BYOD 환경에서 기업 내부 서비스 접근에 따른 상황 인식에 관한 연구

조창민, 강동완, 임채태
한국인터넷진흥원
e-mail:jocm1309@kisa.or.kr, lupin428@kisa.or.kr, chtim@kisa.or.kr

A Study on the Recognition of Context in BYOD Environment

Jo Chang Min, Kang Dong Wan, Im Chae Tae
Korea Internet & Security Agency

요 약

시간과 장소에 구애받지 않고 인터넷을 이용할 수 있는 환경이 보편화됨에 따라 BYOD 환경이 도입되면서 외부에서도 개인 단말기기를 통해 업무를 처리하는 모습을 어렵지 않게 볼 수 있다. 이처럼 BYOD는 점차 기업 문화의 한 트렌드로 받아들여지고 있다. 반면에, 그에 따른 보안 위협에 대해서는 신중하게 접근해야 한다. 기존에는 기업 내부 기밀 정보의 외부 유출이 엄격히 관리되었으나, BYOD 환경이 도입됨에 따라 내부 정보 유출에 대한 통제가 어려워졌다. 또한 공개 Wi-Fi 등 보안이 취약한 공용 네트워크를 통해 기업 내부 서비스에 접속할 경우 해킹에 따른 보안 위협도 무시할 수 없다. 이러한 보안 위협에 대처하기 위해서는 근본적으로 사용자의 모든 행위에 대해 상황을 인식하고 관리해야 한다. 본 논문에서는 BYOD 환경에서 사용자의 기업 내부 서비스 접속 및 이용에 따른 모든 상황을 단위 정보로 정의함으로써 상황을 인식하는 방안을 제안한다. 이렇게 정의된 정보는 기업 내부 보안 정책 수립, 비정상 행위 탐지 등에 활용 될 수 있다.

1. 서론

시간과 장소에 구애받지 않고 인터넷을 이용 할 수 있는 환경이 보편화됨에 따라 BYOD 환경이 도입되면서 회사 외부에서도 스마트폰, 태블릿 PC 등을 이용해 업무를 처리하는 모습을 어렵지 않게 볼 수 있다. VMware에서 발표한 'New way of life 2013'[1]에 따르면 한국의 경우 설문 응답자의 93%가 개인 소유의 단말기기를 활용하여 회사의 업무를 처리한다고 했으며, 평균적으로 2.4대의 개인 단말기기를 보유한 것으로 나타났다. 이들이 개인 단말기기를 업무에 활용하는 주된 이유는 고객의 요구에 신속하고 원활하게 응대할 수 있으며, 개인기기에 있는 소프트웨어가 더 편리하고 익숙하기 때문인 것으로 보인다. 이처럼 업무의 효율성 증대, 업무 처리 비용 절감, 업무 스트레스 감소 등의 많은 장점으로 인하여 BYOD는 점차 기업 문화의 한 트렌드로 받아들여지고 있다.

반면에 BYOD 환경을 도입함으로써 나타나는 보안적 위협 요소에 대해서는 조금 더 신중하게 접근해야 한다. 기존에는 기업 내부 기밀 정보의 외부 유출이 엄격히 관리되었으나, 개인 소유의 단말기기를 통해 외부에서 회사 업무를 볼 수 있는 환경이 조성됨에 따라 기업 내부 기밀정보 유출에 대한 통제가 어려워졌다. 또한 무선 Wi-Fi 등 보안이 취약한 공용 네트워크를 통해 기업 내부 서비스를 이용하는 경우 해킹에 따른 보안 위협 요소도 무시할 수 없다.

이러한 모든 보안 위협에 대처하기 위해서는 근본적으로 다방면의 시각을 가지고 사용자의 행위에 대해 인식 할 필요가 있다. 예를 들면, 어떠한 사용자가 기업 내부 서비스에 접근하였는지, 어떠한 기기를 통해 접속하였는지, 어떠한 네트워크 환경에서 접속하였는지, 현재 어떤 서비스를 이용하고 있는지 등을 들 수 있다. 본 논문에서는 사용자의 기업 내부 서비스 접속 및 이용에 따른 모든 상황을 단위 정보로 정의함으로써 상황을 인식하는 방안을 제안한다.

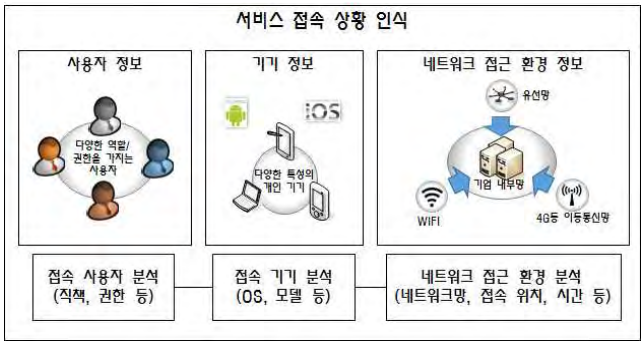
본 논문의 구성은 다음과 같다. 2장에서 사용자의 접속 및 이용에 따른 '상황 정보'에 대한 정의 및 분류, 3장에서 해당 상황정보의 수집 방법에 대해 설명하고, 4장에서는 수집 된 정보의 활용 방안, 5장에서 결론 및 향후 연구에 대해 기술한다.

2. 상황정보 정의 및 분류

'상황 정보'란 사용자가 기업 내부 서비스에 접속, 그리고 이용하는 모든 행위를 하나의 데이터로 규정하여 상황을 인식하기 위한 정보를 말한다. 어떠한 권한을 가진 사용자가 서비스를 요청했는지, 현재 사용자가 어떤 서비스를 이용하며 어떤 행위를 하고 있는지 등의 모든 상황에 대해 인식이 가능하다면 사용자의 비정상적인 행위에 대해 즉시 대처할 수 있을 것이다.

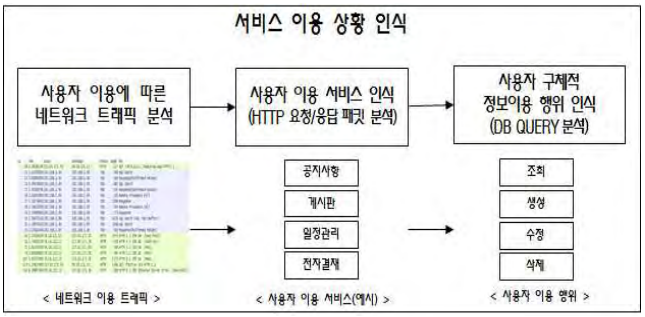
상황을 인식하기 위해서는 우선 사용자의 모든 행위에 따른 상황 분류가 먼저 필요하다. 본 논문에서는 크게 접속 시점에서의 상황정보, 그리고 이용 시점에서의 상황정보로 분류하였다.

접속 시점에서는 주로 어떠한 사용자가 접속하였는지, 어떠한 기기를 통해 접속하였는지, 어떤 네트워크 환경에서 접속하였는지 등의 상황적 인식을 할 수 있다. 정리하면, 접속 시점에서의 상황 인식을 위한 정보는 사용자 정보, 기기 정보, 네트워크 접근 환경 정보로 분류 될 수 있다. 즉, 위의 세 가지 분류 정보를 기반으로 어떠한 권한을 가진 사용자가 어떤 기기를 가지고 어떤 네트워크 환경에서 기업 내부 서비스에 접속을 하였는지의 상황적 인식이 가능하다.



(그림 1) (서비스 접속 상황 인식)

이용 시점에서는 현재 사용자가 어떠한 서비스를 이용하고 있으며, 어떠한 행위를 하고 있는지의 여부 등의 상황적 인식을 할 수 있다. 기업 내부 서비스에는 여러 서비스가 존재한다. 본 논문에서는 WEB 서비스 이용 관점에서 네트워크 트래픽 분석을 통해 사용자의 이용 상황에 대해 인식하는 방안을 연구하였다. WEB 서비스 이용 관점에서는 사용자가 공지사항, 게시판, 자료실 등 WEB 서비스 내의 어떠한 서비스를 이용하고 있는지, 이전에 이용하던 서비스는 무엇이었는지, 해당 서비스를 이용하며 어떤 행위를 하였는지, 요청한 정보는 무엇인지 등의 정보를 통해 이용 상황을 인식할 수 있다.



(그림 2) (서비스 이용 상황 인식)

접속 및 이용 상황 인식을 위한 세부 데이터는 아래 표와 같다. 접속 상황정보는 사용자 정보, 기기정보, 네트워크 접근환경 정보로 구분하여 작성하였으며, 이용 상황정보는 WEB 서비스 이용 관점에서 수집 가능한 데이터들을 정리하였다.

<표 1> 접속 및 이용 상황 인식을 위한 데이터 항목

접속 상황 인식 정보		이용 상황 인식 정보		
사용자 정보	사용자 ID	웹 서비스 이용 정보	접속 IP	
	사용자 권한, 직책		웹 서비스 요청 URI	
	사용자 상태		이전 페이지 URI	
기기 정보	기기명		웹 서비스 요청 시간	
	단말기 종류		웹 서비스 요청 port	
	OS 정보		웹 Session ID 정보	
	브라우저 정보		요청 File 이름	
	Screen Size 정보		요청 File 형식	
	MAC		요청 File Size	
네트워크 접근환경 정보	접속 시간		구체적 행위	조회
	사용자 IP			생성
	접속 국가			수정
	접속망			삭제

3. 수집 방법

접속 시점에서 사용자 정보, 기기 정보, 네트워크 접근 환경 정보에 대해 언급하였다. 사용자 정보는 사용자의 웹 서비스 접속 인증 시 인증 서버에 해당 사용자의 권한과 상태를 조회함으로써 정보를 수집할 수 있다. 기기 정보는 Browser Fingerprinting[2] 기술을 활용하여 해당 기기의 식별을 위한 정보를 수집할 수 있으며 내부 네트워크 접속 사용자의 경우 내부 IP 주소 할당 시 발생하는 DHCP 패킷을 통해 기기의 MAC 주소를 추가로 수집할 수 있다. 네트워크 접근 환경 정보는 기기의 접속 IP를 중심으로 접속 위치, 이용 네트워크망 등을 분석하여 상황정보를 수집 할 수 있다. 이 외에 HTTP 패킷 헤더 내의 Session ID 정보 수집을 통해 NAT를 통한 웹 서비스 접속 사용자의 식별이 가능하다.

이용 시점에서는 사용자와 웹 서버 간의 네트워크 트래픽과 웹 서버와 데이터베이스 간의 트래픽 분석을 통해 상황 인식을 위한 정보 수집이 가능하다. HTTP 요청/응답 패킷[3]을 통해 사용자의 웹 서비스 이용 행위를 인식할 수 있으며 데이터베이스 쿼리문을 수집함으로써 사용자의 구체적인 정보 이용 행위 정보를 수집 할 수 있다. 또한, 데이터베이스 트래픽 중 RPC 타입의 TDS 패킷 수집을 통해 사용자의 웹 서비스 요청에 따라 데이터베이스에 어떠한 프로시저를 호출하고 있는지의 분석이 가능하다.

4. 상황정보 활용 방안

위의 수집 방법을 통해 사용자의 기업 내부 서비스 접속 및 이용에 따른 상황을 정형화된 데이터로 수집 할 수 있다.

정형화된 데이터를 활용하여 사용자의 접속 및 이용 행위에 대한 상황적 인식이 가능하며, 상황 인식 정보들을 관리함으로써 사용자 별로 주로 사용하는 기기, 주로 접속하는 위치, 주로 이용하는 서비스 등 사용자 행위에 따른 패턴화된 프로파일 정보를 생성할 수 있다. 이러한 프로파일 정보를 바탕으로 과거 행위 패턴과 현재 사용자 행위에 대한 비교가 가능하다. 이 외에 사용자의 사내 서비스 접속

및 이용에 따른 기업 내부 서비스 접근 시의 보안 정책을 수립하는데 상황정보들을 활용할 수 있다.

5. 결론 및 향후 연구

BYOD 환경에서는 개인 소유 단말기기를 통해 기업 내부 업무를 처리하므로 기업 내부 기밀 정보 유출, 해킹에 따른 보안위협 등에 대한 완전한 통제가 어렵다. 따라서 이러한 보안 위협에 대처하기 위해서는 우선 사용자가 어떠한 사용자인지, 어떤 기기를 통해 접속하였는지, 어떠한 네트워크 환경에서 기업 내부 서비스에 접근하였는지, 어떤 서비스를 이용하고 있는지 등의 모든 상황적 인식이 필요하다.

본 논문에서는 사용자의 기업 내부 서비스 접속 및 이용에 따른 모든 상황을 단위 정보로 정의하여 상황을 인식하는 방법을 제안하였다. 이러한 상황 인식 데이터를 통해 상황을 인식함으로써 사용자별로 주로 사용하는 기기, 주로 접속하는 위치, 주로 이용하는 서비스 등 패턴화 된 프로파일 정보를 생성할 수 있다. 이 정보들을 활용하여 기업 내부 보안 정책을 수립하는데 도움이 될 뿐만 아니라, 기업 내부 서비스의 비정상적인 접속 및 이용 행위에 대해서 탐지가 가능할 것이다. 향후에는 본 논문에서 제안한 상황 정보를 수집하기 위한 시스템을 개발하고 검증할 예정이다.

ACKNOWLEDGMENT

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행하였음. [10045109, BYOD, 스마트워크 환경에서 상황정보 기반 동적 접근통제 기술 개발]

참고문헌

[1] VMware. “New way of life 2013”, 2013

[2] Peter Eckersley. “How Unique Is Your Web Browser?”, Lecture Notes in Computer Science Volume 6205, 2010, pp 1-18

[3] IETF ‘RFC 2616-HTTP 1.1’