http://dx.doi.org/10.5392/JKCA.2015.15.05.027

BYOD환경에서 키 생성 및 접근 제어 프로토콜에 관한 연구

A Study for Key Generation and Access Control Protocol in BYOD Environments

민소연*, 진병욱, 이광형***, 이근왕******

서일대학교 정보통신학과*, 숭실대학교 컴퓨터학과**, 서일대학교 인터넷정보학과***,
청운대학교 멀티미디어학과****

So-Yeon Min(symin@seoil.ac.kr)*, Byung-Wook Jin(quddnr4511@naver.com)**,
Kwang-Hyoung Lee(dreamace@seoil.ac.kr)***, Keun-Wang Lee(kwlee@chungwoon.ac.kr)****

요약

스마트 기기 사용자의 증가와 통신 기술 발전으로 시간과 장소에 제약 없이 업무환경에 대한 영역이 확대되고 있다. 사용자 개인의 장비를 활용하여 업무에 도입되어지고 있으며, 이를 BYOD(Bring Your On Device)라고 한다. 하지만 기존의 무선 환경에서 발생하고 있는 보안위협에 취약하며, 기업 내부에 의한 중요 정보 유출, 사용자 부주의로 인한 단말기 분실/도난 등으로 인하여 보안취약점이 이슈화 되고 있다. 그러므로 본 논문에서는 BYOD환경에서 사용자 정보 기반으로 세션 키를 생성하여 사용자 권한에 따른 접근 제어 프로토콜에 관하여 연구하였다. 사용자 정보 및 사용자 기기 정보를 기반으로 세션 키를 생성하였으며, 이후 접근제어 프로토콜을 설계하였다. 제안하는 프로토콜은 BYOD 환경 및 무선 랜 환경에서 발생할 수 있는 공격으로부터 보호할 수 있고, 사용자 권한을 관리하여 기업 내부의 중요 콘텐츠 유출로부터 보안 요구사항과 안전성을 강화하였다.

■ 중심어 : | BYOD | 접근제어 | 인증 |

Abstract

Depending on the smart device user growth and development of communication technology, the area about working environment was extended without constraints of time and places. It is introducing to work using user's devices and this environment is called 'BYOD(Bring Your On Device)'. But it is vulnerable to security threat that happened in existing wireless environment and its security threat issue which is caused by inside information leak by an inside job and lost or stolen terminal which is caused by careless user is getting heated. So we studied about access control protocol by user rights under the BYOD situation make a session key based on the user information. We make a session key based on the user information and user device information, after that we design an access control protocol. The protocol we suggest can protect from attack under the BYOD situation and wireless communication situation and also safety and security requirement from inside information leak because it controls user rights.

■ keyword : | BYOD | Access Control | Authentication |

접수일자 : 2015년 01월 29일
수정일자 : 2015년 03월 05일
심사완료일 : 2015년 03월 09일
교신저자 : 이광형, e-mail : dreamace@seoil.ac.kr

I. 서 론

스마트 기기 사용자의 지속적인 증가와 모바일 오피스 확산으로 시공간 제약 없이 근무하는 환경으로 빠르게 발전하고 있다. 사무실에서 업무를 처리했던 과거와는 달리 자택, 커피숍, 열자, 버스 등 시간과 장소를 구애받지 않으며 언제 어디서나 업무를 처리할 수 있는 장점이 있다[1]. 이러한 개념을 BYOD(Bring Your Owen Device)라는 개념으로서 새로운 근무환경을 제공해주고 있다. BYOD는 사용자가 소유한 기기를 장소 상관없이 기업 업무에 활용할 수 있으며, 업무적으로 효율성을 높이고 있으며, 기기 구매에 대한 비용적인 측면에서 절감적인 효과를 나타내고 있다[2][4].

하지만 사용자 기기들이 기업 내부의 중요 콘텐츠를 접근함으로써 기밀정보유출, 악성코드 감염, 개인정보 유출등과 같은 보안 문제가 발생하고 있다. 또한 사용자 소유의 장비는 도난 및 분실과 낮은 보안성 등으로 인하여 악의적인 사용자의 위협으로 안전할 수 없다. BYOD의 특성상 다양한 장비를 통하여 기업 내부의 콘텐츠를 접근할 수 있는 환경이 존재하므로 사용자권한에 알맞은 안전한 접근통제방식이 요구되고 있다[3][5]. 본 논문에서는 사용자의 특성 및 정보를 활용하여 접근 제어 프로토콜에 관하여 연구하였다. 사용자 정보를 기반으로 세션 키를 생성하고, 이를 기반으로 콘텐츠의 정보와 사용자의 정보의 비교분석 작업을 통하여 데이터 통신을 수행한다.

2장에서는 BYOD의 정의 및 특징, BYOD 환경 주요 접근 제어 솔루션, 모바일 오피스 환경의 보안 요구사항에 대하여 서술하였으며, 3장에서는 사용자 등록 및 키 생성, 사용자 인증 및 데이터통신 프로토콜을 설계하였다. 그리고 4장에서는 제안된 프로토콜에 관하여 기존 시스템과의 비교 및 안전성에 관하여 분석하였으며, 마지막으로 결론에서는 본 논문에서 제안된 프로토콜의 향후 연구 방향에 관하여 논의하였다.

II. 관련연구

1. BYOD(Bring Your Own Device)

1.1 BYOD 정의 및 특징

스마트폰의 발전으로 모바일 산업은 기하급수적으로 발전하고 있으며, 기존 무선 네트워크 통신기술이 점차적으로 확산되는 추세이다. 스마트 디바이스를 적극적으로 활용하기 위해 사용자 소유의 스마트폰, 태블릿 PC, 노트북과 같은 장비를 업무환경에 알맞게 활용되고 있다. 이러한 환경을 스마트 오피스 BYOD라 정의되고 있다[3].

사용자 장비를 활용하여 비공식적(private) 및 개인적인(personal) 구분 없이 업무에 활용하여 사내입장에서도 효율적으로 진행할 수 있다는 점이 BYOD 환경의 장점이라 할 수 있다. 또한 사용자의 장비를 활용하여 회사 및 기업업무에 즉시 투입되는 추세로 새로운 업무 프로세스 환경으로 구축되고 있다. 하지만 개인 소유의 장비를 활용하여 회사 및 기업 내부의 콘텐츠 유출 및 허술한 내규정책으로 문제점이 발생할 수 있으며 기존의 무선통신방식에 보안위협이 계승함으로써 보안정책 및 안전성에 대한 보안설계가 요구되고 있다. 따라서 안전한 BYOD 환경을 구축하기 위해서는 사용자 인증, 사용자 장비에 대한 강력한 등록 절차, 분실에 대한 모바일 기기 관리(MDM: Mobile Device Management) 기능 구현체계가 요구되어 지고 있으며 관리에 대한 강력한 조치와 통제 정책이 필요하다. 또한, 유・무선 인프라에 대한 점검이 지속적으로 이루어져서 안전한 네트워크 구현 및 모니터링을 요구하고 있다[4][5].

1.2 BYOD 환경 주요 접근 제어 솔루션

NAC (Network Access Control) 솔루션

NAC(네트워크 접근 제어) 솔루션은 종단 대 종단간의 프로토콜을 사용하여 기존의 내부 망에 접근 시도 후 내부망에 접속하는 솔루션이라 할 수 있다. 또한 보안 정책을 적용하여 네트워크 접근을 제어하고 통제한다.

MDM (Mobile Device Management) 솔루션

스마트 기기의 사용자가 늘어나면서 기업 및 공공기관에서 사용자의 스마트 기기를 지원하도록 하는 추세이다. 다종의 다양한 기기를 허용하는 효율적으로 관리해주는 솔루션이라 할 수 있다. 주요기능으로는 다양한 OS 디바이스 지원, 애플리케이션 관리, 보안관리, 자산

관리, 디바이스 분실 등이 있다.

MAM (Mobile Application Management) 솔루션

- 기업 및 공공기관에서 애플리케이션을 설계 및 구현하여 직원들에게 배포 후 애플리케이션을 활용하여 각종 관리 기능을 지원하고 보안기능을 강화하는 솔루션이라 할 수 있다. 모바일 단말에 설치된 애플리케이션과 데이터를 관리할 수 있다는 장점이 있다[4][5].

2. 모바일 오피스 보안 요구사항

2.1 모바일 단말기 보안 위협

모바일 단말기의 휴대성으로 인한 특정한 사용자의 관리적인 측면에서 부주의로 인하여 도난·분실에 대한 위협이 존재한다. 스마트폰은 개인적인 측면에서 통화내역, (SMS : Short Message Service), 메신저, 연락처, 개인일정 등과 같은 정보와 업무적인 측면에서는 회사의 기밀·업무정보를 저장하고 있으므로 도난 또는 분실될 경우 정보유출을 대한 피해가 심각하다.

악의적인 사용자가 스마트폰을 습득하면, 스마트폰 내에 개인정보 및 업무정보를 정보유출, 위·변조와 같은 행위가 가능하다. 그러므로 스마트폰에 도난·분실적인 측면에서 사용자 인증, 접근제어와 같은 보안취약점이 발생하므로 사용자 접근에 대한 보안기술 및 정책이 요구되어지고 있다[8][9].

2.2 무선 네트워크 보안 위협

모바일 단말기는 이동통신망, (WLAN:Wireless Local Area Network) 및 Bluetooth를 활용하여 데이터 통신을 하고 있어 기존의 무선 환경에서 발생할 수 있는 보안 위협을 계승하고 있다. 대표적인 예로는 사용자가 무선데이터의 요금을 절약하기 위해 Wi-Fi(Wireless Fidelity)를 활용하여 후 통신하는 사례를 볼 수 있다. Wi-Fi는 무선공유기(AP: Access Point)를 이용하여 사용하는데 악의적인 의도를 가진 사용자가 악성코드를 집어넣고 접속을 유도하여 악성코드 유 및 해킹공격을 취할 수 있다. 또한 모바일 단말기(스마트폰, 태블릿 PC)와 PC의 취약점을 이용하여 수집한 사례가 있으며, 악의적인 사용자가 위장한 AP를 통한 개인·중요정보 유출사례가 꾸준히 발생하고 있다.

3. 접근 제어 및 키 생성 프로토콜에 관한 연구

강제적 접근제어(MAC : Mandatory Access Control)은 사용자가 원하는 네트워크 또는 콘텐츠에 접근할 때 상호간에 보안 등급을 참고하는 방식으로 정보에 접근을 제한하는 방법이다. 네트워크의 객체를 추상화하고 그 객체를 사용하고자 하는 사용자, 장비를 설정 후 각 주체의 허가 등급을 부여한다. 이후 주체가 객체에 관하여 접근하고자할 때 권한을 확인하는 방식이다. 또한 임의적 접근 제어(DAC : Discretionary Access Control) 방식은 접근 제어 정책으로 객체에 대한 접근을 사용자 개인 또는 그룹의 식별자를 기반으로 하는 접근 제어 방식이다. 접근 권한을 가지는 관리자가 판단에 따라 사용자에게 권한을 부여할 수 있다. 사용자의 위치, 직위, 수행하는 일에 따라서 접근권한 등급을 부여하여 제어하도록 하는 방식이다. 마지막으로 디피-헬만 키 교환 프로토콜(Diffie - Hellman key exchange) 방식을 활용하여 상호간의 비밀키를 공유하는 방식이 있다. 키 교환 방식의 하나로 공개키 알고리즘과 대칭키 알고리즘의 장점을 살려 두 가지 형태의 알고리즘을 결합한 알고리즘으로서 많이 쓰이고 있다. 하지만 중간자 공격에 취약한 것으로 판명되어 이를 보완하기 위한 여러 연구가 진행되고 있으며 키 분배 관리, 디피-헬만 기반의 세션 키 생성 알고리즘이 활용되고 있다. 위에서 언급했던 기술은 공공기관이나 기업의 서로 다른 보안 요구사항들과 정책 요구를 만족시킬 수 없으므로 BYOD 환경을 위협하는 보안위협 및 취약점이 발생할 수 있다[9-11].

III. 제안 시스템

1. 제안시스템 구성도

본 논문에서 제안하는 시스템 구성도는 [그림 1]과 같다. 사용자 도메인, 사내 네트워크, 서버 도메인으로 나누어져 있다. 제안 시스템 시나리오는 사용자가 자신의 장비(노트북, 스마트폰, 태블릿 PC 등)을 가지고 유・무선 네트워크를 통하여 사내 네트워크에 접속하여 사용자 등록 및 사용자 등급에 알맞은 세션 키를 생

성 받는다. 이 후 사용자의 정보와 세션 키를 활용하여 인증을 완료 후 사용자 등급에 알맞은 콘텐츠에 접근하여 데이터를 통신하는 방식이다.

본 논문의 가상 사항은 다음과 같다.

- 서버 도메인(Server Domain)의 (KGS: Key Generation Server)는 사용자 등급을 검사 후 이를 기반으로 세션 키를 생성할 수 있다.
- 사용자 장비는 악성코드 및 바이러스로부터 감염되지 않는 안전한 장비이고 애플리케이션에 비밀번호가 설정되어 있어야 한다.
- 서버 도메인의 (CMS: Content Management Server)는 콘텐츠를 저장할 때 사용자 등급에 따른 값(Value)을 저장한다.
- 사용자 기기는 사용자 등록 후 비밀번호(PASSWORD)가 3회 이상 틀리면 자동으로 $User_{Cert}$, $Device_{Info}$, SK_{User} 값이 삭제되도록 설계되어야 한다.

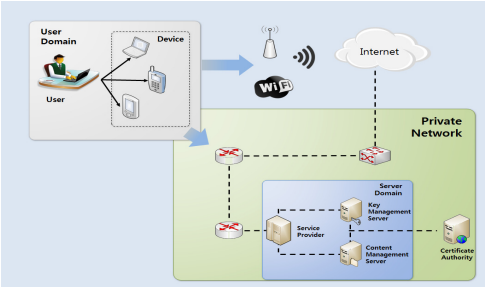

그림 1. 제안 시스템 구성도

표 1. 약어표

Abbreviations	Full Name
EKPUB_XX	Encrypted with the public key of xx
EKPRI_XX	Encrypted with the private key of xx
PAD	Padding Value
TIMESTAMP	String that represents a Particular time
SP	Service Provider
KGS	Key Generation Server
CA	Certificate Authority
CMS	Content Management Server
DeviceSN	Device`s Serial Number
USERINFO	User`s Information
UDValue	User serial number and Timestamp of the XOR operation value
USERCert	User Certification Value
USERSK	User`s Session Key
USERLevel	User Authority Level
ContentLevel	Content Authority Level

2. 제안시스템 설계

2.1 사용자 등록 및 키 생성

BYOD환경에서 사용자 등록 및 키 생성을 설계하는 단계이다. 우선 사용자는 1차적으로 사용자의 정보를 확인 후, 2차적으로 사용자의 장비를 등록한다. 송신된 Value를 기반으로 사용자와 (SP: Service Provider)간의 $User_{SK}$를 생성 후 USER로 발송하는 것을 마무리한다. 상세프로토콜은 [그림 2]와 같다.

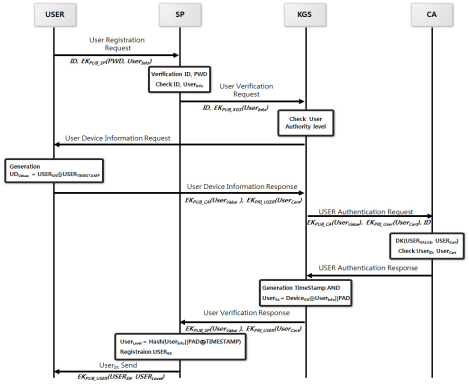

그림 2. 사용자 등록 및 키 생성 프로토콜

1) 사용자 등록 요청

사용자는 BYOD환경의 Private Network에 접속하기 위해서 SP로부터 사용자 등록 요청 메시지를 발송한다. 사용자의 ID와 SP의 공개키로 암호화된 PWD, 사용자 정보를 발송한다.

$$ID, EK_{PUB-SP}(PWD, User_{Info}) \quad (1)$$

2) 사용자 검증 요청

SP는 송신 받은 메시지 값의 ID, PWD를 검증하고 ID, $User_{Info}$를 검사한다. 이후 ID와 KGS의 공개키로 이용하여 $User_{Info}$를 암호화를 수행한 후 KGS로 발송한다.

$$ID, EK_{PUB-KGS}(User_{Info}) \quad (2)$$

3) 사용자 장비정보 요청

KGS는 사용자의 권한등급을 확인 후 사용자로부터

Private Network에서 사용하는 장비의 요청 메시지를 전송한다.

4) 사용자 장비요청 메시지 응답

사용자는 사용자의 장비 값을 생성 후, 사용자의 장비 값과 타임스탬프는 CA의 공개키로 암호화, 사용자 인증 값은 사용자의 개인키로 암호화하여 사용자 장비 정보 응답 메시지를 전송한다.

$$UD_{Value} = USER_{SN} \oplus USER_{Time\,stamp} \quad (3)$$

$$EK_{PUB-CA}(User_{Value}), EK_{PRI-User}(User_{Cert}) \quad (4)$$

5) 사용자 인증 요청 및 응답

KAS는 사용자로부터 송신 받은 메시지를 (CA: Certificate Authority)로 전송하여 사용자 검증을 위한 메시지를 전송한다. CA는 사용자의 정보와 사용자 공인인증서의 서명 값을 확인 후 KAS로 응답 메시지를 전송한다.

$$DK(User_{Value}, User_{Cert}) \quad (5)$$

6) 세션 키 생성

KGS는 사용자등급에 알맞은 세션 키와 타임스탬프를 생성 후 SP로 세션 키 값을 SP로 전송한다. 세션 키는 다음과 같다.

$$User_{SK} = Device_{SN} \oplus USER_{Info} \| PAD \quad (6)$$

$$EK_{PUB-Sp}(User_{Value}, Time\,Stamp), \quad (7)$$
$$EK_{PRI-User}(User_{Cert})$$

7) 세션 키 등록

SP는 KGS로 송신 받은 세션 키와 사용자 정보 값을 저장한다. 이때 사용자 등급이라는 값을 생성하여 등록하도록 한다. 등록을 마친 후 사용자로 세션 키를 발송한다.

$$User_{Level} = Hash(User_{Info} \| PAD \oplus Time\,Stamp) \quad (8)$$

$$EK_{PUB}(USER_{SK}, USER_{Level}) \quad (9)$$

2.2 사용자 인증 및 데이터 통신

사용자가 Device를 이용하여 로그인 후 인증하는 단계 및 콘텐츠에 접근하여 데이터를 통신하는 단계이다. 사용자 로그인이 완료되면 사용자는 콘텐츠에 접근하여 콘텐츠정보와 사용자 권한등급을 분석하여 사용자에게 접근할 수 있는 콘텐츠인지 확인 후 데이터를 통신하는 방식을 설계하였다. BYOD환경에서 내부자의 악의적인 행동에 의한 콘텐츠 접근 및 유출에 대한 안정성을 확보하였으며, 상세 프로토콜은 [그림 3]과 같다.

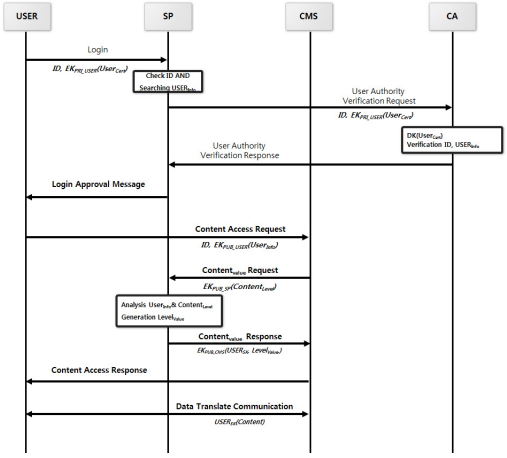

그림 3. 사용자 인증 및 데이터 통신

1) 로그인

사용자는 SP로 로그인을 요청한다. 로그인 사용자의 ID와 사용자의 개인키로 암호화를 수행한 인증 값을 첨부하여 포함하여 로그인을 요청한다.

$$ID, EK_{PRI}(User_{Cert}) \quad (10)$$

2) 사용자 권한 검증 요청

SP는 사용자로부터 로그인을 요청받은 후 ID, $User_{Info}$를 분석 후 CA로 사용자 권한 검증 메시지를 요청한다.

$$ID, EK_{PRI-User}(User_{Cert}) \quad (11)$$

3) 사용자 검증 응답 및 로그인 승인 완료

CA는 사용자ID 검증 및 정보를 검증 후 SP로 사용자 검증 응답 메시지를 전송한다. 그리고 사용자로부터 로그인 메시지를 전송한다.

4) 콘텐츠 접근 요청

사용자는 ID와 자신의 공개키로 사용자 정보를 암호화하여 CMS로 콘텐츠 접근 요청 메시지를 전송한다.

5) 콘텐츠 값 송신 및 $Level_{value}$ 생성

CMS는 사용자가 접근하는 $Content_{Level}$을 SP의 공개키로 암호화 하여 SP로 송신한다. 이후 SP는 $USER_{Info}$와 $Content_{Level}$을 분석 후 $Level_{Value}$를 생성한다.

6) $Level_{value}$ 전달 및 콘텐츠 접근

SP는 CMS의 공개키로 $USER_{SK}$와 $Level_{Value}$를 암호화 후 CMS로 콘텐츠 Value 메시지를 발송한다. CMS는 콘텐츠 접근 응답 메시지를 USER로 발송 후 $USER_{SK}$를 이용하여 암호화 후 콘텐츠를 통신한다.

IV. 기존 시스템과의 비교분석

1. 보안성 분석

본 절에서는 BYOD환경의 보안 위협에 관하여 보안성을 분석하였다. TTA 표준자료인 기업 무선 랜 환경에서 위협 장치를 위한 보안 기능 요구 사항을 참고하였으며, 표준에서 대표적으로 언급된 사용자/시스템 인증 기능, 안전한 정보 전달 기능, 보안 정보 공유 기능에 관하여 분석하였다. 그 밖에도 기존 시스템에서도 제공했던 기밀성, 무결성, 안전성, 부인방지에 관하여 설계되었다. 사용자/시스템 인증기능에서는 TTA 표준 요구사항 UAR(User/System Authentication function Requirement)요구사항에서 3, 4, 5, 6, 7, 8, 9 항목에 해당하는 부분을 만족하며 사용자의 권한관리 보안하였다. 그리고 안전한 정보 전달 기능에서 SDR(Secure Information Delivery functional Requirement)요구사항에서 1, 2, 3, 4 항목에 해당하는 부분을 만족하였으며 콘텐츠 보호 접근 통제부분에 보안성을 강화하기 위해서 설계되었다. 마지막으로 보안 정보공유 부분에서는 ISR(Security Information Sharing function Requirement) 요구사항 2, 4항목에 해당하는 부분을 만족 후 사용자 및 디바이스 정보 관리를 강화하였다. 아래 표는 기존 시스템(기업의 무선 랜 환경)과 제안 시스템의 보안성에 관하여 비교분석하였다.

표 2. 기존 시스템과 제안시스템의 보안성 분석

Separate	Exist System	Proposed System
Confidentiality	O	O
Integrity	O	O
Safety	O	O
Repudiation	O	O
UAR Requirement (User Authority Management)		O
SDR Requirement (Content Protection)		O
ISR Requirement (Personal Information Management)		O

아래의 그림은 Eclipse환경에서 Java Library를 활용하여 콘텐츠 암호화를 성능비교를 하였다. 기존의 시스템의 콘텐츠 암호화 방식인 (AES, SEED, RC5)와 본 논문에서 제안한 세션 키 방식의 수행속도를 비교한 결과는 [그림 4]와 같다.

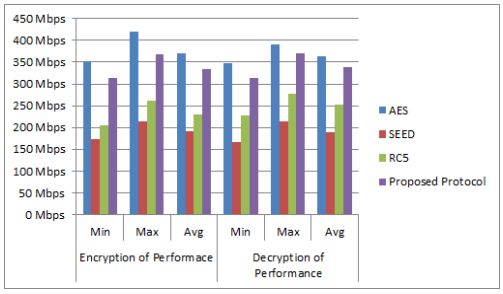

그림 4. 기존시스템과 제안시스템의 암호성능 비교

제안 프로토콜에서는 기존 시스템에서 수행하고 있는 AES보다는 속도가 느리지만, 사용자와 장비의 정보

를 활용하여 세션 키를 생성함으로서 기존 무선 환경에서 발생하는 중간자 공격, 재생 공격에 관하여 안전하다. 또한 기업 무선 랜 환경에서 위협 장지를 위한 보안 기능 요구 사항을 적용함으로써 보안성을 강화하였다.

2. 안전성 분석

제안된 프로토콜의 안전성을 평가하기 위해 BYOD 환경과 기존의 기업 무선 랜 환경에서 발생하는 공격기법에 관한 안전성을 분석하였다. 각각의 공격기법의 시나리오를 분석하여 그에 해당하는 공격으로부터 안전성에 대하서 분석하였다.

가장공격(Impersonation Attack) : 악의적인 사용자가 사용자 정보를 이용하여 올바른 사용자로서 위장하는 공격기법으로 사용자 등록 프로토콜에서 사용자의 $User_{Info}$와 $User_{Cert}$를 검증함으로써 사용자의 진위여부를 확인한다. 또한 사용자의 $User_{Info}$와 $Device_{Info}$를 활용하여 사용자 권한에 알맞은 등급을 분석함으로써 가장공격은 실패한다.

재생공격(Replay Attack) : 공격자가 사용자의 통신내용을 가로채어 다시 네트워크 도메인의 SP, KMS, CMS로 다시 전송하는 공격기법이다. 본 논문의 제안된 프로토콜에서는 사용자 등록과정 중 TimeStamp를 활용하여 인증함으로써 재생공격이 어렵다. 이후 사용자 인증 과정 중에 악의적인 사용자가 로그인을 성공했다는 가정 하에 콘텐츠 접근에서는 TimeStamp, $User_{Cert}$, $Device_{Info}$를 활용한 세션 키를 암·복호화하여 데이터 통신을 수행함으로써 콘텐츠 접근이 실패한다.

중간자공격(In Middle in Attack) : SP로 위장하여 사용자의 정보를 탈취 공격하는 기법이다. 사용자의 개인키 값을 알아야하며 사용자의 KMS, CMS의 개인키 값을 가지고 있어야 위장이 가능하므로 중간자 공격을 할 수 없다.

피싱공격(Fishing attack) : 사용자 입장에서 정상적인 SP로 위조하여 접속을 유도하는 공격기법이다. 사용자 등록과정에서 KAS, CA와의 SP간의 비 대칭키 암호화방식으로 통신 후 단계적으로 검증하고 있다. 또한 KAS에서 세션 키를 생성 후 이를 기반으로 암·복호화를 수행하고 있으므로 피싱공격에 대한 공격을 막을 수 있다.

내부자에 의한 정보유출(Information outflow by insider) : 내부자에 의한 정보유출은 기업의 사내 네트워크(Private Network)에서 많이 발생하는 사례이며, 본 논문에서는 사용자 및 콘텐츠 등급에 관한 접근제어 시스템과 인증방식을 통하여 설계하였다. KAS에서 사용자 권한 에 알맞은 세션 키를 생성하고 CMS에서 콘텐츠 권한 관리 등급을 설정하여 이를 보완함으로서 내부자에 의한 콘텐츠 유출 대한 피해를 막을 수 있다.

V. 결론

본 논문에서는 BYOD환경에서 사용자 정보 및 기기 정보를 기반으로 세션 키를 생성 후 콘텐츠 접근제어 프로토콜에 관하여 연구하였다. 제안 프로토콜은 사용자등록 후 사용자 정보를 기반으로 세션 키를 생성하였으며, 기업 무선 랜 환경에서 Private Network Domain의 로그인을 수행하여 콘텐츠를 접근하도록 설계하였다.

사용자는 SP를 통하여 KMS에서 사용자 등급에 알맞은 세션 키를 발급 후 콘텐츠 통신과정에서는 CMS에서 저장된 콘텐츠 등급과 사용자 등급에 알맞은 콘텐츠를 비교분석 후 데이터 통신 프로토콜을 설계하였다.

성능평가부분에서 본 논문에서 제안한 프로토콜은 TTA 표준자료를 참고하여 기존의 있는 시스템에서 언급된 사용자 권한 관리, 콘텐츠 보호, 개인정보관리 등에 관하여 보안성을 분석하였다. 또한 기존 시스템에서 세션 키를 생성 수행방식을 비교하여 보안성을 강화하였으며, 기존 기업 무선 랜 환경에서 발생하는 가장공격, 재생공격, 중간자공격, 피싱공격, 내부자에 의한 정보유출 등과 같은 공격기법들에 관하여 안전성을 분석하였다.

제안한 시스템을 BYOD환경을 구축하고 있는 기관,

기업에서 적용하기 위해서는 사용자 권한에 따른 인증 기술뿐만 아니라 악성코드 탐지 및 분산 서비스 거부 공격(DDoS: Distributed Denial of Service)공격에 따른 보안기법에 관한연구가 요구되며, 각각의 기관 및 기업에서도 적용할 수 있는 보안 정책 수립이 필요하다.

참 고 문 헌

[1] 강동완, 오주형, 임채태, "BYOD 환경에서 기업정보보호를 위한 사내서비스 비정상접근/이용행위 탐지방법에 관한 연구", 한국통신학회종합학술발표회 논문집(추계), pp.771-772, 2013.

[2] 이재호, 이용진, 양승미, 금봉수, "공공부문에 BYOD기반 모바일 오피스 도입시 고려사항에 관한 연구", 한국통신학회종합학술발표회 논문집(하계), pp.856-857, 2013.

[3] 민소연, 진병욱, "U-Health환경에서 안전한 개인정보 관리를 위한 통합 인증스키마 설계", 한국산학기술학회 논문지, 제15권, 제6호, pp.3865-3871, 2014.

[4] 민소연, 장승재, "익명 게시판 환경에서 가상 아이디를 이용한 개인정보보호에 관한 연구", 한국산학기술학회 논문지, 제13권, 제9호, pp.4214-4223, 2012.

[5] 윤관식, *스마트워크 환경에 따른 접근 권한 제어 시스템 설계 및 구현*, 아주대학교 지식정보보안학과, 2013(2).

[6] A. Scarfòo, "New security perspectives around BYOD," in Proc. 7th Int. Conf. Broadband, Wireless Computing, Communication, Application(BWCCA), Victoria, Canada, pp.446-451, 2012(11).

[7] H.-S. Yoon, S.-B. Hong, H.-Y. Youm, and I.-J. Kim, "Mobile VPN architecture for smart work environment," Journal of Korean Institute of Information Technology, Vol.9, No.5, pp.59-166, 2011(5)(in Korean).

[8] L. Liu, R. Moulic, and D. Shea, "Cloud service portal for mobile device management," in Proc. IEEE 7th Int. Conf. e-Business Eng.(ICEBE), Shanghai, China, pp.474-478, 2010(11).

[9] K. W. Miller, "BYOD: Security and Privacy Considerations," IT Professional, Vol.14, No.5, pp.53-55, 2012(10).

[10] 이광형, 박정효, "개인정보보호를 위한 스마트카드 기반의 익명 인증 기법", 한국산학기술학회 논문지, 제13권, 제12호, pp.6071-6080, 2012.

[11] KISA, *안전한 모바일 오피스 도입과 운영을 위한 정보보호 수칙*, 2012(12).

[12] 남길현, 원동호, *정보시스템 보안론*, 2011.01.10.

[13] TTA, *기업 무선 랜 환경에서 위협 방지를 위한 보안 기능 요구사항*, 2012(12).

저 자 소 개

민 소 연(So-Yeon Min) 정회원

- 1994년 2월 : 숭실대학교 전자공학과(공학사)
- 1996년 2월 : 숭실대학교 전자공학과(공학석사)
- 2003년 2월 : 숭실대학교 전자공학과(공학박사)
- 2005년 3월 ~ 현재 : 서일대학교 정보통신과 부교수

<관심분야> : 통신 및 신호처리, 정보통신

진 병 욱(Byung-Wook Jin) 정회원

- 2010년 2월 : 청운대학교 멀티미디어학과(문학사)
- 2013년 2월 : 숭실대학교 컴퓨터학과(공학석사)
- 2013년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 박사수료

<관심분야> : 사물지능통신, 인증, 접근제어

이 광 형(Kwang-Hyoung Lee) 정회원

- 1998년 2월 : 광주대학교 컴퓨터공학과(공학사)
- 2002년 2월 : 숭실대학교 컴퓨터학과(공학석사)
- 2005년 2월 : 숭실대학교 컴퓨터학과(공학박사)
- 2005년 3월 ~ 현재 : 서일대학교 인터넷정보과 부교수

<관심분야> : 멀티미디어 데이터 검색, 영상처리, 멀티미디어 보안, USN, 학습콘텐츠

이 근 왕(Keun-Wang Lee) 정회원

- 1993년 2월 : 한밭대학교 전자계산학과(공학사)
- 1996년 2월 : 숭실대학교 컴퓨터학과(공학석사)
- 2000년 2월 : 숭실대학교 컴퓨터학과(공학박사)
- 2001년 3월 ~ 현재 : 청운대학교 멀티미디어학과 부교수

<관심분야> : 컴퓨터 통신, 멀티미디어 통신, 멀티미디어 응용