스마트워크 환경에 접근 가능한 안전한 디바이스 인증 기법 연구

고웅*, 곽진*
*순천향대학교 정보보호학과
e-mail:wgo@sch.ac.kr, jkwak@sch.ac.kr

A Study on Secure Device Authentication Method in Smartwork

Go Woong*, Jin Kwak*
*Dept of Information Security Engineering, Soonchunhyang Univ.

요 약

최근 들어 스마트 기기의 확대로 인해 생활환경에 큰 변화가 나타나기 시작했다. 특히 스마트 기기를 활용하여 언제 어디서든지 업무를 지속할 수 있는 스마트워크 환경에 대한 관심과 연구가 증가하고 있다. 그러나 국내 스마트워크 연구는 초기 단계에 머물러 있으며, 스마트워크 환경에 접근하는 디바이스에 대한 보안 연구 또한 미비한 실정이다. 따라서 본 논문에서는 스마트워크 환경에서 업무 지속성을 위해 접근되는 디바이스의 안전한 접근을 위한 디바이스 인증 기법을 제안한다.

1. 서론

최근 정보통신의 발전과 스마트 기기의 출현으로 인해 삶의 질을 향상 시킬 수 있는 업무 효율성 증가에 대한 관심이 증가하고 있다. 기존의 업무 환경이 특정 제한된 공간에서의 일정 시간동안의 업무를 수행해야 하면서, 이와 같은 관심이 증가하였다. 특히 재택근무, 이동근무 등과 같이 시간과 장소에 제한되지 않는 스마트워크 환경 구축에 대한 요구가 증가하고 있다.

스마트워크 환경은 재택근무, 스마트워크센터근무, 이동근무를 통해 시간과 장소에 상관없이 업무의 지속성을 보장하는 환경이다. 이와 같은 환경은 실내 기업 내부망에 접근하여 업무를 지속하기 때문에 정당한 사용자 및 디바이스에 대한 인증이 중요한 보안 요소로 작용하고 있다.

그러나 현재 스마트워크 환경에 대한 연구는 초기단계에 머물러 있으며, 인증에 대한 연구 또한 미비한 실정이다. 또한 스마트워크 환경에 대한 명확한 표준이 없어 기업마다 개별적으로 환경을 구축하고 있는 실정이다.

따라서 본 논문에서는 스마트워크 환경에 접근하는 정당한 디바이스에 대하여 안전한 인증 기법을 제안한다.

본 논문의 구성은 2장에서 스마트워크 환경에 대한 개요를 분석하고 3장에서 문제점에 대하여 분석한다. 4장에서는 안전한 디바이스 인증 기법을 제안하고 5장에서 보안성 및 효율성을 분석한다. 그리고 6장을 결론으로 끝을 맺는다.

2. 스마트워크 개요

스마트워크는 기존의 제한된 공간, 시간에서 탈피하여 언제 어디서나 효율적이고 편리하게 업무를 지속할 수 있는 업무환경이라고 정의할 수 있다. [1]

이러한 스마트워크는 시간과 장소에 따라 재택근무, 스마트워크센터 근무, 이동근무 등으로 구분이 가능하며, 원격근무(Teleworking), Telecommuting, Flexible Working 등의 용어와 개념적으로 유사하게 사용되고 있다.[2]

<표 2> 스마트워크 근무 유형 분석

유형	근무형태	장점	단점
재택근무	자택에서 네트워크를 통해 업무 수행	- 별도의 공간 불필요 - 출퇴근 시간 및 비용 감소	- 노동자의 고립감 증가 및 협동 업무 효과 감소 - 보안성 부족으로 일부 업무만 가능
이동근무	모바일 기기 등을 이용하여 현장에서 업무 수행	- 대면업무 및 이동이 많은 경우 유리	- 위치추적 등을 통한 개별 감시 및 프라이버시 침해 - 보안성 부족으로 일부 업무만 가능
스마트워크 센터근무	인근 원격사무실에서 업무 수행	- 충분한 업무 환경 제공 - 근태관리 용이 - 보안성 확보 용이 - 업무 집중도 향상 가능	- 별도의 공간 및 비용 소요 - 시스템 구축 및 관리 필요

국내에서는 2015년 공공 50개, 민간 450개의 스마트워크센터 구축을 목표로 정부에서 추진하고 있다. 그러나 스마트워크 활성화는 국내에 비해 국외에서 더욱 원활히 진

행되고 있다. 미국의 경우 연방기관 중 원격근무를 관장하는 인사관리처(OPM : Office of Personnel Mangement)와 일반행정청(GSA : General Services Administration)을 두고 체계적으로 진행하고 있다. 또한 일본에서는 '기업을 위한 텔레워크 도입, 운용 가이드북'을 통해 스마트워크 환경 구축을 위해 필요한 부분을 지원하고 있다. [3][4]

3. 보안 문제점 분석

스마트워크 환경은 기본적으로 유/무선 디바이스를 이용하여 외부에서 기업 내부로 네트워크를 통한 접근을 수행하게 된다. 따라서 사용자 인증뿐만 아니라 정당한 디바이스에 대한 인증 과정이 필수적으로 필요하다. 현재 디바이스 인증에 대한 연구는 다양하게 진행되고 있으나, 기존의 디바이스 인증 기법을 스마트워크 환경에서 적용하기에는 다소 무리가 있다.

스마트워크 환경에서는 다수의 디바이스가 다수의 기업에 접근하게 되며, 다루게 되는 정보 또한 기업의 기밀정보 등 높은 등급의 보안 수준을 요구하는 경우도 많다.

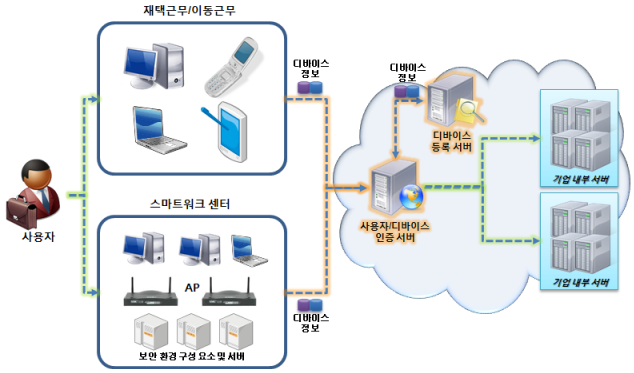
스마트워크 센터의 경우에는 일정한 보안 수준을 만족하기 위하여 보안 인프라가 구축되어 보다 안전한 수준의 접근이 가능하다. 그러나 이동근무나 재택근무와 같은 경우, 보안에 대한 위험이 상대적으로 높다. 또한 스마트워크 센터가 상대적으로 안전하다 하더라도 정당한 디바이스에 대한 검증이 수행되지 않는다면 스마트워크 센터 내 시스템에 불법프로그램, 악성코드 등으로 인한 문제가 발생할 수 있다.

따라서 이와 같은 보안 문제를 해결하기 위해서 안전한 디바이스 인증 기법에 대한 연구가 필요하다.

4. 안전한 디바이스 인증 기법 제안

안전한 디바이스 인증 기법을 위하여 본 논문에서는 스마트워크 환경에서 접근하는 디바이스에 대하여 등록 단계 및 인증 단계로 구분하여 제안한다.

다음은 그림은 본 논문에서 제안하는 디바이스 인증 기법의 전체 흐름도를 나타낸다.

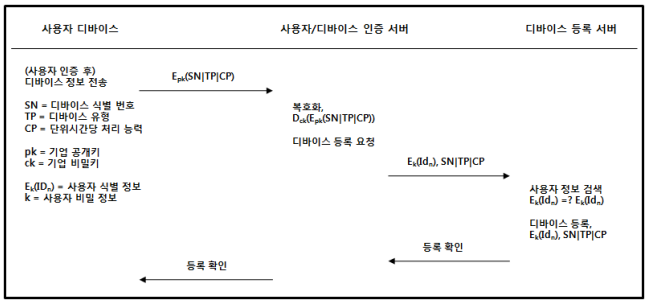


(그림 1) 제안 방안 전체 흐름도

4.1 디바이스 등록 단계

디바이스 등록 단계는 스마트워크 환경에 접근하는 모든 디바이스에 대한 등록을 수행하며, 사전 등록 과정을 거친다. 디바이스 등록 시에는 디바이스의 식별 번호(Serial Number), 유형, 단위시간당 처리능력 등의 정보를 함께 저장하게 되는데, 이는 정당한 디바이스의 식별과 가능한 업무 제한을 위하여 사용된다.

다음은 디바이스 등록을 위한 프로토콜에 대하여 기술한 것이다.



(그림 2) 디바이스 등록 단계

본 논문에서 진행되는 디바이스 등록 단계 전제조건으로 사용자 인증을 수행한 후 진행되는 것으로 가정한다. 따라서 사용자 인증에 대한 수행 과정은 포함하고 있지 않다.

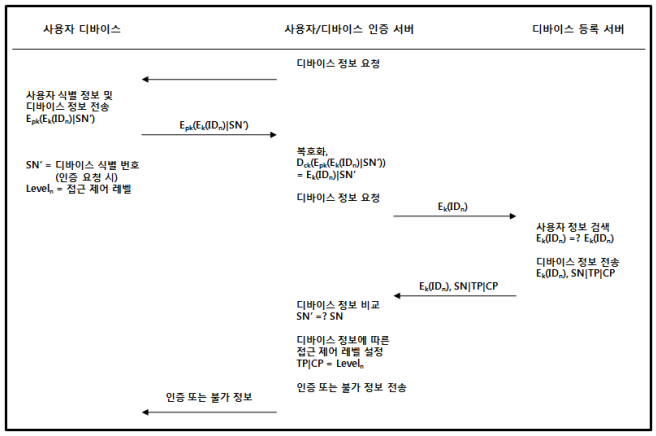
디바이스 등록은 사용자에 대한 인증이 정상적으로 수행되고 나면 서비스 이용을 위한 사용자의 디바이스 등록 요청이 수행된다.

① 먼저 디바이스 식별번호와 디바이스 유형(PC, 스마트폰, PDA 등), 단위시간당 처리 능력 정보를 기업의 공개키로 암호화하여 등록 요청을 한다. ② 기업의 사용자/디바이스 인증 서버는 해당 정보를 복호화하고 사용자의 식별 정보와 함께 등록 서버로 전송한다. 본 단계는 내부망을 통해 전송되므로 별도의 암호화를 수행하지 않는다. ③ 디바이스 등록 서버는 전송된 정보를 통해 사용자 정보를 검색한다. 이는 사용자가 하나의 디바이스만 사용하는 것이 아니므로 다수의 디바이스를 등록하기 위하여 수행되며, 사용자 식별 정보를 인덱스로 하여 등록 테이블을 구성한다. 이를 통해 사용자의 중복 등록을 방지한다. ④ 최종적으로 사용자 검색을 마치고 나면 등록 확인 정보를 사용자에게 전송한다.

4.2 디바이스 인증 단계

디바이스에 대한 등록이 완료되고 사용자가 기업 망에 접근하여 업무 및 서비스를 이용하고자 할 때에는 정당한 사용자 인증뿐만 아니라 디바이스에 대한 인증을 수행한다. 이 때, 사용자의 디바이스 유형 및 성능에 따라 접근 가능한 업무를 제한한다.

다음은 디바이스 인증을 위한 프로토콜에 대하여 기술한 것이다.



(그림 3) 디바이스 인증 단계

사용자가 기업 망에 접근하여 업무 및 서비스를 수행하고자 할 때에는 디바이스 인증 단계가 수행된다. 디바이스 등록 단계와 마찬가지로 사용자 인증 완료를 전제조건으로 가정한다.

① 기업 망의 사용자/디바이스 인증 서버는 사용자 인증 후 디바이스에 대한 정보를 요청한다. ② 사용자는 자신의 디바이스 인증을 위하여 사용자 식별 정보와 디바이스의 식별 번호를 기업의 공개키로 암호화하여 전송한다. 이 때, 사용자의 식별 정보를 같이 보내는 이유는 해당 기업 망에 다수의 사용자가 접근하기 때문에 디바이스 식별 정보가 혼선을 빚는 것을 방지하기 위해서 전송된다. ③ 디바이스 정보가 전송되면 사용자/디바이스 인증 서버는 이를 복호화하고 디바이스 등록 서버에 사용자 식별정보를 전송하여 디바이스 정보를 요청한다. ④ 디바이스 등록 서버는 사용자 식별 정보를 통해 디바이스 정보를 검색하고 이를 다시 사용자/디바이스 인증 서버로 전송한다. 여기에서 보내지는 사용자 식별정보도 ② 단계와 마찬가지 이유로 함께 전송된다. ⑤ 전송받은 식별 정보 중 디바이스 식별 번호를 비교하여 해당 디바이스의 등록 여부를 확인한후, ⑥ 디바이스 유형과 단위시간당 처리 능력 여부를 기반으로 접근제어 레벨 테이블에서 접근 가능한 업무 범위를 설정한다. ⑦ 최종적으로 모든 인증 과정이 완료되면 인증 완료 또는 불가 정보를 전송한다.

5. 안전성 및 효율성 분석

본 논문에서 제안한 안전한 디바이스 인증 기법을 통해 인증을 수행할 경우, 스마트워크를 통한 업무를 수행하는데 있어 다음과 같은 이점을 가져올 수 있다.

<표 3> 안전성 및 효율성 분석

분류	기존 방안	제안 방안
정당한 디바이스 인증	- 사용자 인증 기반 - 별도의 디바이스 인증 없음	- 디바이스 별도 인증 - 비인가된 디바이스 접근 불가
중요 정보 노출 방지 및 추적 용이	- 디바이스의 사용자 확인 불가(추적 불가)	- 사용자 정보 등록으로 인한 정보 노출 예방 - 등록된 디바이스의 사용자 추적 가능
악의적인 사용자의 접근 방지	- 사용자의 정보만 있으면 접근 가능	- 사용자의 정보만 가지고 접근 불가능 - 사용자 정보와 디바이스 정보가 일치해야만 접근 가능
디바이스 별 업무 접근제어 가능	- 디바이스 별 접근제어 불가능 (획일적인 통제)	- 디바이스 유형 및 성능에 따른 개별적 업무 접근제어 제공

6. 결론

정보통신기술의 급격한 발달은 공간과 시간의 제약이 존재하는 업무환경에 커다란 변화를 가져오고 있다. 기존의 업무 환경이 특정 제한된 공간에서의 일정 시간동안의 업무를 수행해야 하면서 좀 더 효율적이고 유연한 업무 환경에 대한 요구가 증가하게 되었다. 따라서 이러한 요구를 만족시킬 수 있는 스마트워크 환경에 대한 관심이 증가하게 되었으며 다수의 기업 및 공공기관에서 이를 활용하고 있는 사례가 증가하고 있다. 그러나 아직까지 스마트워크 환경에 대한 연구는 초기 단계에 머물러 있고, 특히 보안에 대한 연구는 미비한 상황이다. 그 중에서도 다수의 디바이스가 다수의 기업에 접근하는 스마트워크 환경에서 디바이스에 대한 인증 단계는 필수적으로 요구된다.

이에 본 논문에서는 스마트워크 환경에 접근하는 다양한 디바이스에 대하여 안전하고 정당한 인증과 디바이스 성능에 따른 업무 접근제어를 수행하는 방안을 제안하였다.

이를 통해 스마트워크 환경을 구축하고 내부망에 접근하여 업무를 수행할 때, 인가되지 않은 디바이스에 대한 원천적 차단이 가능하고 중요 정보 노출 차단 및 유출 정보 추적이 가능할 것으로 기대할 수 있다. 이를 통해 스마트워크 환경 전반에 대한 보안성을 향상시킬 수 있을 것으로 기대된다.

참고문헌

[1] 스마트워크센터, http://www.smartwork.go.kr/
[2] 이재성, 김홍식. “스마트워크 현황과 활성화 방안 연구”, 한국지역정보화학회지, 제13권 제4호, pp.75-96, 2010.
[3] 한국정보화진흥원, “IT기반 원격근무 재조명과 정책이슈”, 제7호, 2009
[4] OPM, "Status of Telework in the Federal Government", 2011.