Physical, Data link layer를 Infrastructure security layer로 정의하고, Network, Transport layer를 Network services security layer로 정의한다. 마지막으로 Session, Presentation, Application layer를 Application Security layer로 정의한다. 이와 같이 3개의 Security layer에 속하는 자산과 위협을 분류하고, 각 Security layer에 맞는 대응책을 Deter, Protect, Detect, Respond, Recover 프로세스에 적용하여 효과적인 보안대응을 강조하였다. 하지만, 스마트폰 단말관점에서는 단말과 네트워크 영역까지 고려하여 안전한 서비스를 제공할 수 있으나, 모바일보안 관점에서는 서비스 전 영역을 고려해야 하므로 서비스를 제공하는 서버, 사용자 및 정보영역에 대한 보안도 고려해야 할 필요가 있다.



〔그림 2〕 MedImob 시스템 아키텍처

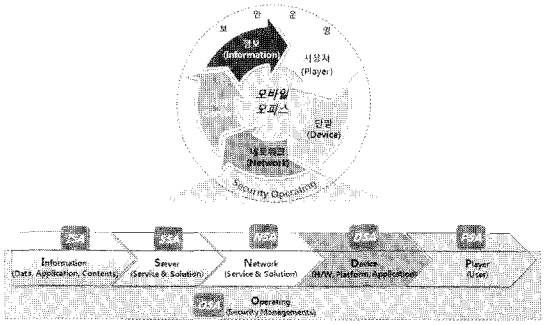
[그림 2]의 MedIMob[9] 아키텍처는 의료기술 분야에 모바일 인스턴트 매시징 시스템(Mobile Instant Messaging System)을 이용한 정보보안 위험분석모델이다. 이동 중에도 실시간으로 즉시적인 IM(Instant Messaging)정보를 PC와 모바일 단말간 송수신하기 위해 제안한 모델로, 민감한 의료정보를 효과적으로 보호하기 위해 서비스 구간 별 영역을 구분하였다. 그리고 정보의 분석방법을 제시하여 위협과 위험수준을 도출하였고, 보호해야 할 정보를 선정하는 모델을 제시하였다. 그러나, MedIMob 모델은 스마트폰이라는 특성을 적절히 반영하지 않은 모델이며, 아키텍처는 단말, 네트워크, 서버의 3개 구간만으로 분류하여 암호화통신(TLS, Transport Layer Security)을 적용하였다. 이러한 분류방법은 다양한 서비스 환경과 지속적으로 발전하는 Smrt work의 스마트폰 보안 환경에서는 적합하지 않다.

Ⅲ. 제안모델

기업은 Smart work를 이용한 업무 향상과 안전성 모두를 추구하기 위해서는 보안을 고려한 모델이 제시 될 필요가 있다. 본 장에서는 안전한 스마트폰 보안 모델을 구체적으로 제시하기 위해 스마트폰 서비스의 정보제공 흐름과 이벤트 발생관점에서 그림 3과같이 대상을 구분하였다. 본 논문에서는 Smrt work 서비스의 주 대상을 스마트폰으로 정의하였으나, Smart work를 지원하는 모든 휴대용단말에 적용 가능할 것이다.

보안은 스마트폰 서비스의 전 영역에 걸쳐 고려해야 하며, 그러기 위해서는 서비스 영역을 상세화하여 구분하기 위한 보안기준이 있어야 한다. 이러한 서비스 영역을 보안 관점에서 구분하는 것은 보안위협의 효과적인

결과를 가질 수 있다. 본 제안모델에서는 보안위험과 피해규모를 고려하여 그림 3과 같이 구분하였다. 그림 3에서 상단의 원을 기업의 업무프로세스 관점으로 보면 하단과 같이 표현할 수 있다.



〔그림 3〕 모바일보안 대응모델을 위한 주요 보호대상 및 보안서비스 영역 구분 기준

구분 된 각 보안영역의 정의는 다음과 같다. ISA(Information Security Area)는 사용자에게 송/수신되는 컨텐츠, 어플리케이션을 포함 한 단일 데이터 또는 모든 데이터의 집합체를 의미하며, SSA(Server Security Area)는 사용자의 단말과 정보를 전달하기 위한 기반시스템 중 정보의 저장과 공유를 위한 게시 및 사용자의 요청에 응답하기 위한 서버시스템에 해당한다. NSA (Network Security Area)는 사용자의 단말과 서버시스템 간 허용 된 정보만을 전달하기 위한 네트워크 기반시스템이며, DSA(Device Security Area)는 사용자에게 장소와 시간의 제한 없이 정보를 송수신하는 스마트폰 단말로 정의할 수 있다. PSA(Player Security Area)는 스마트폰을 이용하여 네트워크를 통해 서버에 정보를 요청하고 생성하는 사용자로 정의할 수 있다. 마지막으로, OSA(Operating Security Area)는 ISA부터 PSA까지 적용 된 보안운영측면에서 필요한 보안관리를 의미한다. OSA는 각 영역에서 필요로 하는 모든 보호대책별 운영의 범위가 광범위하므로 본 논문에서는 언급하지 않을 것이나, 각 영역에 도출 된 보호대책의 운영이 해당된다고 보면 될 것이다. 이와 같이 구분 및 정의 한 보안영역을 적용했을 때 다음과 같은 효과를 기대할 수 있다.

- 정보의 흐름순서대로 보안위협과 보호대책을 도출하여 상호 이해를 높일 수 있다.
- 각 보안영역 별 보호해야 할 정보를 선정하여 비교함으로써 중복과 누락을 최소화 할 수 있다.
- 각 영역간 상호연관성을 고려하여 최소의 비용과 노력으로 중요정보를 선별 및 집중하여 보호할 수 있다.

이와 같이 구분 된 각 영역의 보안위협과 보호대책은 명확하게 구분되어 적용되지 않을 수 있다. 그 이유는 한 영역에서 발생 된 보안위협이 타 영역에도 영향을 미칠 수 있고, 동일한 보안위협이 여러 영역에서도 발생할 수 있기 때문이다. 그러므로 중복된 보안위협과 보호대책이 제시될 수 있다. 본 논문에서 제안하는 모델은 이러한 중복을 최소화하고 효율적으로 중요한 정보를 보호할 수 있는 방법을 제시하는 이유이다.

본 논문에서 제시하는 모델의 위험분석 도출 방법은 스마트폰 서비스의 보안 관점에서 발생할 수 있는 보안위험을 "발생 가능성"과 "위험영향도"의 비교 Matrix에 적용하여 위험수준을 도출하였다. 즉, 모바일 환경에서 발생할 수 있는 위험 빈도수를 "모바일 위험 발생가능성(Mobile Risk Likelihood)"으로 정의하였고, 기업정보의 유출 및 서비스 연속성에 영향을 주는 피해를 "모바일 위험영향도(Mobile Risk Impact)"로 정의하였다.

B2B인 Smrt work환경에서 보안위협은 B2C의 보안위협과 동일한 수준으로 볼 수 있다. 그러나 B2B인 Smrt work 환경에서는 발생할 수 있는 피해의 규모 측면에서 광범위하며, 이러한 이유는 그림 3에서 구분 한 보안영역을 기준으로 간략히 언급하면 다음과 같다.

- *Server* 보안영역: 회사기밀정보를 보관하고 있는 사내 인프라 시스템을 대상으로 한 해킹공격으로 서버시스템의 가용성을 저해하는 보안위협
- *Network* 보안영역: 다수의 스마트폰 단말에서 악성코드가 WCDMA, Wi-Fi 망을 통해 의도하지 않은 트래픽을 일시적으로 발생시켜 네트워크의 가용성 저해하는 보안위협
- *Device* 보안영역: 기밀정보를 저장하고 있는 단말에서 악성코드 및 해킹을 통한 정보유출 보안위협
- *Information* 보안영역: *Server, Network, Device* 및 *Player*에서 발생하는 정보의 무단유출 보안위협 관련
- Player: *Device, Information*에서 발생하는 모든 보안위협과 관련

본 제안모델에서는 스마트폰의 B2C에서 발생 가능

한 보안위협과 동일한 수준에서 보안위협을 다룰 것이며, 보호대책은 Smrt work 환경에 필요한 B2B 보호대책을 선정하여 제시 할 것이다. 이와 같이 구분 된 보안영역 별 위협과 보호대책은 다음과 같이 상세화 하였다.

3.1 Information 보안 영역 (ISA, Information Security Area)

[표 1]의 보안위협에 대응할 수 있는 보호대책은 다음과 같이 정의할 수 있다. Mobile Firewall은 모바일 단말에서 발생하는 통신 트래픽을 모니터링하여 허용되지 않은 포트의 송/수신 이벤트 발생 시 알림 또는 제한 기능을 제공한다. Mobile Anti-Virus는 모바일 단말에서 악성코드(바이러스, 웜, 트로이목마, 스파이웨어)의 감염을 알리고 치료하는 기능을 제공하며, Code Sign은 서버에서 단말로 어플리케이션 다운로드 시 어플리케이션의 무결성을 보장하는 기능 제공한다. Two-Factor 인증은 단일 인증과정이 아닌 개인이 보유 또는 유추할 수 있는 정보를 입력받아 2회 이상의 인증과정을 거치는 것으로, 개인이 보유한 정보는 생체 고유의 인식 가능한 기능(홍채, 지문 등) 또는 타 기기(OTP, One Time Password, 보안카드, 단말인증 등)를 이용한 인증 등을 포함하는 기술이다.

DRM(Document Right Management)은 저작권이 있는 컨텐츠 및 파일의 사용을 허용된 사용자에게만 제한하거나, 파일의 암호화 및 권한제어를 수행하여 허용된 사용자에게만 파일의 접근을 허용하는 기능을 제공한다. PKI(Public Key Infrastructure)는 메시지의 암호화 및 제 3의 공인기관을 통한 전자서명으로 보안시스템 환경을 제공하는 기술로 주로 인증서(Certificate) 제공을 위한 보안서비스에 사용된다. SSL/TLS (Secure Socket Layer/Transport Layer Security)는 네트워크 또는 인터넷 접속에서 데이터나 메시지 전송의 안전한 보안통신을 제공하는 암호 프로토콜이며, 보안 API는 플랫폼 또는 어플리케이션 레벨에서 보안 API를 제공하여 개발 시 암호화 기능을 개발자에게 제공하는 것을 의미한다.

Device Management는 원격에서 단말의 보안 업데이트(Anti-Virus, 플랫폼 보안패치, 펌웨어 업데이트), 분실 시 원격 데이터 삭제, 사용제한 등의 기능을 제공한다. 마지막으로, Secure Kernel은 Kernel 자체의 보호 및 암호화 기능과 Device에 대한 Security Kernel 외 접근경로의 제거기능, 보안 커널이 정상적으로 동작하고 있는지 감시하는 기능, 보안 커널에 대한 비정상적인 접근에 대한 로그와 같은 커널수준의 보안기능을 제공한다.

3.2 Server 보안 영역 (SSA, Server Security Area)

SSA와 NSA(Network Security Area)의 보호대책 구분기준은 Network의 다양한 보안검증을 통해 충분히 안전하다고 판단 된 패킷이 기업 내의 주요 서비스영역에서 처리 되는 것을 기준으로 구분하였다. 이러한 기준으로 구분 된 SSA의 보안 위협은 표 2와 같다.

[표 2]의 보안위협에 대응할 수 있는 보호대책은 기존 Legacy IT 인프라에 적용된 보안기술과 유사하며,

〔표 1〕 ISA에서의 보안위협

보안위협	설명
악성코드	웜, 바이러스, 트로이목마, 스파이웨어와 같은 Malware 공격
모바일 어플리케이션 취약점/에러	어플리케이션의 취약점, 에러를 이용한 권한획득 및 인증우회
스팸	홍보성 또는 사회공학적 정보를 악이용한 공격
지적재산권 위반	S/W license를 불법 위반하여 사용하여 발생하는 공격
인증우회 및 사용자 가장	인증 루틴을 임의 우회하도록 코드를 재수정하거나 타 사용자 가장
사용부인	어플리케이션이나 해당 정보를 사용하지 못하게 하는 행위 및 공격

〔표 2〕 SSA에서의 보안위협

보안위협	설명
서버 OS 취약점	서버 운영체제의 취약점을 이용한 공격
서버 어플리케이션 취약점	운영체제에서 동작하는 (WEB)어플리케이션의 취약점을 이용한 공격
악성 어플리케이션 업로드/배포	악성어플리케이션의 서버업로드 및 사용자 배포에 의한 위협
악성코드 내포/감염 컨텐츠	악성코드(바이러스, 웜, 트로이목마, 스파이웨어)가 내포 및 감염 된 컨텐츠 배포
소스코드 취약성	서버의 서비스 웹페이지에 소스코드 보안 취약점에 의해 노출 된 취약점 공격

〔표 3〕 NSA에서의 보안위협

보안위협	설명
비인가 네트워크 송/수신	허용되지 않은 네트워크 트래픽의 송/수신으로 인한 트래픽 과다 점유로 타 사용자의 서비스 품질에 악영향을 미치는 행위
도청	사용자의 음성통화를 타 사용자가 도청하여 개인정보가 유출되는 행위
방해전파 발신	방해전파를 발생시켜 해당 전파범위내의 사용자에게 정상 통화를 방해하는 행위
Rogue AP	악의적인 목적으로 위장한 무선랜 중계기를 이용한 공격
유해 트래픽 (Flooding)	네트워크에 다량의 트래픽 유발로 전체 네트워크의 처리 수준을 떨어뜨리는 행위
기지국/Core망 공격	악의적인 목적의 사용자가 기지국 및 Core망 공격으로 인한 침해행위

각각의 내용은 다음과 같다. Secure OS는 서비스 제공을 위한 서버에서 다양한 보안기능을 제공하기 위해, 기존의 운영체제에 보안 기능이 통합된 보안커널(Security Kernel)을 이식한 보안운영체제다. 서버시스템 자체를 통제하는 OS에 보안기능을 부여하여 보다 강화된 보안기능을 제공하는 보호대책이다. DB보안은 대량의 정보를 효율적으로 관리하는 DB에 정보의 삽입, 검색, 수정 및 백업에 이르는 대부분의 작업을 안전한 절차를 거쳐 접근할 수 있는 정보처리 보안시스템이다. 서버보안 운영교육은 다양한 형태의 서버를 관리하는 운영자를 대상으로 한 서버관리 보안교육을 위한 지침서 또는 교육서를 통한 교육으로 안전한 운영자 관리를 유도하는 보호대책이다. SMS/MMS, E-mail 대상의 Filtering System은 네트워크를 통해 서버에 Inbound/Outbound 되는 모든 패킷을 대상으로 스팸, 악성코드, 피싱(Phishing) 등의 내용 포함여부를 검사하고 제거하는 시스템이다.

3.3 Network 보안 영역 (NSA, Network Security Area)

NSA는 사용자와 컨텐츠 제공자가 보안적인 측면에서 능동적으로 관여하기에는 통신사업자 위주의 서비스로 보호대책 수립에 제한이 많은 영역이다. 그러므로 발생 가능한 보안 위협대비 적용 가능한 보호대책은 제한적임을 참고하여, 보안위협과 보호대책은 다음과 같이 정의할 수 있다. Network Firewall(방화벽)은 서버 관리 영역에 인입되는 모든 패킷을 대상으로 공격성향이 있는 패킷을 IP와 Port 수준에서 1차로 구분하는 기능의 네트워크 방화벽이다. Network IPS(Intrusion Prevention System)는 방화벽을 통해 인입 된 패킷 중 공격적 형태(Signature)를 갖는 패킷을 DPI(Deep Packet Inspection)[10]기반 기술로 패킷의 헤더(Header)와 페이로드(Payload)에 포함 된 데이터까지 심층적으로 분석하여 비정상 트래픽을 탐지 및 차단하는 네트워크 시스템이다.

Web Firewall은 웹 포트를 통한 공격형태를 감지하여 보안차단하기 위한 네트워크 시스템이며, Anti-DDoS는 분산 된 불특정 다수의 좀비(Zombie) 단말로부터의 공격을 방어하기 위한 패킷 감지시스템이다. Viruswall은 HTTP, FTP, E-Mail(SMTP, POP3, IMAP) 패킷을 통해 전달되는 악성코드 중 파일에 탑재 된 악성코드를 스캔하는 안티바이러스 시스템이다.

3.4 Device 보안 영역 (DSA, Device Security Area)

[표 4]의 보안위협에 대응할 수 있는 보호대책은 다음과 같이 정의할 수 있다. Secure Storage는 단말에 저

〔표 4〕 DSA에서의 보안위협

보안위협	설명
펌웨어 취약점	단말의 펌웨어 보안 취약점을 이용한 공격
모바일 플랫폼 취약점 및 위/변조	플랫폼 내부의 취약점이나 특정 영역을 변경하여 보안 공격을 하기 위한 상태로 만드는 행위
인터넷 브라우저 취약점	다양한 웹 어플리케이션이 동작하는 웹 브라우저의 취약점을 이용한 공격
단말 분실/도난/재사용	분실, 도난으로 인한 악의적 사용자의 단말 재사용 행위
불법 위치 추적	GPS기반의 개인 위치를 악용할 수 있는 보안위협
전자기 펄스 및 부하로 인한 장애	악의적 목적으로 전자기 펄스나 전원 과부하를 발생시켜 단말에 고장이나 전원을 방전시키는 공격
평문저장 된 개인정보 유출	암호화 되지 않은 개인 정보의 외부유출 공격
악성코드 및 단말해킹	악성 코드 감염에 의한 기기 오작동, 개인정보 유출 및 어플리케이션 이상 행위나 OS루팅을 통한 보안 설정 해제, 시스템공격
인증우회	단순 패스워드 등 취약한 인증 체계의 인증우회를 통한 사용자정보 침해

장되는 개인 데이터를 자동으로 암호화 저장하는 기능으로, 해킹에 의한 외부 유출 시에도 개인정보를 보호할 수 있는 보호기능이다. mTPM은 TPM(Trusted Platform Module)을 모바일에 적용한 H/W기반의 공통보안 핵심모듈 기술로 사용자 인증, 플랫폼 인증, 기기 인증, 데이터 보호 및 무결성 보장 등 플랫폼에 인가되지 않은 접근 및 수정을 감지하기 위한 보호대책이다. Device 인증은 모바일 디바이스 자체를 인증하기 위해 인증서를 적용하여 허용 된 디바이스에서만 특정 외부와 접속될 수 있는 기술로, 컨텐츠 보호차원의 효과와 디바이스의 불법 유통을 차단하는 효과를 기대할 수 있다.

3.5 Player 보안 영역 (PSA, Player Security Area)

PSA는 사용자를 대상으로 한 보안위협으로 DSA와 ISA에서 발생되는 보안위협의 직접적인 대상에 해당한다. 그러므로 보안위협은 DSA와 ISA에 해당하는 영역과 유사하다고 볼 수 있으며, 사용자의 보안위협 행위에 직접적으로 관련되는 보안위협은 표 5와 같다.

〔표 5〕 PSA에서의 보안위협

보안위협	설명
사회공학적 위협	Phishing과 같은 사회공학적 공격
지적재산권 위반	정상 구매 어플리케이션이 아닌 Crack 된 불법 유료버전을 사용하기 위해 검증되지 않은 사이트에서 발생되는 Side-loading 행위
사용자보안설정 미숙/부주의	사용자의 보안인식 미숙으로 발생되는 보안위협

PSA의 보안위협에 대응하기 위한 보호대책은 다음과 같이 정리할 수 있다. 스마트폰을 이용한 Smrt work 사용자를 대상으로 보안가이드 및 변화관리로 사용자의 보안 사고방지와 보안사고로 인한 피해 인식확대를 기대할 수 있다. 또한, 지속적인 홍보 및 여론조사를 통해 변화관리 방안을 제공하여야 한다. 정책 수립 및 적용 방안으로는 스마트폰 보안 정책 및 지침을 수립하여 사내 정보유출을 최소화 할 수 있는 정책과 지침 적용으로 보안사고 문제를 최소화 할 수 있다.

본 장에서는 보안 모델에서 구분 된 각 보안영역 별 발생 가능한 보안 위협과 보호대책을 설명하였다. 이와 같이 구분 된 각 영역 별로 보호대책을 제시함으로써 다양한 보안위협으로부터 능동적인 대응이 가능하다. 하지만, 다수의 보호대책을 이해하고 서비스에 적용하는데 선택의 어려움이 있을 수 있다. 이러한 점을 고려하여 다음 장에서는 가상의 보안위협 시나리오를 통해 발생될 수 있는 위협과 필요한 보호대책을 살펴볼 것이다.

Ⅳ. 시뮬레이션 분석 (시나리오 기반)

앞서 제시 한 보안모델의 안전성 분석을 위해 발생 가능한 시나리오를 통해 각 보안영역에서 발생하는 보안위협을 도출하여 제안모델의 기준에 따라 분석 및 분류할 것이다. 또한, 각 보안위협에 해당하는 보호대책을 제시하여 발생 가능한 보안위협에 대응할 수 있는 방안을 함께 제시할 것이다.

4.1 모델 분석 기준 및 순서

본 제안 모델에서는 시나리오 분석에서 정성적, 정량적인 영향력을 함께 파악하기 위해 두 가지 비교기준을 정의하여 위험의 우선순위를 도출하였다. 첫 번째 적용기준은 위험 발생 가능성(Risk Likelihood)이며, 두 번째는 위험으로 인한 위험영향도(Risk Impact)이다. 이 두 가지 위험 요소를 반영하여 위험수준(Risk Level)을 정의하였으며, 각각의 내용은 [표 6]과 같다.

〔표 6〕 보안위험 발생 가능성

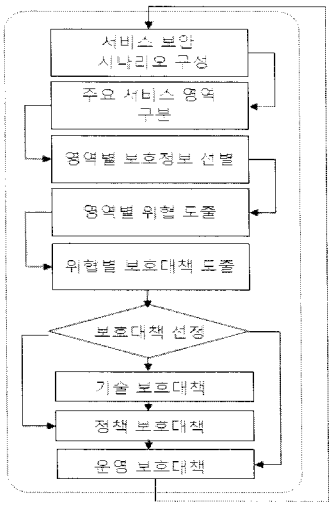
구분	의미
Very small	발생 가능성이 0.1% 미만으로 매우 낮은 수준
Small	발생 가능성이 0.1~1%의 낮은 수준
Medium	발생 가능성이 1~5%의 가끔 발생하는 수준
High	발생 가능성이 5~20%의 자주 발생하는 수준
Very high	발생 가능성이 20%이상으로 매우 자주 발생하는 수준

* 발생가능성(%)[9]=Cases/Time
* Time: 최근 서비스 점검시간 이후부터 다음 서비스 점검시간까지의 시간이며, 주로 한 달을 기준으로 함
* Cases: 보안 위험 발생 횟수 (보안 위험 발생 수렴과 발생 전 완화 모두 포함)

위험의 피해규모는 표 6과 같이 다섯 가지 수준으로 정의할 수 있다. Very small은 피해 영향력이 거의 없어 보안의 3요소인 무결성, 가용성, 기밀성에 영향을 거의 주지 않는 정도를 의미한다. Small은 피해 영향력이

경미하여 사용자에게 경미한 방해로 가용성에 미약한 영향을 줄 수 있는 정도로 기밀성, 무결성에는 영향을 주지 않는 수준이다. Medium은 모든 서비스 사용자를 대상으로 장시간 장애를 제공하는 것으로 기밀성과 무결성에는 영향을 주지 않는 수준이며, High는 서비스 일부분의 문제로 가용성, 기밀성, 무결성에 문제가 발생하는 것으로 사용자 일부에게 사용제한이 발생하는 수준이다. 마지막으로 Very high는 정보의 기밀성, 무결성, 가용성에 영향을 주는 수준으로 모든 사용자와 서비스 전체에 보안문제로 인해 정상적인 서비스가 제공되지 않는 수준이다. 표 6에서 언급 한 위험 발생가능성과 위험 영향도를 산정하여 다음과 같은 네 가지의 위험수준을 정의할 수 있다.

- *Insignificant*: 100% 수용해도 서비스 운영에 문제가 되지 않을 정도의 경미한 위험 수준
- *Low*: 수용할 수 있는 위험으로 위험이 재발하거나 위험수준을 높일 수 있는지 주시하여 모니터링 필요
- *Moderate*: 수용할 수 있는 위험으로 해결하거나 감소시키기 위해 인력이 투입되어 일정 시간 동안 문제해결 필요
- *High*: 수용할 수 없는 위험으로 위험을 제거하기 이전에는 서비스 제공이 불가능한 수준



〔그림 4〕 보안모델 적용 순서

[표 6]에서 언급 한 보안 위험기준을 다음 시나리오에 적용하여 보안위험의 수준을 확인해 볼 것이다. 다음 시나리오에서 보안위협을 제시하고, 이러한 보안위협수준에 필요한 보호대책이 무엇인지 설명할 것이다. 제공되는 시나리오는 [그림 4]의 순서[11]에 따라 보안위협과 보호대책을 적용할 것이다.

본 논문에서는 위험분석의 비교대상 중 정보자산 산정에 필요한 자산가치 산정방법은 논제의 범위를 벗어나므로 생략하고 위 적용순서에 따라 적용 할 것이다. 모든 Smrt work 서비스의 분석은 그림 4의 분석방법 순서를 적용하여 도출가능하다. 분석방법의 프로세스는 위협에 적합한 보호대책이 도출될 때까지 반복하여 적용함으로써 완성도를 높일 수 있다.

4.2 보안위협 시나리오

시나리오는 Smrt work에서 가장 많이 사용될 수 있는 이메일을 시나리오로 선정하였다. 공격은 우측의 이메일을 통한 악성코드 배포자가 좌측의 사용자를 대상으로 진행하며, 각 영역 별 주요 공격은 다음과 같다.

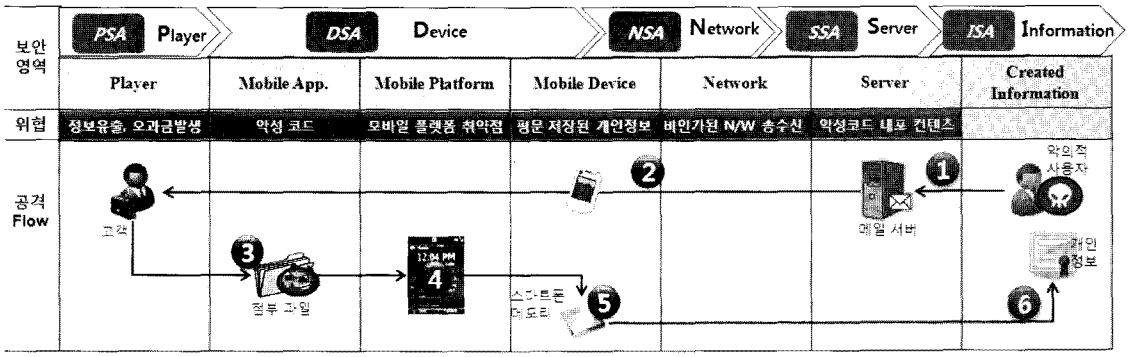
각 영열 별 주요 이벤트는 다음 순서와 같다.

① 악성코드를 포함한 E-Mail 첨부파일을 인터넷을 통해 송신
② 사용자가 E-Mail을 수신
③ 악성코드가 포함된 E-Mail 첨부파일을 실행
④ 스마트폰의 플랫폼 취약점을 통해 악성코드 감염
⑤ 스마트폰에 저장된 개인정보 접근
⑥ 개인정보를 네트워크를 통해 외부로 유출

위의 영역 별 이벤트에서 발생되는 보안위협의 우선순위는 다음 장에서 보안위험분석을 통해 선별할 것이다.

4.3 보안위협

본 제안모델의 보안위험분석은 총 25가지의 보안위협을 도출할 수 있으나, 그림 5의 시나리오에서 도출 한 보안위협 열 가지를 대상으로 할 것이다. 각 보안영역별 보안위협을 정리하면 다음과 같다. ISA에서는 ①악의적 의도의 악성코드 내포 컨텐츠 생성 및 배포가 있을 수 있다. SSA 보안영역에서는 ②메일서버에는 악성코드가 내포 된 컨텐츠가 저장되어 있고, NSA에는 ③비인가된 네트워크 송수신이 있을 수 있다. DSA의 H/W 디바이스에는 ④암호화되지 않은 개인정보가 악성코드로 하여금 확인 및 유출될 수 있고, ⑤감염 된 어



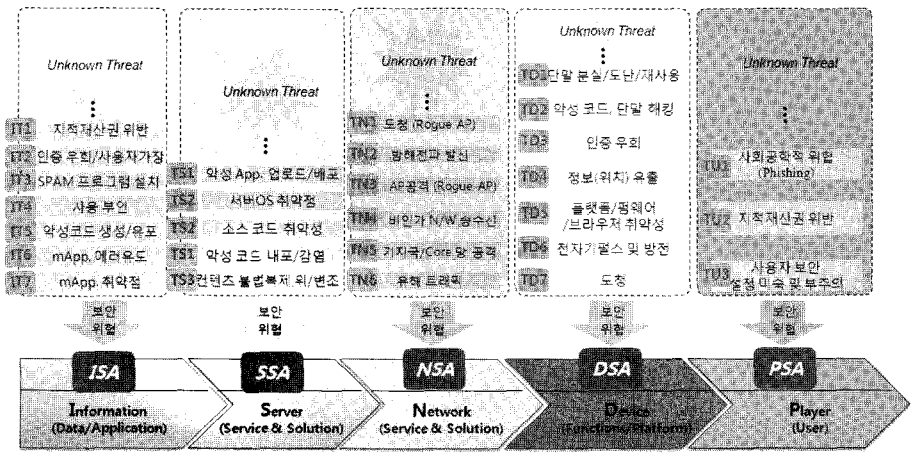
〔그림 5〕 이메일 악성코드를 통한 정보유출 시나리오

플리케이션이 비정상적인 동작으로 전원 소모현상과 ⑥ 오동작 현상으로 만달의 가용성이 저해될 수 있다. DSA의 플랫폼에서는 ⑦플랫폼 취약점을 이용한 악성코드 감염이 발생할 수 있다. 또한, DSA의 어플리케이션에서는 ⑧악성코드로 인해 개인정보가 외부로 유출될 수 있다. PSA에서는 사용자의 정보가 외부로 유출되어 ⑨사용자가 원하지 않는 오과금이 발생할 수 있고 ⑩제2의 보안위협에 이용될 수 있다. 각각의 보안위협을 발생가능성과 피해영향도의 두 관점에서 분석하면, 표 7과 같은 2차원 보안위협 Matrix[12,13] 테이블로 정리할 수 있다.

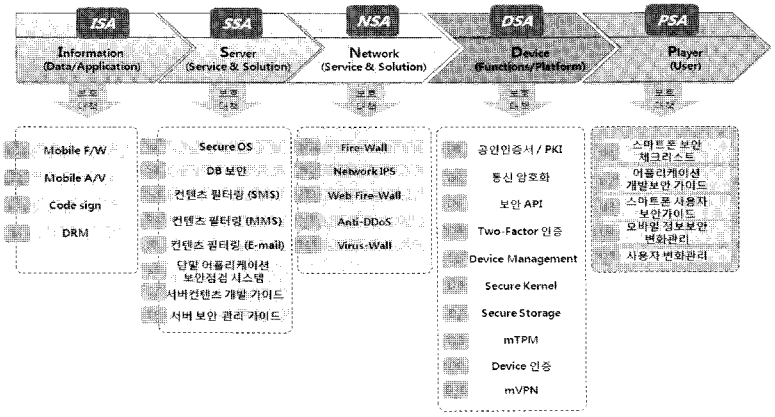
〔표 7〕 보안 위험분석 Matrix

구분		피해영향도 (Risk Impact)				
		1.Very small	2.Small	3.Medium	4.High	5.Very high
발생 가능성 (Likelihood)	1.Very	⑤		⑩		
	2.Small		⑥		⑨	⑧
	3.Medium			⑦		
	4.High					
	5.Very high	②				
범례		Low	Insignificant	Moderate	High	

분석 된 보안위협은 위 [표 7] 에서 확인할 수 있듯이 High 수준은 ①, ③, ④이며, Moderate 수준은 ②, ⑦, ⑧, ⑨이고, Low와 Insignificant 수준은 각각 ⑤, ⑥, ⑩이다. 이와 같이 보안위협 분석 Matrix에서 위험수준이 높은 High와 Moderate를 주 대상으로 보호대책을 제공함으로써 서비스에 필요한 보호대책을 최소화하고 집중하여 보호할 수 있다. Smrt work에서 발생할 수 있는



〔그림 6〕 보안구간 별 발생 가능한 보안위협



〔그림 7〕 보안구간 별 적용 가능한 보호대책

보안위협을 각 영역별로 도출하면 [그림 6]과 같다.

[그림 6]에서 도출 된 보안위협들은 각 보안영역 별 대표적인 위협들이다. 보안위협은 지속적으로 발전, 진화되고 있으며, 알려진 위협보다 알려지지 않은 위협이 더 큰 피해를 발생시킬 수 있음을 인지해야 할 필요가 있다.

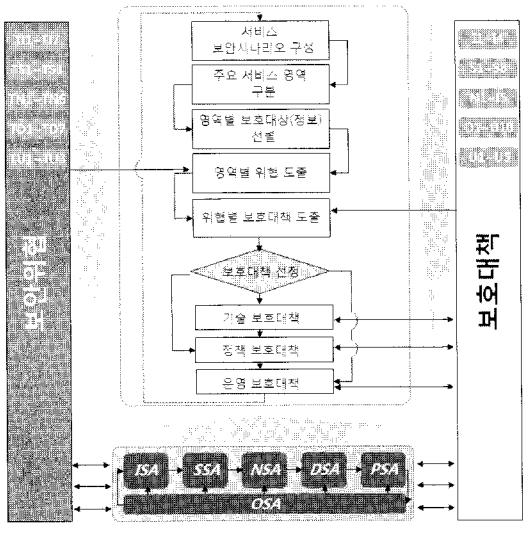
4.4 보호대책

위 시나리오에서 언급 된 보호대책을 포함하여 Smrt work 환경에서 각 보안영역 별 보호대책들은 [그림 7]과 같이 정리할 수 있다.

[표 6]에서 도출 된 각 보안영역의 보안위협에 대 응할 수 있는 보호대책을 설명하면 다음과 같다. ISA에서는 개발자를 위한 컨텐츠 개발 가이드를 제공하여, 모바일 어플리케이션 개발자들의 정보보호에 대한 인식 개선을 통해 스스로 보안을 고려할 수 있도록 하기위한 보호대책이다. SSA에서는 업로드 된 어플리케이션의 통합보안 점검 시스템으로, Anti-Virus를 이용하여 서버에 업로드되는 컨텐츠를 점검하는 기능과 Code Sign이 필요하다. NSA에서는 트래픽 모니터링 및 알림을 위한 Mobile Firewall로 네트워크 트래픽 모니터링을 통한 정보유출을 방지하는 기능이다. PSA에서는 스마트폰 사용자 보안가이드 및 변화관리를 통한 보안 교육이며, DSA에서는 Mobile Anti-Virus, mTPM, 암호화 저장을 위한 Secure Storage 기능, MDM은 다운로드 되는 컨텐츠에 대한 악성코드 진단과 컨텐츠의 실행 권한 제한 및 모바일 플랫폼에 대한 주기적인 보안패치 적용 기능을 제공하여 보안위협을 방지할 수 있다.

4.5 보안모델 적용방법

그림 6과 그림 7에서 제시 된 것과 같이 각 보안영역 별 발생 가능한 위협과 보호대책을 참고하여 스마트폰에서 발생할 수 있는 다양한 보안위협에 대응할 수 있다. 하지만, 위에 제시 된 모든 보호대책을 Smrt work 서비스에 제공하는 것은 비용적인 부담과 운영인력의 투입 및 기간 등에 있어서 현실적인 한계가 있을 수 있다. 제시 된 보호대책들을 서비스에 적용할 때는 해당 서비스에서 취급하는 정보의 중요성과 보안사고 시 피해의 심각성 및 서비스의 환경과 특성, 목적 및 의도를 고려하여 보호대책을 선정하는 것이 서비스의 품질과



〔그림 8〕 안전한 Smrt work 보안모델의 Architecture

안전한 모바일 환경을 동시에 제공하는 방법일 것이다.

이러한 방법을 체계적으로 적용하기 위한 제안모델의 전체적인 구성은 그림 8과 같다. 보안위협은 그림 6에서 언급 된 보안위협에 해당하며, 보호대책은 그림 7에서 언급 한 보호대책을 의미한다. 보안위협을 도출하고 보호대책을 적용할 때 서비스의 각 영역 별 구분기준과 보호해야 할 정보의 대상 및 우선순위는 보안모델의 적용 순서에 따라 선정한다[14,15,16]. 이러한 순서와 구성에 따라 Smrt work 서비스를 세분화하여 보호대책을 적용하면, 중복투자를 줄일 수 있고, 보호해야 할 정보에 집중하여 처리함으로써 보안기술의 투자 및 운영비용을 줄일 수 있는 효과를 가질 수 있을 것이다.

V. 결 론

본 논문에서는 기업에서 스마트폰을 이용한 Smrt work 도입 시 발생할 수 있는 보안위협과 이에 효과적으로 대응하기 위한 모바일 보안 대응 모델을 보호대책과 함께 제시하였다. 그리고 위협시나리오를 도출하여 제시한 모델에서 발생되는 위협의 수준을 분석하였고, 이에 필요한 보호대책을 서비스 전체 구간별로 제시하였다. 모바일 환경에서 보안은 모바일 이전의 유선환경에서와 마찬가지로 보호해야 할 정보를 선정하는 단계를 거침으로써 정보의 가치를 산정하는 것이 선행되어야 한다. 이러한 정보의 가치를 산정하는 것은 각 기업마다 보호하려는 정보의 대상과 사업배경에 따른 서비스 모델이 상이하므로, 다양한 보안사고를 모두 대응하는데 있어 시간과 비용의 투자로 인한 현실적인 한계가 있을 수밖에 없다. 이러한 한계를 극복하기 위한 효과적인 방법은 보안위협이 발생하는 주요 구간을 보안영역으로 세분화하고, 이에 적합한 보호대책을 제공함으로써 효과적으로 보안사고를 줄이는 것이다. 이러한 방법을 제시하기 위하여 본 논문에서는 Smart work 환경에서 발생 가능한 보안위협과 보호대책을 보안구간별로 세분화하여 제시하였다. 그리고 Smrt work를 도입하려는 각 기업의 의사결정권자들에게는 다양한 환경에 적용할 수 있도록 보안위협과 보호대책을 상세히 언급하였다. 또한, 모바일 분야의 보안을 공부하는 학생들에게는 다양한 형태의 보안이슈와 해결방안을 제시함으로써, 모바일 환경의 보안을 공부할 수 있는 발판을 제공하기 위해 최근 기술에 근거한 보안이슈를 중심으로 기술하였다.

본 논문에서 제시 된 보안 모델에서 보안운영자의 역할을 추가로 고려해 볼 수 있다. 향후 보안위협과 보호대책의 효과적인 대응방안에서 보안운영자의 효율적인 관리방안과 Smrt work의 능동적인 보안관리 방안을 연구하여, 실 서비스에 서비스의 품질을 고려한 보안적용 방안을 연구과제로 진행 할 예정이다.

참고문헌

[1] A. Charlesworth, "The ascent of smartphone," Institution of Engineering and Technology, pp. 32-33, Feb. 2009.

[2] B. Bae, W. Kim, C. Ahn, S. I. Lee and K. I. Sohng, "Development of a T-DMB extended WIPI platform for interactive mobile broadcasting services," Consumer Electronics, IEEE Trans., pp. 1167-1172, Jnu. 2006.

[3] S. Ryan, C. J. Kolodgy and S. D. Drake, "World wide Mobile Security 2010 - 2014 Forecast and Analysis," IDC #222348, Volume:1, Mar. 2010.

[4] C. H. Lin, J. C. Liu, H. C. Huang and T. C. Yang, "A Defending Mechanism against DDoS Based on Registration and Authentication," 2008 The 9th International Conference for Young Computer Scientists, pp. 2192-2197, Apr. 2008.

[5] R. C. Basole, "Visualization of interfirm relations in a converging mobile ecosystem," Journal of Information Technology, pp. 144-159, Jun. 2009.

[6] Y. Zhiyu, Z. Linwei and L. Wenna, "Study on security strategy of wireless Smart Office system," *First International Workshop on Education Technology and Computer Science*, pp. 495-498, Mar. 2009.

[7] D. Keely, "A security strategy for mobile e-business," Security and Services organization of IBM Global Services, Jul. 2001.

[8] D. Eschenbrücher, J. Mellberg, S. Niklander, M. Näslund, P. Palm and B. Sahlin, "Security architectures for mobile networks," *Ericsson review* No.2, pp. 68-81, Feb. 2004.

[9] E. Bones, P. Hasvold, and E. Henriksen "Risk analysis of information security in a mobile in-

stant messaging and presence system for healthcare," *International Journal of Medical Information*, pp. 677-687, Jun. 2006.

[10] G. A. Jacoby, S. Mosley, "Mobile Security Using Separated Deep Packet Inspection," 5th IEEE Consumer Communications and Networking Conference, pp. 482-487, Jan. 2008.

[11] M. Decker, "A Security Model for Mobile Processes," Mobile Business, ICMB '08. 7th International Conference, pp. 211-220, Jul. 2008.

[12] Aagedal. J. O., D. Braber. F., Dimitrakos. T., Gran, B. A., Raptis. D., Stolen. K., "Model-based Risk Assessment to Improve Enterprise Security," 6th IEEE International Enterprise Distributed Object Computing Conference, pp. 51-62, Sep. 2002.

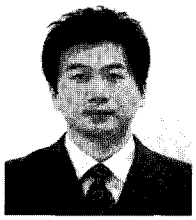
[13] M. Ekstedt, T. Sommestad, "Enterprise Architecture Models for Cyber Security Analysis," IEEE PES Power Systems Conference Exhibition, pp. 1-6, Oct. 2009.

[14] C. Cares, X. Franch, "Selecting Smart Office Devices using a Goal-Oriented Approach," Research Challenges in Information Science, pp. 143-154, Apr. 2009.

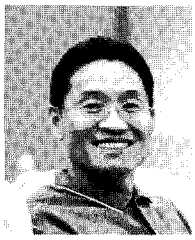
[15] M. C. WU, B. UNHELKAR , "Extending Enterprise Architecture with Mobility," Vehicular Technology Conference, IEEE, pp. 2829-2833, May. 2008.

[16] Standards Australia, "AS/NZS 4360: Risk Management," Standards Association of Australia, AS/NZS 4360, 1999.

〈著者紹介〉



황 해 수 (Hwang Hae Su)
정회원
2011년 3월~현재 : 성균관대학교 기술경영 박사과정
2009년 5월~현재 : 인포섹 (주) 컨설팅사업본부 재직 중
관심분야: 정보통신공학, 정보통신 정책분야,정보보호학,기술경영,



이 기 혁 (Lee Gi Hyouk)
정회원
2008년 3월 : 건국대학교 공학박사
1994년 5월~현재 : SK Telecom (주)정보기술연구원 재직 중
관심분야: 정보통신공학, 정보통신 정책분야,정보보호학,개인정보보호공학 등