스마트워크의 유·무선시스템 보안설계

천재홍* · 박대우**

*호서대학교 벤처대학원

Smartwork Wired Wireless System Security Design

Jae-Hong Cheon* · Dea-woo Park**

*Hoseo Graduate School of Venture

E-mail : jhcheon1971@gmail.com, prof_pdw@naver.com

요 약

기술 발전 속도가 증가되고, 고성능의 디지털 기기가 확산되고 있다, 기존 유선 환경에 최적화 되어 제한적으로 활용되던 PC와 같은 유선 디지털 기기에서 시·공간의 제약에서 벗어나, 언제 어디서나 효율적인 업무 수행이 가능한 스마트워크로 전환되고 있다. 유선환경에 비해 단말기 분실, 도난 및 파손 등 물리적 위협과 도난, 서비스 거부, 비인가 접근 등 기술적 위협 등 다양한 보안 위협에 대해 무결성과 가용성을 확보할 수 있는 시스템 보안설계가 필요하다. 본 논문 연구에서는 스마트워크의 네트워크시스템, 유·무선 링크시스템, 디지털 스마트기기를 분석한다. 현재 업무에 사용되고 있는 스마트워크 유선시스템과 향후 무선시스템을 위한 보안설계 방안을 연구한다. 본 연구는 안전한 스마트워크 구축에 기초자료로 활용될 것이다.

ABSTRACT

The speed of technology development is increasing, and high-performance digital devices are spreading. Smart walks that can work effectively anytime and anywhere by being restricted from space and time in wired digital devices such as PC, . System security design is needed to secure integrity and availability against various security threats such as physical threats such as lost, stolen and damaged terminals, technical threats such as theft, denial of service, and unauthorized access, compared with the wired environment. In this paper, we analyze smart work network system, wired / wireless link system, and digital smart device. We study security design method for smart work wired system and future wireless system which are used in present work. This study will be used as basic data for building a secure smart work.

키워드

스마트워크, 스마트워크 보안위협, 네트워크보안시스템 설계, 유·무선링크시스템 보안설계,
디지털 스마트기기 보안설계

Ⅰ. 서 론

스마트워크는 시간과 장소의 제약에서 벗어나 업무를 처리하는 방식이다.

스마트워크를 위해 유·무선 네트워크와 고성능 디지털 기기 등 ICT기술을 이용한다. 기존 랩탑 컴퓨터를 포함하여 스마트 폰, 테블릿 등 고성능 디지털 스마트기기의 확산과 인프라 확충으로 스마트워크 운영 환경이 마련되고 있다.

기업은 스마트워크 시스템을 구성하여 운영함으로, 업무 생산성과 비용절감 등 효율성이 향상될 수 있다.

하지만 악성코드 침입과 해킹과 같은 기존의 보안위협과 함께 스마트기기 사용에 따른 단말기 보안위협, 앱 보안위협 및 네트워크 보안위협 등

분실 및 도난 등의 새로운 보안 위협이 나타나고 있다.

본 논문에서는 스마트워크의 보안 위협 중 유·무선 네트워크 보안위협에 대해 연구하고 보안 유·무선 네트워크 설계를 통해, 안전한 스마트워크의 운영을 위한 네트워크를 구성하고자 한다.

II. 관련연구

2.1. 스마트워크 기술

스마트워크의 안전한 구성 및 운영을 위해 디지털 스마트기기 및 네트워크 구성 운영을 위한 정보통신기기 및 네트워크 관련 기술과 사용자 인증, 콘텐츠 암호화, 네트워크 통제 및 암호화, 디지털 스마트기기 보안 등 악성코드 대응을 위한 보안 관련 기술 및 스마트워크 솔루션 운영을 위한 운영관리 기술이 필요하다.

스마트워크는 스마트워크 네트워크 기술, 스마트워크 서비스 기술, 스마트워크 콘텐츠 기술, 스마트워크 플랫폼 기술 등 다양한 요소 기술의 조합으로 이루어져 있다.

2.2. 스마트워크 표준화

해외의 경우 스마트워크 표준화는 텔레프레즌스를 중심으로 ITU-T, IETF 등 국제 표준화 기구에서 진행되고 있으며, 국내에서는 스마트워크 표준화가 진행되고 있지 않고 다만 표준화 기관인 TTA에서 스마트워크 활성화를 위한 스마트워크 포럼과, 스마트워크 프로젝트 그룹을 준비중에 있다.

2.3. 스마트워크 보안위협

스마트워크 환경에서 보안위협 요소는 스마트폰, 테블릿 등 디지털 스마트기기의 도난·분실, 중요자료 외부 유출 등의 물리적 보안위협과 악성코드 감염, 앱 등을 이용한 원격접근 및 정보유출 등의 소프트웨어 보안위협, 일반 인터넷을 통한 접속에 따른 네트워크 보안위협 등이 있다.

- 물리적 보안위협

휴대가 용이하고, 대용량 메모리와 고성능 CPU가 장착된 디지털 스마트기기에는 통화내역, 메시지, 연락처, 일정 및 위치정보, 금융정보 등의 개인정보와 업무 수행에 따른 기업 기밀정보가 저장된다.

디지털 스마트기기의 도난·분실 시 저장된 개인정보와 업무정보가 외부로 유출되어 피해가 발생할 가능성이 상존하고, 이를 악용해 기업 내부 업무시스템에 접속하여 정보 유출·파괴 또는 위·변조를 할 수 있다.

- 소프트웨어 보안위협

스마트 폰 등 디지털 스마트기기는 네트워크 접속 기능이 있는 장비로 인터넷 환경에서 발생할 수 있는 모든 보안위협이 스마트 폰에서도 동일하게 발생할 수 있다.

악성코드 감염, 부주의한 관리로 인한 비인가 앱 설치 등으로 개인정보 유출, 유해 사이트 접속, 원격제어, 정상동작 방해 등이 발생할 수 있다.

업무에 사용하는 스마트 폰이 원격 제어가 될 경우 스마트 폰에 저장된 개인정보와 회사 기밀정보, 기업 내부 업무시스템에 저장된 정보가 유출될 수 있다.

- 네트워크 보안위협

기업 외부에서의 유·무선 접속으로 기업 내부 업무시스템에 접속하는 경우 인터넷망에서 발생할 수 있는 도·감청 등의 보안위협이 발생할 수 있다.

III. 스마트워크 유·무선시스템 분석관련

3.1. 네트워크시스템 분석

스마트워크에서 사용자는 주로 외부에서 기업 내부 업무시스템에 접속하여 업무를 수행한다.

외부 인터넷이나 전산장비를 통해 외부에서 기업 내부 업무시스템에 접속하는 것은 기업 내에서 접속하는 것에 비해 상대적으로 많은 보안위협에 노출되고, 내부 시스템이 외부에 노출될 수 있는 위험이 커지게 된다.

또한 DoS, DDoS 등 외부의 악의적인 공격으로 정상적인 업무시스템에 접속 및 업무수행이 어려울 수 있다.

3.2. 유·무선 링크시스템 분석

무선랜 등 공개된 장치와 공개된 네트워크를 경유한 기업 내부 업무시스템 접속은 악성코드 전파 및 감염 경로로 이용되거나, 비인가 유해 소프트웨어의 유포경로로 악용되어 개인정보 및 기업정보 유출 및 좀비 단말기로 이용될 수 있다.

또한 공개된 네트워크 사용 시 음성, 데이터에 대한 도·감청 등으로 개인정보, 중요 기업정보가 노출되거나 위·변조 될 가능성이 상존한다.

3.3. 디지털 스마트기기 분석

디지털 스마트기기에는 연락처, 메시지, 위치정보 등 개인정보와 업무용 정보를 안전하게 보호하기 위해 단말기 전용 방화벽과 분실 및 도난의 위협에 대응하기 위해 데이터의 암호화 및 이중 백업체계를 마련하여야 한다.

디지털 스마트기기의 비인가 사용자 인증과 무단사용 제한을 위해 안전한 비밀번호를 설정할 수 있도록 하고, 분실과 도난 시 데이터가 유출을 방지할 수 있도록 보안대책 마련이 필요하다.

Ⅳ. 스마트워크 유·무선시스템 보안설계

4.1. 네트워크 보안시스템 설계

해킹, 악성코드 등 사이버 보안위협에 대응하고, 비인가자의 접근통제를 위해 외부 유·무선 통신망과 접속되는 구간에 침입차단시스템을 구축·운영하여야 하고, 비정상 접속 및 트래픽 모니터링을 위한 유해트래픽탐지시스템과 DoS, DDoS 등 서비스거부 공격에 대응할 수 있는 서비스거부공격 대응시스템을 구축·운영할 수 있도록 설계 한다.

4.2. 유·무선링크 보안시스템 설계

기업 내부 업무시스템 접속은 이동통신망(CDMA, W-CDMA, Wibro)에 한하여 접속할 수 있도록 허용하고, WiFi와 같은 무선랜과 블루투스를 통한 접속과 테더링을 통한 접속은 차단할 수 있도록 설계한다.

음성 및 데이터의 도·감청 차단을 위해 AES 128bit, ARIA 128bit 또는 그 이상의 암호 알고리즘을 사용하여 VPN 통신채널을 사용할 수 있도록 설계한다.

4.3. 디지털 스마트기기 보안시스템 설계

디지털 스마트기기에는 기업의 네트워크 환경이나 외부 환경에 맞도록 개인 방화벽을 필수적으로 설치하여야 한다.

또한 데이터의 안전성 확보를 위해 데이터를 AES 128bit, ARIA 128bit 또는 그 이상의 암호 알고리즘으로 암호화하여 사용자의 디지털 스마트기기와 기업 내부의 전용 스토리지에 백업 또는 저장할 수 있도록 설계한다.

디지털 스마트기기의 사용자 인증을 위해 9자리 이상의 비밀번호로 일방향 암호화하고, 비밀번호가 미설정 또는 일정횟수 이상 입력 오류 시 일정 시간 접속이 차단될 수 있도록 하여야 한다. 보안성이 높은 경우 추가적으로 PKI, OTP 및 지문 등 생체정보를 이용한 인증을 적용하여야 한다.

디지털 스마트기기 분실·도난에 대비하여 원격삭제 및 위치추적이 가능하도록 MDM 등의 디지털 단말기 전용 보안시스템을 적용하여야 한다.

Ⅴ. 결 론

본 논문에서는 안전한 스마트워크 체계 구축 및 운영을 위해 네트워크시스템 분석, 유·무선 링크시스템 분석, 디지털 스마트기기 분석 등을 수행하고, 분석결과에 따른 보안대책을 마련하였다.

안전한 스마트워크 환경 구축 및 운영을 위해서 체계적인 위험관리를 통해 보안위협에 대응하고 취약점 분석을 통해 적절한 보안대책을 수립 적용함으로써 보다 높은 신뢰성을 담보할 수 있도록 지속적인 연구가 필요하다.

참고문헌

[1] 이형찬, 이정현, 손기욱 “스마트워크 보안위협과 대책”, 한국정보보호학회지 제21권 3호, pp. 12-21, 2011년 5월.

[2] 정명수, 이동범, 곽진 “스마트워크 보안위협 및 보안 요구사항 분석”, 한국정보보호학회지 제21권 3호, pp. 55-63, 2011년 5월.

[3] 김재생, 한광식 “스마트워크의 핵심 기술 요소와 국내외 동향”, 한국콘텐츠학회 제14권 1호, pp. 14-20, 2016년 3월.

[4] 현욱, 강신각, “스마트워크 표준화 동향 - 텔레프레즌스를 중심으로”, 전자통신동향분석 제26권 제2호, pp. 42-49, 2011년 4월.

[5] 박승권, 이주한, “스마트워크 기술과 표준화 동향”, TTA Journal Vol.136, pp. 79-84, 2011년 7월.

[6] 한국인터넷진흥원, “인터넷&시큐리티 이슈”, 2012년 4월.