스마트워크 보안 아키텍처 연구

이동범*, 곽진*
*순천향대학교 정보보호학과
e-mail : dblee@sch.ac.kr, jkwak@sch.ac.kr

Security Architecture of Smartwork Network

Dongbum Lee*, Jin Kwak*
*Dept of Information Security Engineering, Soonchunhyang University

요 약

스마트워크 환경을 이용하는 많은 조직의 직원은 스마트워크 기술을 이용하여 외부 위치에서 다양한 작업을 수행할 수 있다. 하지만 외부 네트워크와 외부 호스트에서 보호된 자원에 접근하는 원격 접근 기술과 스마트워크의 본질은 일반적으로 조직 내부에서 접근하는 기술보다 위험하고 스마트워크 사용자가 원격 접근을 통해 내부 자원을 이용하는 것은 위험을 증가시킨다. 따라서 본 논문에서는 안전한 스마트워크 서비스 환경을 구축하기 위하여 보안 취약점을 분석하여 이를 바탕으로 안전한 접근 제어 기능을 제공하는 스마트워크 보안 아키텍처를 제안한다.

1. 서론

스마트워크는 많은 사람들이 조직 시설 이외의 다른 장소에서 직원과 계약자가 업무를 수행할 수 있는 환경을 말한다. 스마트워크 사용자는 이메일 읽기 및 보내기, 웹 사이트 접근, 문서 검토 및 편집 등 많은 작업들을 수행하기 위해 데스크톱, 노트북과 같은 다양한 클라이언트 단말을 사용한다. 대부분의 스마트워크 사용자는 조직의 시설과 다른 외부 위치에서 조직의 비공개 컴퓨팅 자원에 접근하기 위하여 원격 접근을 사용한다.

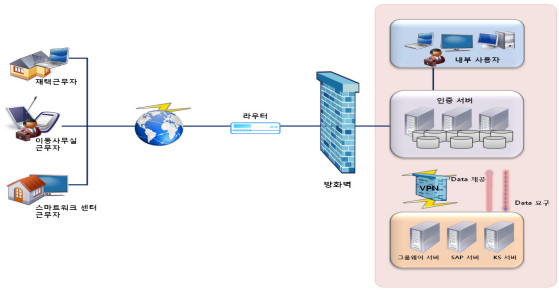
스마트워크 환경을 이용하는 많은 조직의 직원 및 계약자는 스마트워크 기술을 사용하여 외부 위치에서 작업을 수행할 수 있다[1].

하지만 외부 네트워크와 외부 호스트에서 보호된 자원에 접근하는 원격 접근 기술과 스마트워크의 본질은 일반적으로 조직 내부에서 접근하는 기술보다 위험하고 스마트워크 사용자가 원격 접근을 통해 내부 자원을 이용할 수 있게 하는 위험을 증가시킨다. 원격 접근을 통하여 접근한 클라이언트 단말, 원격 접근 서버 및 내부 자원을 포함하는 스마트워크와 원격 접근 기술의 모든 구성요소는 위협 모델을 통하여 예상되는 보안 위협으로부터 보호해야 한다.

따라서 본 논문에서는 안전한 스마트워크 서비스 환경을 구축하기 위하여 보안취약점을 분석하여 이를 바탕으로 안전한 접근제어 기능을 제공하는 스마트워크 보안 아키텍처 모델을 제안한다.

2. 스마트워크 개요

스마트워크는 정보통신기술(ICT : Information Communication Technology)을 활용하여 시간과 장소의 제약 없이 업무를 수행하는 근무 형태를 의미한다. 자택에서 본사의 통신 네트워크에 접속하여 업무를 수행하는 재택근무나 자택 인근 원격 사무실에 출근하는 스마트워크 센터 근무, 스마트폰 등을 이용하여 현장에서 업무를 수행하는 이동근무 등이 모두 스마트워크에 포함된다[2]. 스마트워크의 업무형태를 이용하면 출·퇴근에 따른 시간, 비용 절감 및 업무의 효율성과 자율성을 보장 받을 수 있다.

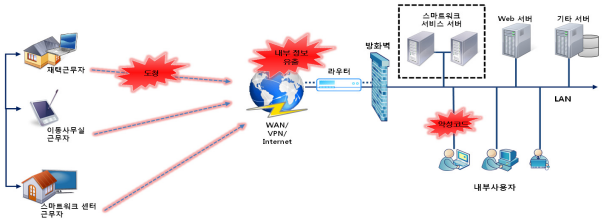


[그림 1] 스마트워크 시스템 구성도

3. 보안 위협

조직은 위험 평가를 이용하여 개발 생명 주기 전체를 포함한 스마트워크 시스템의 잠재적 위협 및 위험의 규모를 판단해야 한다. 이 과정에서 출력은 위험 완화 과정에서 위험을 감소 또는 제거하기 위한 적절한 관리 방법을 식별하는데 효과적이다[3].

위험이 발생할 가능성을 판단하기 위해서 잠재적 취약성과 스마트워크 시스템에 도입된 통제와 함께 스마트워크 시스템에 대한 보안 위협 분석이 필요하다.



[그림 2] 스마트워크 환경에서의 보안 위협

3.1 도청

대부분의 모든 원격접속은 인터넷을 통해 이루어지기 때문에 조직들은 일반적으로 스마트워크 근무자들이 사용하는 외부 네트워트의 보안을 통제할 수 없다. 원격접속에 사용되는 통신시스템들은 전화기와 모뎀, 광대역 전용회선, 무선통신장치들이다. 이러한 통신시스템들은 도청에 취약하여 원격접속 하는 동안 전송되는 민감한 자료들이 유출될 수 있다. 중간자 공격으로 인하여 통신내용이 변경되어 전송될 위협도 있다. 따라서 조직들은 재택근무나 스마트워크 센터 등 스마트워크 업무 네트워크와 조직사이의 통신 네트워크는 신뢰할 수 없다는 것을 고려해야 한다.

3.2 내부정보 유출

원격접속은 외부의 전산장비들이 조직 내에 있는 내부 자원들을 접근할 수 있게 한다. 이러한 내부자원들이 전에는 외부 네트워크로부터 접근될 수 없었지만 원격접속을 통해 접속이 가능해졌다. 이러한 외부에서 내부자원들을 접속할 수 있도록 하는 것은 내부 자료들을 신뢰할 수 없는 장비들과 통신 네트워크로 노출시켜 중요한 내부 자료가 외부로 유출될 수 있는 가능성을 증가 시킨다. 내부자원을 접근할 수 있는 스마트워크 센터 근무, 이동근무, 재택근무 등으로 내부자원에 접속 가능하기 때문에 각 조직은 이러한 근무들로 인해 내부 자료가 유출 될 경우의 영향에 대비해야 하고 접근제어의 균형을 고려해야 한다.

3.3 악성코드

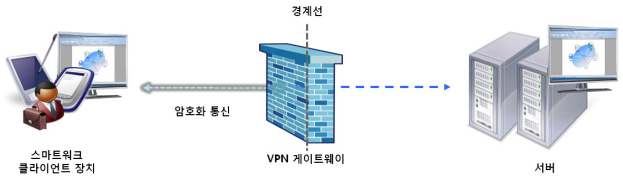
재택근무 장비 중 노트북, 스마트폰 등 모바일 장비는 종종 외부 네트워크에서 사용 된 후 내부로 옮겨져 조직에 내부 네트워크에 직접 접속된다. 공격자가 장비에 악성코드를 설치하여 그 장비로 접근할 수 있는 시스템으로부터 정보를 얻을 수 있다. 만일 재택근무 장비가 악성코드에 의해 감염되었다면 악성코드가 감염된 장비가 조직의 내부 네트워크에 접속되어 조직전체로 악성코드를 전파할 수 있다. 각 조직들은 재택근무, 스마트워크 센터 근무, 이동 근무에 쓰이는 장비들이 언제든지 악성코드에 감염될 수 있는 것을 고려하여 조직 내부 네트워크에 접속하기 전 장비의 보안속성을 확인하는 등 통신 접근 제어 활용도 고려해야 한다.

4. 안전한 스마트워크 원격 접근 시스템

본 논문에서는 안전한 스마트워크 서비스 환경을 구축하기 위하여 접근제어 기능을 제공하는 스마트워크 보안 아키텍처를 제안한다.

4.1 터널링 아키텍처

대부분의 원격 접근 방법은 인터넷과 같은 공용 네트워크를 포함하는 네트워크들간의 정보 교환을 할 수 있는 안전한 통신 터널을 제공한다. 터널은 일반적으로 가상사설통신망(VPN : Virtual Private Network) 기술을 통하여 설치된다. 스마트워크 사용자의 클라이언트 단말과 조직의 VPN 게이트웨이 사이에 VPN 터널이 설치되면 스마트워크 사용자는 터널을 통해 조직의 컴퓨팅 자원에 접근을 할 수 있다. VPN을 사용하기 위해 사용자들은 자신의 클라이언트 단말에 적합한 VPN 소프트웨어가 있거나 VPN 게이트웨이 시스템을 가진 네트워크가 있어야 한다. VPN 클라이언트는 각각의 클라이언트 단말에 설치되고, VPN 서버 소프트웨어를 실행하는 단일 VPN 게이트웨이가 있다. 명암이 있는 점선은 클라이언트 단말과 VPN 게이트웨이 사이의 안전한 원격 접근 연결을 나타낸다. 이 연결을 통해 클라이언트 단말에 설치된 전자 우편 클라이언트, 웹 브라우저와 같은 클라이언트 소프트웨어는 조직 내의 서버에 위치한 어플리케이션의 서버 소프트웨어와 통신한다. VPN 게이트웨이는 사용자 인증, 접근 제어 및 스마트워크 사용자에 대한 보안 기능을 다룰 수 있다. 터널은 클라이언트 단말과 VPN 게이트웨이 사이에 전송되는 정보의 무결성과 기밀성을 보호하기 위해서 암호화를 사용한다.



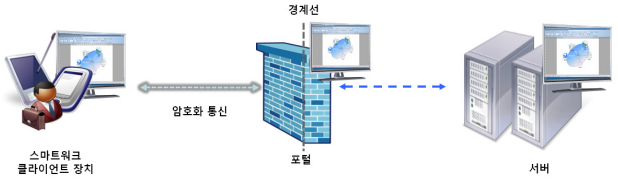
[그림 3] 터널링 아키텍처

4.2 포털 아키텍처

포털은 단일 중앙 인터페이스를 통하여 하나 이상의 어플리케이션에 대한 접근을 제공하는 서버이다. 스마트워크 사용자는 포털에 접근하는 스마트워크 클라이언트 단말에 포털 클라이언트를 사용한다.

포털은 포털 클라이언트 단말과 포털 사이의 정보를 보호하고 인증, 접근 제어, 기타 보안 서비스를 제공하는 것이 특성이다. 그러나 터널과 포털 사이에 어플리케이션의 클라이언트 소프트웨어와 연결된 데이터의 위치가 중요하다. 터널에서 소프트웨어와 데이터는 클라이언트 단말에 위치한다. 포털에서는 포털 서버에 위치한다. 포털 서버는

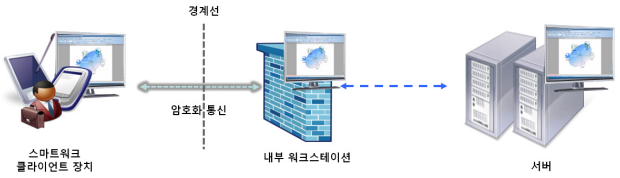
바탕화면이나 웹 페이지와 같은 데이터를 클라이언트 단말로 전송하여 데이터는 일반적으로 터널링 기술을 이용하여 데이터를 일시적으로 클라이언트 단말에 저장한다. 조직의 중앙 어플리케이션 소프트웨어 방식을 이용하여 조직은 분산 원격 접근 솔루션 보다 소프트웨어와 데이터 보안을 효과적으로 제어할 수 있다.



[그림 4] 포털 아키텍처

4.3 원격 데스트톱 접근 아키텍처

원격 데스크톱 접근 기술은 스마트워크 사용자가 자주 사용하는 원격 클라이언트 단말을 이용하여 사무실에 있는 특정 데스크톱 컴퓨터를 자신의 컴퓨터에서 제어하는 능력을 제공한다. 스마트워크 사용자는 원격 컴퓨터의 마우스 및 키보드를 제어 할 수 있으며 스마트워크 클라이언트 단말의 화면에 해당 컴퓨터의 화면을 볼 수 있다. 원격 데스크톱 접근은 사용자가 어플리케이션, 데이터 및 사무실의 컴퓨터로부터 사용할 수 있는 모든 자원을 접근할 수 있다. 원격 데스크톱 접근 클라이언트 프로그램이나 웹 브라우저 플러그인은 각각의 스마트워크 사용자 클라이언트 단말에 설치되어 조직 내부의 네트워크에서 스마트워크 사용자와 대응되는 내부 워크스테이션과 직접 연결한다.



[그림 5] 원격 데스크톱 접근 아키텍처

4.4 직접적인 어플리케이션 접근 아키텍처

원격 접근은 원격 접근 소프트웨어를 사용하지 않고 수행할 수 있다. 스마트워크 사용자는 어플리케이션이 제공하는 통신 암호화, 사용자 인증 등 보안 요소를 이용하여 각 어플리케이션에 직접적으로 접근 할 수 있다. 스마트워크 클라이언트 단말에 설치된 어플리케이션의 클라이언트 소프트웨어는 일반적으로 조직 경계에 위치한 서버로 연결을 시작한다.

직접적인 어플리케이션 접근의 가장 일반적인 경우는 웹 메일로 알려진 이메일 웹 서버의 접근이다. 스마트워크 사용자는 웹 브라우저를 실행하고 이메일 접근을 제공하는 웹 서버에 연결한다. 웹 서버는 HTTP 상에서 SSL 및 HTTPS를 운영하여 통신을 보호하고 스마트워크 사용자의 이메일에 접근하기 전에 웹 메일 어플리케이션은 서버에서 스마트워크 사용자를 인증한다.

[그림 6] 직접적인 어플리케이션 접근 아키텍처

5. 결론

본 논문에서 분석한 스마트워크는 종래의 사무실 내에서만 근무하는 형태를 벗어나 언제 어디서나 효율적으로 일할 수 있도록 모바일 오피스, 원격근무, 재택근무를 포함하는 서비스이다. 스마트워크를 도입한 조직들은 조직의 운용측면에서 비용을 절감 할 수 있고, 업무의 효율성 또한 향상시킬 수 있다.

하지만 외부 네트워크와 외부 호스트에서 보호된 자원에 접근하는 원격 접근 기술과 스마트워크의 본질은 일반적으로 조직 내부에서 접근하는 기술보다 위험하고 스마트워크 사용자가 원격 접근을 통해 내부 자원을 이용하는 것은 위험을 증가시킨다. 원격 접근을 통하여 접근한 클라이언트 단말, 원격 접근 서버 및 내부 자원을 포함하는 스마트워크와 원격 접근 기술의 모든 구성요소는 위협 모델을 통하여 예상되는 보안 위협으로부터 보호해야 한다.

따라서 본 논문에서는 안전한 스마트워크 서비스 환경을 구축하기 위하여 보안취약점을 분석하여 이를 바탕으로 안전한 접근제어 기능을 제공하는 스마트워크 보안 아키텍처를 제안하였다. 본 논문을 통해 스마트워크 서비스 사업자들이 데이터 보안, 사용자/디바이스의 인증, 접근제어 등 보안 환경을 구축하는데 적용할 수 있다.

참고문헌

[1] Karen S., Paul H., Murugiah S., "Guide to Enterprise Telework and Remote Access Security", NIST Special Publication 800-467, Revision 1, June 2009.

[2] Arpad H., "Environmental analysis of telework: What we know, and what we do not know and why", IEEE International Symposium on Sustainable Systems and Technology(ISSST), 17-19 May 2010.

[3] Joshi K., Pant S., "Development of a framework to assess and guide IT investments: an analysis based on a discretionary-mandatory classification", International Journal of Information Management, Vol. 28, No. 3, pp.181-193, June 2008.