스마트워크 환경에서 동적으로 접근 권한을 제어하기 위한 메커니즘

윤관식*, 김강석*, 김기형**, 예홍진**
*아주대학교 대학원 지식정보공학과
**아주대학교 정보컴퓨터공학과
e-mail:bbangtte@ajou.ac.kr

A Mechanism for Controlling Accesses Dynamically in Smartwork Environment

Kwansik Yoon*, Kangseok Kim*, Ki-Hyung Kim**, Hongjin Yeh**
*Dept. of Knowledge Information Engineering, Graduate School of Ajou University, Suwon, Korea
**Dept. of Information and Computer Engineering, Ajou University, Suwon, Korea

요 약

정보통신기술의 발전으로 기업의 내에서만 업무를 하던 시대에서 벗어나 언제 어디서나 손쉽게 업무를 수행할 수 있는 스마트워크 환경이 가능하게 되었다. 특히 모바일 디바이스의 성능 발전과 급속한 보급은 스마트워크를 이용하는 환경이 다양해지는 계기가 되었고 이로 인해 동일한 사용자라 할지라도 스마트워크에 접근하는 방법이나 환경이 동적으로 변경 될 수 있다. 이러한 특성은 보안 위협의 유형도 다양하게 하여 기업 내부의 정보를 보호하기 어렵게 만들었다. 이로 인해 기존의 사용자 정보 중심의 통합 인증 관리시스템인 EAM(Extranet Access Management)만으로 다양한 위협에 대응하기에는 부족하게 되었다. 이에 본 논문에서는 기존 EAM 시스템의 한계를 알아보고 스마트워크 환경에서 사용자 정보 외에 디바이스, 네트워크, 위치 정보를 활용하여 접근 시의 환경에 따라 사용자의 권한도 동적으로 생성하는 방식을 제안한다.

1. 서론

스마트워크는 정보통신기술을 이용하여 시간과 장소의 제약 없이 업무 수행에 있어서 관계자들과 협업하고 지속적인 업무 수행을 지원하는 근무 형태라 할 수 있다[1].

스마트워크는 개인에게는 언제 어디서나 업무를 처리할 수 있어 편리성과 창의성을 제공하고 기업에게는 신속한 업무처리로 효율성 향상 및 비용절감을 제공하여 정부기관과 여러 기업에서 도입을 검토하고 있다. 또 스마트폰, 태블릿PC와 같은 모바일 디바이스의 보급이 급속히 확장되고, 그 성능도 기존의 데스크탑PC에 근접하여 모바일 디바이스를 이용하여 업무 수행이 가능할 정도로 발전함으로써 이를 중심으로 스마트워크 구축이 활발히 논의 되고 있다[2].

스마트워크는 기업이 관리할 수 있는 범위 밖에서 기업 내부망에 접근하여 업무를 처리한다. 따라서 기업은 구성원들이 기업 내부망 접근 시 이용하는 환경을 매번 조사하여 통제하기에는 무리가 있다. 이로 인해 기업 내부에서의 접근 시 보다 많은 보안 문제가 발생할 수 있다[3][4].

또 다른 문제는 스마트워크를 지원하기 위한 장소, 디바이스, 네트워크가 다양하다는 것이다. 이중 모바일 디바이스의 발전과 대중화는 이러한 환경이 더욱 다양해지는 계기가 되었다.

이처럼 스마트워크를 활용할 수 있는 디바이스와 접근 방법은 다양해 졌지만 기업들은 이러한 환경을 고려하지 않은 채 아이디/패스워드와 같은 사용자 중심 정보만으로 사용자의 권한을 부여하는 EAM 시스템을 사용하고 있다. 따라서 본 논문에서는 스마트워크의 각 유형별로 어떠한 디바이스와 네트워크가 이용되는지 알아보고 기존 EAM 시스템이 스마트워크의 다양한 환경에서 어떠한 한계가 있는지 살펴보고자 한다. 그리고 스마트워크 환경을 통해 내부망에 접근하는 각각의 특성을 구분하고 그 특성과 환경에 따라 차등적인 보안 등급을 설정하여 사용자의 권한을 동적으로 부여하는 방법을 제안한다.

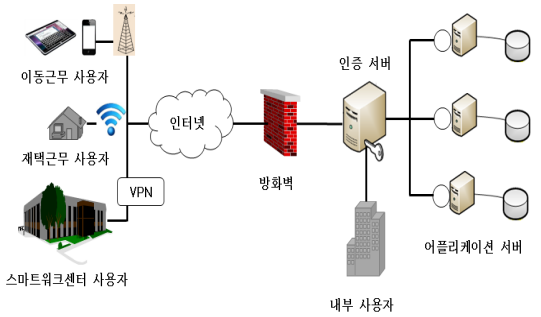
※ 본 연구는 지식경제부 및 한국인터넷진흥원의 "고용계약형 지식정보보안 석사과정 지원사업"의 연구결과로 수행되었음

2. 관련 연구

2.1 스마트워크 환경

2.1.1 스마트워크의 유형

스마트워크는 근무하는 장소의 성격에 따라 모바일 오피스, 재택근무, 스마트워크센터(SWC: Smartwork Center) 등으로 구분이 가능하다. 모바일 오피스는 휴대단말과 이동통신망을 이용하여 현장 중심의 업무 환경을 제공하는



(그림 1) 스마트워크 시스템 구성도

유형이다[5]. 재택근무는 개인PC나 필요 시설과 장비를 준비하여 사용자의 집에서 근무하는 유형이다. 스마트워크센터란 업무에 필요한 S/W와 보안이 강화된 전산망 등의 IT인프라와 독립된 공간, 책상, 회의실 등의 사무환경을 원래 근무지가 아닌 주거지와 가까운 곳에 설치해 놓은 근무 환경이다[6].

2.1.2 스마트워크를 지원하는 디바이스와 접근 방법

스마트워크를 지원하는 디바이스에는 태블릿PC, 스마트폰, 노트북, SBC(Server Based Computing), 개인PC 등이 있다. 또한 이러한 디바이스를 이용하여 기업의 내부망에 접근하는 방법에도 통신사의 3G/4G/Wibro, 공용 Wi-Fi, 가정의 인터넷망, 스마트워크센터에 구비된 VPN망 등 다양하다.

<표 1> 스마트워크의 다양한 환경과 특징

유형	디바이스	네트워크	특징
모바일 오피스	스마트폰 태블릿PC 노트북	3G/4G Wibro Wi-Fi	이동
재택근무	개인PC 태블릿PC	초고속 인터넷망	고정
스마트 워크센터	SWC 개인PC	VPN	고정

2.2 스마트워크의 보안 위협

접근 방법이 다양해진 만큼 스마트워크의 보안 위협도 매우 다양하다[7][8]. 스마트워크 지원 디바이스의 발전과

<표 2> 스마트워크의 다양한 보안 위협

유형	취약점
모바일 오피스	- 제3자의 훔쳐보기 - 단말기의 분실 위험 및 보안 관리 허술 - 네트워크의 노출로 중간자 가로채기 - 검증되지 않은 앱의 설치
재택근무	- 장비의 보안 관리 허술 - 네트워크의 노출로 중간자 가로채기 - 저장된 자료의 유출 가능성
스마트 워크센터	- 공용 사용으로 인한 악성 코드 감염 - 사용 단말에 업무의 흔적 저장

보급으로 기존PC 환경에서와 유사한 보안 위협도 발생하고 있지만 이와 동시에 각 특징에 따라 발생하는 보안 위협의 유형도 나타나고 있다[4].

모바일 오피스의 경우를 살펴보자. 모바일 오피스를 지원하는 디바이스는 휴대가 용이하다는 특징이 있는데 이는 기존의 고정된PC 환경과는 완전히 다른 특징이다. 때문에 디바이스 자체의 분실 및 도난의 위험이 크고 이에 따른 정보의 유출이 쉽다[9].

2.3 EAM 시스템과 한계

2.3.1 EAM

EAM 시스템이란 인트라넷/인터넷 및 일반 클라이언트/서버 환경에서 자원의 접근 인증과 이를 기반으로 자원에 대한 접근 권한을 부여·관리하는 아이디/패스워드 기반의 사용자 중심 통합 인증 관리 솔루션이다.

2.3.2 EAM 시스템의 한계

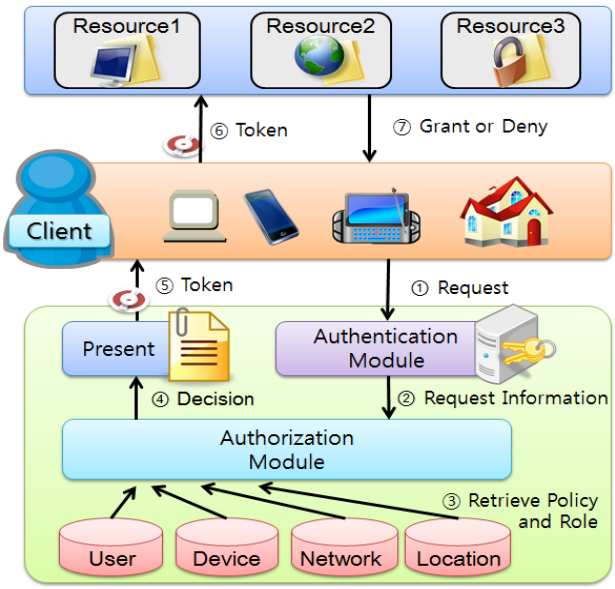
기존의 업무 환경에서는 사용자가 기업 내부망에 접근하기 위하여 이용하는 디바이스나 환경이 제한적이었기 때문에 사용자나 계정에 대한 권한을 미리 부여된 역할(role) 중심으로 부여하였다. 하지만 다양한 디바이스와 접근 방법이 존재하는 스마트워크 환경에서 각각의 특성과 보안 위협을 고려하지 않은 채 사용자나 정보 중심으로 권한을 부여하는 RBAC(Role Based Access Control)[10] 기반으로는 한계가 있다.

3. 제안 방식

3.1 시스템 구성

제안하고자 하는 접근 제어 방법은 기존의 사용자 정보를 활용한 접근 제어 방법에 추가적으로 디바이스, 네트워크, 위치정보를 활용하여 접근 환경을 구분하고 그 환경에 따라 사용자의 권한을 동적으로 생성하는 방법이다. 접근 제어의 결정은 허가된 정책에 의해 수행된다[11]. 따라서 권한 정책을 구성할 때 위에서 언급한 즉 동적으로 바뀔 수 있는 사용자의 접근 정보를 사용하는 것이다. 그리고 이를 바탕으로 사용자의 접근 상황에 따라 권한을 동적으로 만들고 할당 하는 것이다.

전체 적인 시스템 구성은 (그림 2)와 같다. 사용자는 먼저 특정 자원으로의 접근을 위해 아이디/패스워드, 공인인증서, i-PIN, OTP(One Time Password) 등과 같은 방법으로 사용자 인증을 실시한다. 인증에 성공하면 사용자는 자원을 사용하기 위해 권한 정보를 요청하게 되는데 이때 사용자가 자원에 접근할 때의 디바이스 정보, 네트워크 정보, 위치 정보를 권한 모듈로 함께 보내준다. 권한 모듈은 사용자로부터 전달 받은 접근 정보를 미리 정의 되어 있는 각 정책과 비교하여 조건에 맞는 권한을 추출한다. 이 과정을 통해 사용자 접근 환경에 맞는 사용자 권한이 새롭게 생성되며, 생성된 권한에 권한 생성 시간, 권한 유효 시간의 정보를 부가적으로 삽입하여 XML(eXtensible



(그림 2) 제안하는 시스템 흐름도

Markup Language)로 표현한 토큰(token) 형태로 부여한다. 이 후 사용자는 생성된 권한 정보가 들어 있는 토큰을 가지고 접근 가능한 내부 자원에 접근하게 된다.

3.2 접근 정보에 따른 정책 정의

권한 정책은 접근 정보별로 구분하여 미리 정책서버에 정의 한다. 또한 각 환경의 정책서버는 보안 위협수준에 따라 사용가능한 역할을 정의하고 있으며 U_Level 테이블 <표 4>, D_Level 테이블 <표 5>, N_Level 테이블 <표 6>, L_Level 테이블 <표 7>로 예를 들었다. 각 환경에서는 종류별로 보안 레벨을 부여하였으며 자원에 대하여 이용할 수 있는 권한은 Resource Action으로 정의 하였다.

3.3 사용 권한 생성

3.3.1 사용자 접근 정보 전달

사용자 접근 권한은 사용자가 자원 접근 시의 정보를 바탕으로 구분하여 생성된다. 이를 위해 사용자는 자원에 대한 권한의 요청 시 기존의 사용자 정보뿐만 아니라 디바이스, 네트워크, 위치 정보를 함께 보낸다.

3.3.2 접근 정보별 역할 추출 및 권한 생성

권한 모듈은 특정 자원에 대한 사용 요청이 발생하면 전달받은 사용자의 접근 정보를 가지고 정책서버에서 보안 수준에 맞는 역할을 추출한다. 이러한 방법으로 추출된 역할정보는 각각의 정책서버에서 추출한 역할정보와 비교하여 최종적으로 사용자의 접근 환경에 따라 사용가능한 권한을 생성한다(그림 3).

예를 들어 user4의 사용자가 아이폰을 가지고 3G망을 통해 이동 중에 특정 자원R의 사용을 요청하였다고 가정하자. 그럼 권한 모듈은 사용자 정보인 user4, 디바이스 정보인 아이폰, 네트워크인 정보인 3G, 이동중인 위치정보를

<표 3> 활용 하는 접근 정보

정보	종류
사용자	아이디/패스워드, 공인인증서, OTP 등
디바이스	OS, 브라우저, 프로그램 목록 등
네트워크	3G, Wi-Fi, VPN, 내부망 등
위치	IP, GPS/GIS 등

<표 4> 사용자 정보에 따른 역할 정의 예(U_Level)

보안 레벨	구 분	Resource Action
U_Level_1	user1	a1, a2, a3, a4, a5
U_Level_2	user2, user7	a1, a2, a3, a5
U_Level_3	user3, user6	a1, a3, a4
U_Level_4	user4, user5	a1, a2, a6

<표 5> 디바이스 정보에 따른 역할 정의 예(D_Level)

보안 레벨	구 분	Resource Action
D_Level_1	PC	a1, a2, a3, a4, a5, a6
D_Level_2	SBC	a1, a2, a3, a4
D_Level_3	아이폰	a1, a3, a5, a6
D_Level_4	갤럭시	a1, a5, a6

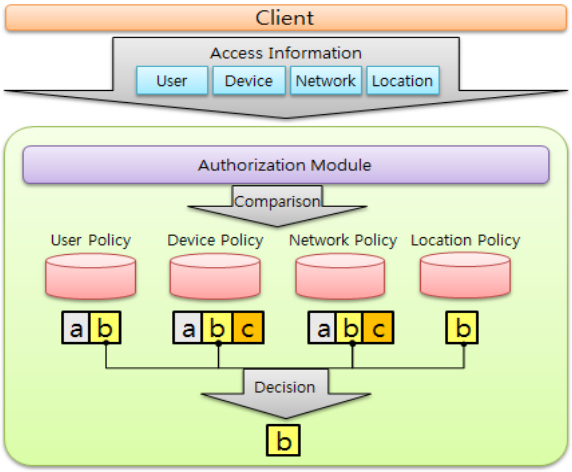
<표 6> 네트워크 정보에 따른 역할 정의 예(N_Level)

보안 레벨	구 분	Resource Action
N_Level_1	내부망	a1, a2, a3, a4, a5, a6
N_Level_2	VPN	a1, a3, a4, a5
N_Level_3	3G	a1, a2, a3, a6
N_Level_4	Wi-Fi	a1, a2, a3

<표 7> 위치 정보에 따른 역할 정의 예(L_Level)

보안 레벨	구 분	Resource Action
L_Level_1	내부	a1, a2, a3, a4, a5, a6
L_Level_2	SWC	a1, a3, a5
L_Level_3	가정	a1, a3, a4, a6
L_Level_4	이동중	a1, a5, a6

가지고 위의 <표 4>, <표 5>, <표 6>, <표 7>에 정의되어 있는 각각의 정책과 비교한다. <표 4>의 U_Level 테이블에서는 user4에에 부여된 Resource Action a1, a2, a6을 추출하고, <표 5>의 D_Level 테이블에서 아이폰의 a1, a3, a5, a6을 <표 6>의 N_Level 테이블에서 3G망의 a1, a2, a3, a6을 <표 7>의 L_Level 테이블에서 a1, a5, a6을 추출하여 비교한다. 그 후 모든 환경에서의 조건을 만족하는 a1, a6에 해당하는 역할이 주어지게 된다.



(그림 3) 접근 정보에 따른 역할 추출

3.4 사용자의 권한 동적 표현

생성된 역할은 사용자에게 전달하기 위해 토큰의 형태로 표현한다. 구성 정보는 다음의 <표 8>과 같다. 먼저 자원 공급자의 정보가 들어가며 자원을 요청하고 사용하려는 사용자의 정보, 사용자가 요구한 자원의 정보, 사용자의 접근 정보를 바탕으로 동적으로 생성된 권한 정보, 권한이 생성된 시간 정보 및 생성된 권한의 유효시간을 토큰에 담는다. 이러한 정보를 바탕으로 구성된 토큰은 XML 형식에 맞춰 구현하고 사용자에게 전달되도록 한다.

<표 8> 토큰 구성 및 표현

구성 정보	XML 표현
자원 공급자	<ResourceAccessPolicy> <Provider> provider </Provider> <User> id </User> <Authority> resource </Authority> <Permission> action </Permission> <Time> date+hh:mm </Time> <Validation> time+α </Validation> </ResourceAccessPolicy>
사용자	
요청 권한	
생성된 권한	
권한 생성 시간	
권한 유효 시간	

이렇게 생성되어 사용자에 부여된 권한은 기존의 사용자 정보를 바탕으로 고정적으로 생성되는 권한과는 달리 동적으로 생성되는 것을 볼 수 있다. 본 논문에서 제안된 방법은 사용자가 자원에 대한 접근 시마다 사용자의 접근 정보를 확인하고, 그 후 저장 되어 있는 정책과 비교 하여 해당 자원에 대한 권한을 새롭게 생성하기 때문이다. 따라서 동일한 사용자라 할지라도 그 접근 환경에 맞게 부여되는 권한의 내용이 바뀔 수 있다.

4. 결론

현재 EAM 시스템은 기존의 사용자 중심 정보만을 이용하여 자원에 대한 권한을 부여 하였다. 이에 본 연구에서는 다양한 환경에 대응하고자 스마트워크를 지원하는 접근 장소, 디바이스, 접근 방법 별로 추가적인 정책을 부여하여 접근 권한을 생성하는 방식을 제안하였다. 동일 사용자라 할지라도 접근 정보에 따라 기업 내부 자원에 접근하는 권한을 다르게 하여 기존의 사용자 정보 중심의 권한 부여 방식에 비해 기업 내 자원에 대해 불필요한 접근을 최소화 하였다. 또 제안된 방법은 자원을 관리하는 기업 입장에서도 미리 접근 환경에 대한 정책을 설정해 놓으면 기업 구성원들의 다양한 접근 방법에 일일이 대응할 필요가 없도록 설계하였다.

그러나 제안된 방법은 사용자 정보 중심 접근 시 보다 많은 정보를 필요로 하므로 사용자 측으로부터 효과적으로 정보를 가져오는 설계가 필요하다. 또 필요 정보를 수집 시 사용자의 사생활 정보가 담겨 있을 수 있어 개인정보보호 범위에 위반 되지 않도록 설계 하는 방안도 필요하다. 사용자 정보와 디바이스 정보, 네트워크 정보, 위치 정보를 이용하여 동적으로 생성된 토큰은 사용자에게 안전하게 전달 및 사용되어야 한다. 이를 위해 토큰의 전송 시 암호화를 적용하여 토큰이 사용자에 전달되는 과정 또는 부여 받은 토큰을 사용자가 사용하는 과정 속에서 악의적인 공격자로부터 유출되지 않도록 설계가 필요하다.

참고문헌

[1] 이재성, 김홍식, “스마트워크 현황과 활성화 방안 연구”, 한국지역정보화학회지, 제13권 제4호, pp.75-96, 2010.

[2] 이형찬, 이정현, 손기욱, “스마트워크 보안 위협과 대책”, 정보보호학회지, 제21권 제3호, pp.12-21, 2011.

[3] 정명수, 이동범, 곽진, “스마트워크 보안위협 및 보안요구사항 분석”, 정보보호학회지, 제21권 제3호, pp.55-63, 2011.

[4] 황해수, 이기혁, “안전한 스마트워크 향상을 위한 Mobile Security 대응모델에 관한 연구”, 정보보호학회지, 제21권 제3호, 2011.

[5] 김평중, “스마트워크 서비스 플랫폼과 활용”, 한국정보처리학회, 제18권 제2호, pp.73-81, 2011.

[6] 행정안전부, 스마트워크센타, http://www.smartwork.go.kr

[7] 나종회, 최영진, 신동익, “스마트워크 환경에서의 보안 위협에 관한 탐색적 연구”, 정보기술아키텍처연구, 제9권, 제1호, pp33-42, 2012.

[8] 이동범, 곽진, “스마트워크 보안 아키텍처 연구”, 한국정보처리학회 제18권 제1호, 2011.

[9] 이경복, 박태형, 임종인, “스마트워크 환경 변화에 따른 보안위협과 대응방안”, 디지털정책연구, 제9권 제4호, pp.29-40, 2011.

[10] Ravi Sandhu, Edward J.Coyne, Hal L, Feinstein, Charles E. Youman, “Role-Based Access Control Models”, IEEE Computer 29, No.2, pp.38-47, Feb. 1996.

[11] David W. Chadwick, Alexander Otenko, “The PERMIS X.509 role based privilege management infrastructure”, Future Generation Computer Systems, 19, pp.277-289, 2003.