안전한 접근제어 기능을 제공하는 스마트워크 보안 프레임워크

이동범*, 곽 진*

요약

많은 기업의 직원 및 계약자는 기업의 스마트워크 기술을 사용하여 외부 위치에서 작업을 수행할 수 있다. 대부분의 스마트워크 사용자는 조직의 비공개 컴퓨팅 자원과 연결하기 위해 원격 접근 기술을 사용한다. 원격 접근 기술과 스마트워크의 본질은 일반적으로 기업 내부에서 접근하는 기술보다 위험하고 스마트워크 사용자가 원격 접근을 통해 내부 자원을 이용할 수 있게 하는 위험을 증가시킨다. 따라서 본 논문에서는 스마트워크 환경에서 발생할 수 있는 보안 취약점을 분석하여 이를 바탕으로 안전한 접근제어 기능을 제공하는 스마트워크 프레임워크를 제안한다.

Smartwork Security Framework with Secure Access Control

Dong-bum Lee*, Jin Kwak**

ABSTRACT

Many organizations' employees and contractors use enterprise smartwork technologies to perform their tasks from external locations. Most smartworkers use remote access technologies to interface with an organization's non-public computing resources. The nature of smartwork and remote access technologies generally places them at higher risk than similar technologies only accessed from inside the organization, as well as increasing the risk to the internal resources made available to smartworkers through remote access. Therefore, in this paper, we will analyze security vulnerability that can occur in smartwork environment, then we proposed smartwork framework that provide secure access control.

Key Words : Smartwork, Access Control, Authentication, Security Framework, Security Channel

* 순천향대학교 정보보호학과(✉dblee@sch.ac.kr)
· 제1저자(First Author) : 이동범 · 교신저자(Correspondent Author) : 곽 진
· 접수일(2011년 6월 23일), 수정일(1차 : 2011년 7월 22일), 게재확정일(2011년 7월 25일)

Ⅰ. 서 론

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

스마트워크 환경을 이용하는 많은 조직의 직원 및 계약자는 스마트워크 기술을 이용하여 외부 위치에서 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. 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[1, 6].

따라서 본 논문에서는 안전한 스마트워크 서비스 환경을 구축하기 위하여 보안취약점을 분석하여 안전한 접근제어 기능을 제공하는 스마트워크 프레임워크를 제안한다.

Ⅱ. 스마트워크 시스템

2.1 개요

스마트워크는 정보통신기술(ICT : Information Communication Technology)을 활용하여 시간과 장소의 제약 없이 업무를 수행하는 근무 형태를 의미한다.

재택근무는 직장이 아닌 집에서 업무를 처리하는 근무 형태로 사무실과 동일한 업무환경을 구축하고 회사의 네트워크로 접속하여 업무를 수행하거나, 본사나 다른 근무자들과 원격회의, 협업 등을 통해 업무를 수행하게 되는 근무 형태이다[2].

스마트워크 센터 근무는 회사에서 구축한 원격업무 시스템을 갖춘 스마트워크 센터 시설로 업무에 필요한 사무공간과 육아시설이나 휴식공간을 제공하는 복합 공간에서 업무를 수행한다. 재택근무와 달리 보안성이 강화되어 실제 회사와 동일한 업무 수행이 가능한 근무 형태이다. 마지막으로 이동근무는 스마트폰을 이용한 모바일 오피스 환경을 구축이나 휴대 가능한 단말기를 이용하여 회사와 멀리 떨어져 있는 장소에서도 업무 정보를 교환하여 장소에 구애받지 않고 근무할 수 있다. 보통 출장이나 고객 대면 등으로 업무 시간의 대부분을 보내는 영업 직종, 컨설팅 업무, 엔지니어들에게 제공되는 근무 형태이다[3-4].

이러한 스마트워크 환경에서의 근무 형태는 표 1과 같이 근무 환경에 따라 구분할 수 있다.

표 1. 스마트워크 근무 형태
Table1. Working Type of Smartwork

형태	내용
재택근무	자택에서 회사 네트워크에 접속하여 근무
스마트워크 센터 근무	자택 부근의 ICT 환경이 갖춰진 원격 근무 사무실에서 근무
이동근무	모바일 오피스 환경을 이용한 현장에서 직접 근무하거나 이동하면서 근무

2.2 보안 취약점 분석

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. 위험이 발생할 가능성을 판단하기 위해서 잠재적 취약성과 스마트워

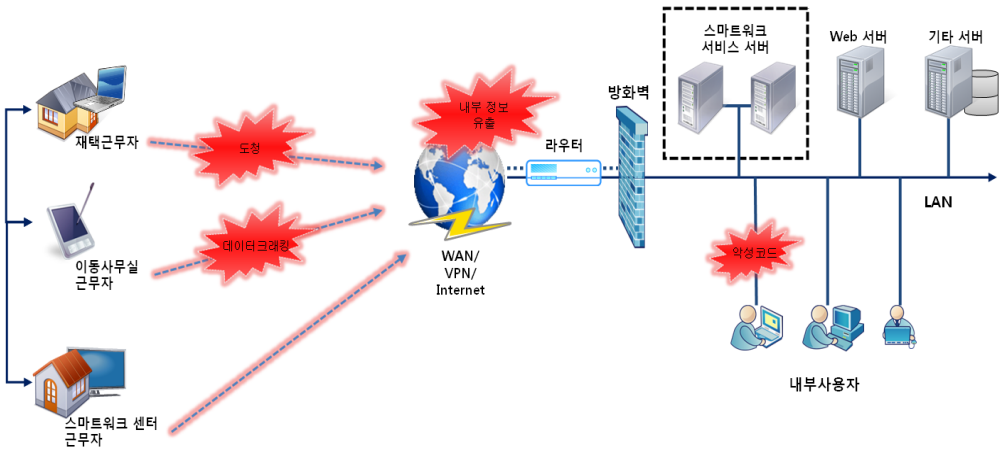

그림 1. 스마트워크 환경에서의 보안 위협
Fig. 1. Security Threat in Smartwork Environment

크 시스템에 도입된 통제와 함께 스마트워크 시스템에 대한 보안 위협 분석이 필요하다[5], [7-10].

2.2.1 스마트워크 환경에 적용하기 위한 사용자/디바이스 인증 기술 부재

기존의 업무에서는 보안이 통제되는 조직 내에서 업무를 처리하게 된다. 하지만 스마트워크 센터 근무나 이동근무 형태에서는 보안이 통제되지 않는 물리적 공간과 제 3자와 함께 시설을 사용하는 등의 노출된 공간에서 업무를 처리하게 된다. 이에 따라, 스마트워크 센터 근무나 이동근무에서는 자신이 처리하는 업무를 제 3자가 볼 수 있는 경우가 발생될 수 있다. 또한 스마트워크 센터에서는 잠시 자리를 비운 사이에 자신이 사용하는 단말기를 제 3자가 사용할 수 있으며, 공동으로 사용하는 PC의 경우에는 자신이 사용하는 데이터 기록이 해당 PC에 남아있을 수 있다.

2.2.2 스마트워크 환경에 적용하기 위한 접근제어 기술 부재

스마트워크 환경에서 핵심 기술로 사용되는 원격 접근기술은 주로 외부에서 업무를 처리할 때 조직 내부 시스템에 접속하여 내부 네트워크의 자원을 원격으로 처리하거나 내부 네트워크를 통하여 본사 내 다른 근무자들과 협업을 통한 업무를 처리하게 된다. 하지만 외부네트워크나 외부 전산장비를 통하여 접속하는 것은 내부에서 사용하는 방식보다 많은 위험이 내재되어 있으며 내부 자원들이 원격 접근을 통하여 외부로 노출될 위험이 높다.

대부분의 원격 접근은 인터넷을 통해 이루어지기 때문에 조직에서는 일반적으로 스마트워크 근무자들이 사용하는 외부 통신 네트워크들의 보안을 통제할 수 없다. 원격 접근에 사용되는 통신은 대부분 스푸핑 공격 및 중간자 공격에 취약하여 원격으로 접속하는 동안 전송되는 내부 중요 데이터들이 유출되거나 통신내용이 변경되어 전송될 수 있다.

또한 기존의 근무형태에서는 조직 내에 존재하는 내부 자원을 외부에서 접근할 수 없었지만, 스마트워크 환경에서는 이러한 내부 자원을 외부에서 원격 접근을 통해 접근이 가능해진다. 이에 따라 외부에서 접근하는 내부 자료들을 신뢰할 수 없는 장비와 통신 네트워크로 노출시켜 중요한 내부 자료가 외부로 유출될 수 있다.

2.2.3 스마트워크 환경에 적합한 데이터 보호기술 부재

최근 유행하는 악성코드는 시간이 지나면서 감염 증상이나 유포 방법이 다양해지고 복잡해지면서 지능화되고 있는 추세이다. 이로 인해 스마트워크에서 모바일 단말기를 이용하는 이동근무나 스마트워크 센터, 재택근무에서 사용되고 있는 PC나 모바일 단말기에 악성코드가 감염될 경우에는 사용자의 개인정보나 조직의 중요한 정보가 유출될 수 있다. 또한 사용자가 악성코드의 감염을 인지하지 못한 상태에서, 악성코드에 감염된 단말기를 사용할 경우에는 감염된 단말기로 조직의 내부 시스템에 접속하거나 다른 사람과 정보를 주고 받는 과정에서 악성코드가 조직 내부의 다른 단말기 및 서버 등과 스마트워크 센터의 단말기나 다른 사용자의 단말기에 전이될 우려가 있다. 이와 같이 전이된 악성코드는 또 다른 사용자에게 감염시키면서 빠른 속도로 악성코드가 확산될 수 있다.

이러한 악성코드는 사용자의 부주의로 악성코드를 유포하는 웹페이지에 접속하거나 P2P 서비스 사용, 불법 복제 프로그램을 사용할 때 감염되거나 내부자나 외부 공격자가 악성코드를 직접 설치하거나 스팸 메일에 포함시키는 등 다양한 경로를 통해 악성코드에 감염될 수 있다.

2.3 보안 요구사항

안전한 접근제어 기능을 제공하는 스마트워크 보안 프레임워크를 구성하기 위해서 만족해야 하는 요구사항은 표 2와 같다[11-13].

표 2. 안전한 접근제어 기능을 제공하기 위한 보안 요구사항
Table 2. Security Requirement for Providing Secure Access Control Function

요구사항	정의
사용자 인증	네트워크를 통하여 서버에 접속하는 사용자가 등록되어 있는 정당한 사용자인지 여부를 신뢰할 수 있게 제공해야 한다.
보안채널	스마트워크 사용자와 조직 네트워크 사이에 안전한 통신 채널을 형성하여 비밀성과 무결성을 제공해야 한다.
접근 제어	스마트워크 사용자의 소속 및 직위를 고려한 권한설정 뿐만 아니라 디바이스 성능, 네트워크 환경 정보들까지 고려하여 접근하는 권한을 제공해야 한다.
디바이스 인증	네트워크를 통하여 서버에 접속하는 디바이스가 등록되어 있는 정당한 디바이스인지 여부를 신뢰할 수 있게 제공해야 한다.

스마트워크 환경에서 발생 가능한 공격 방법은 표 3과 같다[14-16].

표 3. 스마트워크 환경에서 발생 가능한 공격
Table 3. Attack which is Possible in Smartwork environment

요구사항	정의
Replay Attack	공격자가 프로토콜상에서 유효 메시지를 선택하여 복사한 후 재전송함으로써 정당한 사용자로 가장하는 공격
Spoofing Attack	외부 악의적 네트워크 침입자가 임의로 웹사이트를 구성해 일반 사용자들의 방문을 유도, 인터넷 프로토콜인 TCP/IP의 구조적 결함을 이용해 사용자의 시스템 권한을 획득한 뒤 정보를 빼가는 해킹 수법
Man-in-the-Middle Attack	통신하고 있는 두 당사자 사이에 끼어들어 당사자들이 교환하는 공개정보를 공격자의 정보로 변경하여 도청을 하거나 통신내용을 바꾸는 수법

안전한 접근제어 기능을 제공하는 스마트워크 보안 프레임을 구성하기 위해서는 표 2의 요구사항을 만족해야 하며, 표 3에서 분석된 공격 가능한 방법으로부터 안전하게 설계되어야 한다.

III. 스마트워크 시스템

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

3.1 보안 채널 키 관리 서버

스마트워크 환경에서는 보안 채널 구축을 위한 키

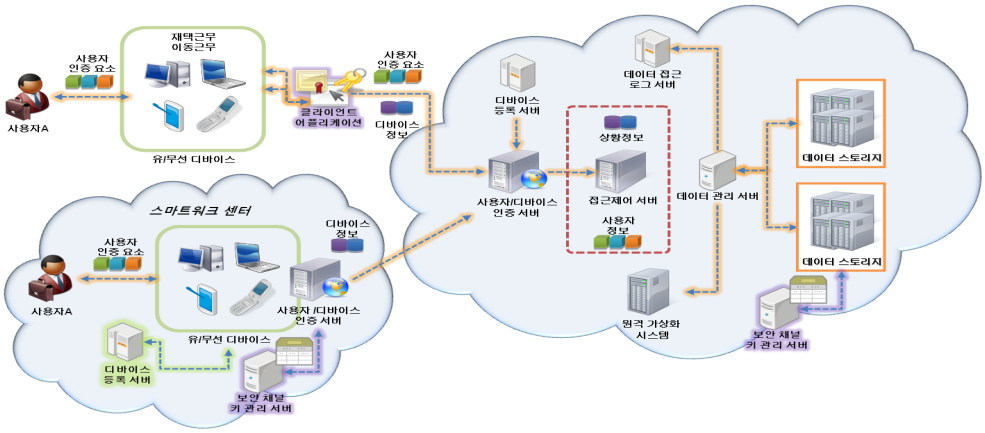

그림 2. 안전한 접근제어를 제공하는 스마트워크 프레임워크
Fig. 2. Smartwork Framework Providing Secure Access Control

관리 기술을 적용하는 구간을 두 가지로 구분할 수 있다. 첫 번째는 재택근무와 이동 근무 중에 자신의 디바이스를 통해 업무를 지속하고자 할 때 구성되는 네트워크 환경이고, 또 다른 하나는 스마트워크 센터를 통해 업무를 지속하고자 할 때 구성된다. 스마트워크 센터의 경우, 다수의 사용자가 조직으로 접근하기 용이하도록 환경이 구축되어야 하므로, 개별적인 보안 채널 구축이 필수적이다. 따라서 사용자는 자신이 속한 조직과 스마트워크 센터의 키 관리 서버 간 보안 채널 구축을 위한 키 교환을 수행한다. 이 때, 사용자는 자신의 계정(ID/PW)을 이용한 인증 요소, 대상 조직의 사용자 인증 정보를 제공하여 보안 채널을 구성한다.

스마트워크 센터 내 보안 채널 키 관리 서버는 조직의 서버에 보안 채널 형성을 요청하고, 조직의 보안 채널 키 관리 서버는 필요한 보안 수준을 요구하게 된다.

또한 네트워크 환경 및 디바이스 성능에 따라 가용되는 프로세스가 상이할 수 있다. 예를 들어 스마트워크 센터 내부에서 조직 네트워크에 접근할 경우에는 구축되어 있는 보안 인프라를 바탕으로 높은 수준의 보안성을 제공할 수 있는 프로세스를 수립할 수 있으며, 보안 채널의 형성 및 유지가 비교적 쉽다.

반면에 스마트워크 센터 외부 공간에서 조직에 접근할 경우, 보안에 관련된 부분이 사용자의 디바이스 안에서만 이루어지므로 애플리케이션에 한정적이다. 따라서 사용자의 인증 요청이 이루어지기 전에 보안 채널을 구성하고 안전한 네트워크 안에서 사용자 및 디바이스 인증이 수행되어야 한다. 이를 위해 사용자 및 디바이스 인증을 위한 프로토콜 구성 및 알고리즘 선택에 가변성을 제공한다. 이와 같은 가변성은 디바이스 성능 및 사용자의 접근 네트워크 환경에 따라 인터페이스 및 인증 세부 요소를 달리 제공하여 보장하고, 보안 채널 내부에서 사용되는 키 관리 기술과 연계하여 보안 키 구성을 수행한다.

보안 수준에 대한 협의가 완료되면 상호간의 보안 채널 통신을 위한 키를 교환하고 사용자가 업무를 지속할 수 있도록 연결해 준다.

표 4. 스토리지에 저장되어 있는 정보
Table 4. Information Stored in Storage

보안 레벨	인증 정보	디바이스	알고리즘	인증 요소	데이터
SL_0	mk_0	$Notebook_0$	RSA	$ID_0 \| PW_0$	Information
	...	...	...	...	...
	mk_i	$Notebook_i$	AES	$ID_i \| PW_i$	Information
SL_1	mk_{i+1}	$Smartphone_{i+1}$	RSA	$ID_{i+1} \| PW_{i+1}$	Information
	...	...	...	...	Information
	mk_j	$Smartphone_j$	AES	$ID_j \| PW_j$	Information
...	...	...	...	...	...

SL_n	mk_{m+1}	$Desktop_{j+1}$	RSA	$ID_{m+1} \| PW_{m+1}$	Information
	...	...	...	...	Information
	mk_n	$Desktop_n$	AES	$ID_n \| PW_n$	Information

3.2 사용자/디바이스 인증 서버

스마트워크 환경에서 정당한 사용자가 업무를 지속하기 위한 사용자/디바이스 인증 기술은 업무를 통하여 취급하는 정보가 조직 정보 및 내부 자료 등 높은 보안을 요구하게 되므로 정당한 사용자 식별 및 안전한 디바이스 사용이 필수적으로 요구된다.

스마트워크 센터와 같은 경우, 사용자가 조직에 접근하고자 할 때에는 사용자/디바이스 인증 서버와 디바이스 등록 서버를 통해 조직과 인증 과정을 수행하게 된다. 이 때, 스마트워크 센터의 사용자/디바이스 인증 서버에는 사용자의 인증 정보가 저장되지 않고 조직에서 전송한 정보와 비교하는 역할을 수행한다. 먼저 사용자의 인증 요소를 디바이스를 통해 입력 받아 특정 연산을 수행하여 이를 전송하게 된다. 그 후 조직의 사용자/디바이스 인증 서버에서 사용자 식별이 완료되면, 사용자의 인증 정보를 스마트워크 센터에 전송한다.

여기에서 식별 정보만을 보내지 않는 이유는 Replay Attack, Man-in-the Middle Attack 등으로 정당하지 않은 사용자를 정당한 사용자로 위장할 수 있기 때문이다. 이러한 정당하지 않은 사용자의 경우, 조직 내부에 접근하지 못하더라도 스마트워크 센터 내부에서 보안상의 위협을 발생시킬 수 있기 때문에 이를 방지하기 위해서 필요하다.

디바이스 인증에서 스마트워크 센터 외부의 공간에서 접근할 때에는 사용자 인증과 같이 디바이스의 인증 정보를 전송하고 조직의 디바이스 등록 서버의 정보와 비교하여 인증을 수행한다. 이를 통해 정당한 디바이스를 통한 접근이 이루어졌는지 확인하게 된다. 스마트워크 센터에서도 앞선 과정을 동일하게 수행하지만 센터 내부에서도 디바이스 등록 서버를 적용한다. 해당 등록 서버는 다수의 사용자가 접근하는 스마트워크 센터에서 발생할 수 있는 보안 문제점을 방지하고, 보안상의 문제를 발생시킨 디바이스 및 사용자에 대한 추적이 가능하도록 활용된다. 스마트워크 센터에서는 다양한 조직 네트워크에 접근하게 되고 각각의 보안 요구사항 및 환경이 다르므로, 디바이스에 대한 인증 절차를 포함하지 않는 경우도 존재한다. 이러한 경우 센터 내부에서 발생하는 보안상의 문제점에 대한 관리를 위하여 디바이스 등록 서버를 활용한다.

3.3 클라이언트 어플리케이션

기본 인프라가 제대로 구축되기 힘든 재택근무나 이동근무 중의 디바이스를 통한 접근 시에는 보안 채널 키 관리 서버를 이용할 수 없으므로, 클라이언트 애플리케이션이 키 관리 기능을 포함하게 된다. 클라이언트 애플리케이션은 사용자 인증, 접근제어를 수행하기 이전에 키 관리 기능을 통해 보안 채널을 구축하고 이를 통해 조직에서 허용한 범위 내의 업무를 지속할 수 있다. 다만 디바이스 컴퓨팅 성능과 네트워크 환경에 따라 보안 수준이 상이할 수 있으므로, 제한적인 업무가 이루어 질 수 있다. 이와 같은 부분은 각 조직이 허용하는 업무 범위를 선정하여 보안성을 향상 시킬 수 있다.

이와 달리 스마트워크 센터 외부의 공간에서 개인 디바이스를 통해 조직 내부로 접근 시에는 스마트워크 센터의 사용자/디바이스 인증 서버와 같은 개별적인 처리 서버를 이용할 수 없으므로, 클라이언트 애플리케이션이 사용자/디바이스 인증 기능을 포함하게 된다. 그러나 이와 같은 환경에서는 사용자/디바이스 인증 기능이 비교 연산을 위하여 사용되는 것이 아니라 안전하게 정보를 전송하기 위한 기능으로 활용된다. 사용되는 디바이스에 따라 인증 요소 및 네트워크 환경이 달라지고 이를 기반으로 하는 알고리즘 및 프로토콜도 다양하게 적용된다. 따라서 접근 환경 요소에 따라 개별적으로 사용자 인증 알고리즘 및 프로토

콜을 적용할 필요가 있다.

3.4 접근제어 서버

본 논문에서는 사용자의 소속 및 직위를 고려한 권한설정 뿐만 아니라 다양한 상황정보(디바이스 성능, 네트워크 환경 등) 정보들까지 고려한 접근제어 기술을 제안한다. 제안 모델의 개념도는 그림 3과 같다.

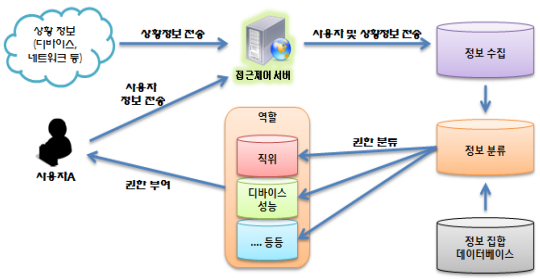

그림 3. 역할 및 네트워크 환경에 따른 접근제어 기술
Fig. 3. Access Control Technique According to Role/Network Environment

각 사용자는 스마트워크 환경에 접근 시, 사용자의 역할을 기반으로 권한을 부여받는다. 또한 사용자가 사용하는 디바이스 성능 및 네트워크 환경에 따라 제공받을 수 있는 보안 서비스의 등급이 다르므로 사용자의 작업 환경에 대한 상황정보를 기반으로 권한을 부여받는다. 이를 통해 각각의 상황에 적절한 권한 설정을 수행하여 불필요한 시스템 자원의 오버헤드를 감소 시키고 안전성을 높일 수 있다.

또한 각 사용자들은 재택근무나 모바일 오피스, 스마트워크 센터에서 사용하는 디바이스를 디바이스 인증서버에 등록을 하고 스마트워크 접근제어 서버는 디바이스의 환경에 따라 시스템에 접근 수준을 결정하는 방식이다. 이는 각 디바이스마다 암호화 연산이나 통신 능력과 같이 하드웨어의 한계에 따른 보안 취약점을 보완하게 된다. 사용자의 PC나 노트북 등의 경우 암호화 능력이 기타 휴대 디바이스와 비교하여 여러 보안적인 기술들을 다양하게 적용이 가능하기 때문에 접근관리시스템이 모든 작업을 할 수 있는 접근 수준을 부여하고, 하드웨어적 성능이 부족한 스마트폰이나 모바일 디바이스 같은 경우는 적용할 수 있는 보안 기술에 따라 접근하여 작업할 수 있는 접근 수준을 PC나 노트북보다는 제한을 하는 형식이다. 또한 스마트워크 시스템을 사용하여 외부 네트워크와 조직의 내부 네트워크를 동시에 사용할 경우 외부 네트워크를 통하여 스마트워크 시스템이 위협을 받을 수 있기 때문에 외부 네트워크에 접근하는 것도 접근제어 서버가 제어를 하게 된다.

접근제어 서버는 등록된 디바이스의 정보를 토대로 각 디바이스가 접근했을 때 권한을 수시로 변경을 한다. 스마트워크의 특징상 동일한 디바이스를 사용하더라도 접근하는 네트워크 환경이 다를 수 있기 때문에 접근제어 서버는 디바이스 등록서버에 등록된 디바이스 정보 외에 접속하는 네트워크의 환경 정보를 수집하고 디바이스 정보와 네트워크 환경정보에 따라 접근 수준을 최종적으로 부여한다.

3.5 디바이스 등록 서버

스마트워크에서는 서로 다른 이기종의 디바이스가 스마트워크 시스템에 접근하여 업무를 수행할 수 있어야 한다. 재택근무에 사용되는 PC나 노트북, 모바일 오피스에 사용되는 휴대 디바이스를 비롯하여 영상회의에 사용되는 영상회의 단말 등 다양한 디바이스의 접근이 이루어지게 된다. 이는 여러 가지 서로 다른 디바이스가 회사의 시스템에 접근을 할 때 기존의 IT 시스템 접근 기술을 그대로 스마트워크 시스템에 적용할 경우 문제가 생길 수 있다는 것을 의미한다. 기존의 시스템에서는 단일 하드웨어에 종속되어 다양한 디바이스의 접근이 이루어졌지만 스마트워크에서는 기존에 구축된 내부 네트워크와 외부 네트워크를 동시에 사용이 가능하기 때문에 네트워크 연동에 따라 발생할 수 있는 보안적인 문제점을 고려해야 한다.

스마트워크 사용자가 스마트워크 시스템에 접근할 때 각 사용자의 디바이스들은 접근관리시스템을 통하여 스마트워크 시스템에서 수행할 수 있는 역할을 할당받게 된다.

디바이스 등록서버에는 각 디바이스의 정보, 디바이스에 저장되어 있는 주요정보, 디바이스의 보안상태(사용하고 있거나 적용 가능한 보안 장치) 등의 정보를 등록 한다.

3.6 데이터 관리 서버

스마트워크 환경에서는 이동 중이거나 사내가 아닌 외부에서 실시간으로 조직 및 정부기관의 업무를 파악하고 조직 네트워크에 접속하여 업무를 처리할 수 있다. 이는 곧 외부에서 내부 데이터에 접근이 가능하고 데이터가 유출될 가능성이 있다는 것을 의미하며 현재 스마트워크는 안정된 인터넷 서비스와 대용량 데이터를 처리할 수 있는 대용량 분산 파일시스템을 사용하여 데이터를 저장한다. 이러한 분산 파일시스템은 대용량의 데이터를 제공과 복제 데이터 유지 및 복구 기능의 장점이 있지만, 가상화를 통해 데이터를 논리적으로 분할 저장함으로써 안전성에 대한 문제가 지적되고 있다.

분산 파일시스템을 이용하는 사용자는 자신의 데이터가 어떤 서버에 저장되는지 정확히 알 수 없으며 해당 데이터가 안전하게 저장되어 있는지 알 수 없다. 데이터 서버들이 가상화되어 하나의 볼륨으로 묶이게 되면 볼륨에 접속한 사용자는 볼륨 내부의 데이터에 자유롭게 접근할 수 있는 구조로 안전성이 제공되지 않고 있으며, 이를 통하여 악의적인 사용자에 의해 민감한 개인정보가 노출될 수 있는 문제점이 존재한다.

따라서 스마트워크를 안전하게 이용하기 위해서 데이터 유출 방지 및 제어 기술 및 데이터 트래킹 관리 기술의 필요성이 증대됨에 따라 접근제어 기술을 기반으로 스마트워크 환경에서 데이터 보안/관리 기술을 제안한다.

제안 모델은 크게 데이터 유출 방지 및 제어 기술과 데이터 트래킹 및 관리 기술로 구분한다.

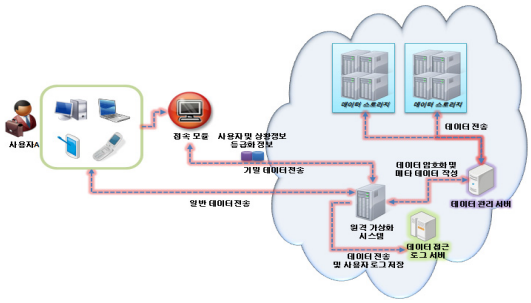

그림 4. 데이터 보안/관리 기술
Fig. 4. Data Security/Management Technique

3.6.1 데이터 유출 방지 및 제어 기술

스마트워크 환경에서는 다수의 서버를 가상화하여 스토리지 서비스를 제공하는 분산 파일시스템을 도입하여 대용량의 스마트워크 데이터를 처리할 수 있게 되었다. 그러나 앞서 언급한 바와 같이 기존에 개발된 분산 파일시스템은 구조상 안전성에 대한 문제점이 존재한다. 이를 해결하기 위해 본 논문에서는 접근제어 방식과 데이터 보안 기술을 참조하여 데이터 유출을 방지하고 제어한다.

분산 파일시스템에 저장된 데이터들은 논리적으로 분할되어 저장된다. 데이터 관리 서버는 이러한 데이터들을 분류하고 관리하는 서버로써 데이터에 대한 등급을 분류하고 접근제어 서버에서 인증된 사용자의 등급에 따라 데이터를 제공한다.

그러나 인가된 사용자라 하더라도 사용자의 상황정보에 따라 데이터 전송을 거부한다. 이는 보안 채널이 형성되어 있지 않은 네트워크나 보안 프로그램이 설치되어 있지 않아 악성 코드에 의한 피해가 발생할 수 있는 디바이스의 경우 데이터 유출을 방지하기 위함이다. 또한 접속 모듈을 통해서만 등급이 높은 데이터에 접근할 수 있게 하여 데이터 유출에 대한 취약점을 해결할 수 있다.

3.6.2 데이터 트래킹 및 관리 기술

일반적인 업무를 수행하는데 있어 접근 모듈을 통한 데이터 접근은 비효율적이다. 따라서 이를 해결하기 위해 본 논문에서는 일반적인 데이터에 부여되어 있는 메타 데이터에 보안 기능을 추가한다. 사용자가 데이터에 대한 접근을 요구할 시, 제공되는 데이터의 메타 값에 제공되는 사용자의 값을 삽입과 동시에 해당 정보를 데이터 로그 서버에도 저장하여 데이터 유출 시, 메타 데이터 값과 데이터 로그 서버를 비교하여 초기 유출 경로 트래킹을 신속하게 수행할 수 있도록 한다.

Ⅳ. 결 론

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 프레임워크 및 위험 관리 방안을 제안하였다.

본 논문을 통해 스마트워크 서비스 사업자들이 데이터 보안, 사용자/디바이스의 인증, 접근제어 등 보안 환경을 구축하는데 적용할 수 있다.

참고문헌

[1] 김성태, "*녹색생활 실천전략IT기반 원격근무*", 한국정보화진흥원, 2009.

[2] 방송통신위원회, "*기업을 위한 스마트워크 도입・운영 가이드북*", 2011.

[3] 행정안전부, "*스마트워크 추진 계획*", 2010.

[4] 김성태, "*녹색생활 실천전략IT기반 원격근무*", 한국정보화진흥원, 2009.

[5] G. Stonebumer, A. Goguen, and A. Feringa, "*Risk Management Guide for Information Technology Systems*", NIST SP 800-30, 2002.

[6] K. Scarfone, P. Hoffman, and M. Souppaya, "*Guide to Enterprise Telework and Remote Access Security*", NIST SP 800-46 Rev 1, 2009.

[7] L. J. Carnahan, and B. Guttman, "*Security Issues for Telecommuting*", National Institute of Standards and Technology, pp. 2-6, 1996.

[8] G. Jacob, H. Debar and E. Filiol, "Malware Behavioral Detection by Attribute-Automata Using Abstraction from Platform and Language", Lecture Notes in Computer Science, Vol 5758/2009, pp. 81-100, 2009.

[9] Y. P. Liaoa, and S. S. Wanga, "A secure dynamic ID based remote user authentication scheme for multi-server environment", Computer Standards & Interfaces, Vol 31, pp. 24-29, 2009.

[10] S. Yu, K. Ren, W. Lou, "FDAC: Toward Fine-Grained Distributed Data Access Control in Wireless Sensor Networks", IEEE INFOCOM, Vol. 22 no. 4, pp. 673-686, 2009

[11] M. K. Khan and J. Zhang, "Improving the security of a flexible biometrics remote user authentication scheme", *Computer Standards and Interfaces*, Vol. 29, No. 1, pp. 82-85, 2007.

[12] T. Finin, A. Joshi, and L. Kagal, J. Niu, R. Sandhu, W. Winsborough, B. Thuraisingham, "ROWLBAC: representing role based access control in OWL",

Proceedings of the 13th ACM symposium on Access control models and technologies, June 11-13, 2008.

[13] Matsunaka, T., Warabino, T., and Kishi, Y., Nakauchi, K., Umezawa, T., Inoue, M., "Device Authentication and Registration Method Assisted by a Cellular System for User-Driven Service Creation Architecture", *Consumer Communications and Networking Conference (CCNC 2009)*, pp. 10-13, 2009.

[14] R. Pries, W. Yu, X. Fu and W. Zhao, "A New Replay Attack Against Anonymous Communication Networks", *In Proceedings of the IEEE International Conference on Communications (ICC)*, May 19-23, 2008.

[15] Y. Yao, W. Yang, and Y. Yao, Y. Li, "A switch-based ARP attack containment strategy", *Communication Systems, Networks and Applications (ICCSNA)*, pp 123-126, June 29 2010-July 1 2010.

[16] K. Ouafi, R. Overbeck and S. Vaudenay, "On the Security of HB# against a Man-in-the-Middle Attack", *Advances in Cryptology - ASIACRYPT 2008*, Lecture Notes in Computer Science, Vol 5350/2008, pp. 108-124, 2008.

감사의 글

본 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2011-0007755).

저자소개

이동범(Dongbum Lee)

2010년 순천향대학교 정보보호학과 (공학석사)

2010년~현재 순천향대학교 정보보호학과 박사과정

※ 관심분야 : 정보보호, 정보보호제품 평가 등

곽 진(Jin Kwak)

2003년 성균관대학교 컴퓨터공학과 (공학석사)

2006년 성균관대학교 컴퓨터공학과 (공학박사)

2007년~현재 순천향대학교 정보보호학과 교수

※ 관심분야 : 암호 프로토콜, 개인정보보호 등