모바일기기의 성능제약을 고려한 단일인증 프로파일의 정의

정종일° 차무홍, 유의혁, 신동규 신동일
세종대학교 컴퓨터공학과
{jijeong°, bidon, solui, shindk, dshin}@gce.sejong.ac.kr

A definition of Single Sign-On profile considering limitation of mobile devices

Jongil Jeong° Moohong Cha Weehyuk Yu Dongkyou Shin, Doingil Shin
Dept. of Computer Engineering, Sejong University

요 약

이동통신사가 선택한 컨텐츠만이 사용자들에게 서비스 될 수 있는 환경에서 다양한 컨텐츠 서비스의 제공을 기대하기는 어려운 실정이다. 이 같은 문제를 해결하기 위해 서비스 제공자들은 이동통신회사의 전송망을 대여하여 자신들의 모바일 포털 서비스를 통해 사용자들에게 다양한 컨텐츠를 제공할 수 있다. 그러나 개별적으로 관리되는 사용자 인증 서버를 통한 인증과정은 사용자들에게 반복적인 인증정보제공절차를 강요한다. 이러한 보안정보의 빈번한 노출로 인하여 잠재적인 보안 취약성이 야기된다. 단일인증이 보안정보 노출의 최소화를 위한 대안이 될 수 있지만 모바일 기기들의 성능적인 제약은 모바일 및 유비쿼터스 환경에 단일인증을 적용하는데 걸림돌이 되고 있다. 본 논문에서는 유무선 통합 환경에서 단일인증을 제공하기 위해 모바일 단말기와 유선도메인 간에 인증정보를 교환하는 profile을 정의하여 모바일 단말기의 성능적인 제약을 극복하기 위한 방안을 제시한다.

1. 서 론

모바일 정보 서비스 영역에서 이동통신사, 컨텐츠 제공자, 빌링 에이전시 그리고 서비스 제공자는 주요 지휘자의 역할을 하고 있다 [1]. 그렇지만 이들이 하나의 회사에 통합된 형태로 운용되기 때문에 각각의 지휘자들이 가져야 할 특성이나 차이점을 발견하는 것은 매우 어려운 실정이다.

통신회사는 컨텐츠 제공자, 인터넷 서비스 제공자 그리고 심지어는 가입자들까지 통제할 수 있는 위치에 있기 때문에 최근까지 모바일 가입자들에게 제공된 컨텐츠 서비스들은 통신회사에 의해 지배 받을 수밖에 없었다. 이러한 일방적인 지배 환경은 통신회사에 의해 선택된 컨텐츠만이 모바일 네트워크를 통해 제공되는 문제를 야기하고 있으며 사용자들에게 보다 다양한 컨텐츠가 제공될 기회를 가로 막고 있다. 이 같은 문제를 해결하기 위해 서비스 제공자들은 이동통신회사의 전송망을 대여하여 자신들의 모바일 포털 서비스를 통해 사용자들에게 다양한 컨텐츠를 제공할 수 있다.

대개 통신회사는 컨텐츠 서비스에 대한 접근을 제공하기 위해 자체의 인증 서버를 관리한다. 즉, 사용자들의 휴대전화 번호만을 이용하여 사용자를 인증할 수 있다. 그러나 전송망을 대여하여 서비스를 제공해야하는 모바일 서비스 제공자들은 사용의 인증을 위해 자체적인 사용자 정보 데이터베이스를 관리해야 하며 사용자는 반드시 사용자의 이름과 패스워드를 제공해야하는 번거로움이 있다.

사용자가 원하는 서비스에 접근할 때 마다 보안정보를 제공하는 일은 매우 번거로운 일이다. 이는 단순히 사용자의 편의성을 훼손하는 것으로 인식될 수 있지만 공개된 망을 통한 보안정보의 빈번한 노출로 인해 잠재적인 보안문제가 발생할 수 있음을 반드시 인식해야 한다. 잠재적인 보안문제에 대한 대책으로서 사용자가 보안정보의 노출을 최소화하는 방안이 마련되어야 한다. 단일인증은 사용자의 보안정보 노출을 최소화 할 수 있는 가장 좋은 방안이 될 수 있다. 그러나 낮은 CPU성능, 낮은 대역폭 그리고 낮은 메모리 저장능력 등 모바일 기기가 갖는 핸디캡은 모바일 및 유비쿼터스 환경에 웹 서비스와 단일인증 같은 새로운 기술들을 적용하는데 걸림돌이 되고 있다.

본 논문에서는 유무선 통합 환경에서 단일인증 방법을 제공하기 위해 모바일 단말기와 유선도메인 간에 인증정보를 교환하는 profile을 정의하여 유무선 통합 단일인증 적용의 걸림돌이 되고 있는 모바일 단말기의 성능적인 제약을 극복하기 위한 방안을 제시한다. 또한 각 도메인 간에 정확하고 안전한 인증정보 교환을 위해 고려되어야 할 보안사항을 정의하고 이에 대한 대책을 제시한다.

2. 배경지식

웹 서비스 프레임워크를 적용하고 있는 모바일 및 유비쿼터스 서비스 환경의 보안을 위해 새로운 접근 방법이 고려되어야 한다. 즉, 웹 서비스를 이용하는 분산된 시스템들이 제공하는 수많은 서비스들 사이에서 특정 서비스에 접근하기위해서는 단일인증 같은 일관되고 단순화된 접근 방법이 제공되어야 한다.

2.1 단일인증

단일인증의 기본적인 개념은 보안 아키텍처의 복잡성을 단일인증서비스에 전가하는 것이다. SAML은 단일인증 후 신뢰관계가 형성된 보안 도메인들 사이에서 사이트 접근을 용이하게 하기 때문에 단일인증을 구현하기 위한 접근방법으로서 매우 적합한 프레임워크이다.

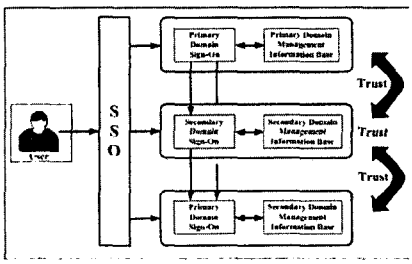

그림 1 다양한 서비스들에 대한 단일인증 서비스

2.2 SAML (Security Assertion Markup Language)

SAML은 OASIS (Organization for Advancement of Structured Information Standards)가 제안한 표준으로 도메인들 간에 사용자, 기기 또는 subject라 불리는 식별이 가능한 엔티티의 인증 및 권한 정보를 교환하기위한 표준이며 assertion기반의 subject를 수용하거나 거절하는 request-response 프로토콜을 정의한다 [2, 3].

Assertion은 사용자, 자원, 속성에 대한 정보를 XML형태로 표현하며 인증, 권한 그리고 속성의 세 가지 타입으로 분류된다.

2.3 Artifact

SAML은 HTTP redirect에 대한 권한 요청이 너무 긴 경우에 artifact 메커니즘을 정의한다. Artifact는 사용자 인증을 위해 보안 도메인 내에서 생성되어 다른 보안 도메인에 전송되며 일종의 토큰의 역할을 한다 [4].

3. 모바일 및 유비쿼터스 서비스 환경을 위한 단일인증 아키텍처의 설계

단일인증 서비스를 얻기 위해 모바일 사용자가 제공하는 인증정보를 유선서비스 환경내의 단일인증 메커니즘으로 전송하기 위해서는 다음을 고려해야한다.

- 모바일과 유선서비스 환경사이에서 사용자의 인증정보를 전송하기위한 적절한 프로토콜로 변환할 수 있는 장비가 필요하다.
- 사용자의 인증정보가 전송되는 동안 기밀성과 무결성이 보장되어야 한다.
- 단일인증 구현을 위한 프레임워크는 각 도메인에서 정의된 사용자 인증 메커니즘을 다룰 수 있도록 포괄적이어야 한다.

그림 2는 모바일과 유선서비스 네트워크를 연결하는 프레임워크의 일례로서 프로토콜 게이트웨이 역할과 전송되는 컨텐츠들을 인코드 및 디코드하는 역할을 한다.

그림 3은 사용자 인증을 얻은 후 다른 도메인에 접근하기 위해 모바일 사용자가 본인의 보안 정보를 유선 서비스 네트워크에 제공하는 단일인증 아키텍처이다.

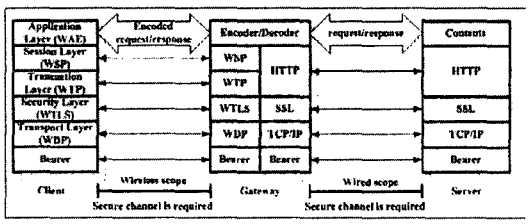

그림 2 WAP 게이트웨이의 연결 [5]

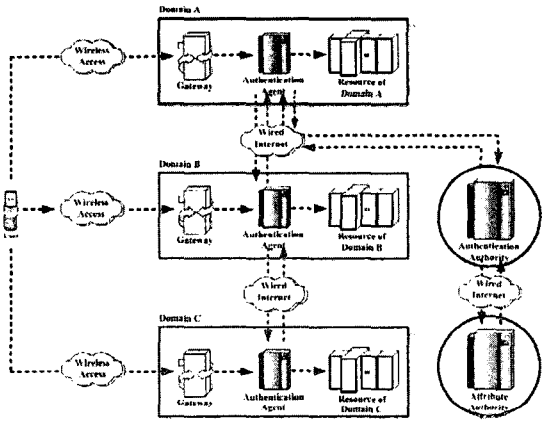

그림 3 유무선 통합을 위한 단일인증 아키텍처

3.1 사용자 인증정보에 의존적인 프로파일과 SAML artifact에 의존적인 프로파일의 비교

그림 3의 단일인증 아키텍처에서 교환되는 사용자의 보안정보와 인증 및 권한정보의 기밀성과 무결성을 보장하기 위해서는 각 메시지를 전자서명하고 암호화할 필요가 있다.

그림 4와 5는 전자서명과 암호화를 처리하는 주체와 위치 및 순서를 표현한다. 그림 4에 대한 설명은 다음과 같다.

(1) 모바일 기기에 있는 사용자의 정보는 authentication authority로 전송된다.

(2) Authentication authority는 사용자를 인증함으로써 인증 정보를 생성한다.

(3) 인증 정보는 안전한 전송을 위하여 전자적으로 암호화되고 서명된다.

(4) 인증 정보는 모바일 디바이스에게 전달된다.

(5) 모바일 디바이스는 전송된 인증정보의 불법적인 위조 및 변조를 막기 위해 무결성을 체크한다.

(6) 모바일 기기는 도메인 B에 접근하기 위해 인증정보를 전송한다.

(7) 도메인 B는 수신된 인증정보의 무결성을 체크하고 암호화된 부분을 복호한다.

(8) 인증정보가 유효하다면 사용자의 접근이 허용된다.

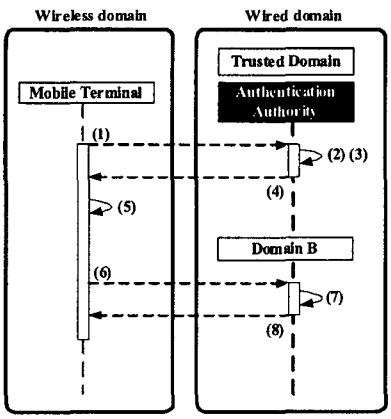

그림 4 사용자인증정보에 의존적인 단일인증 profile

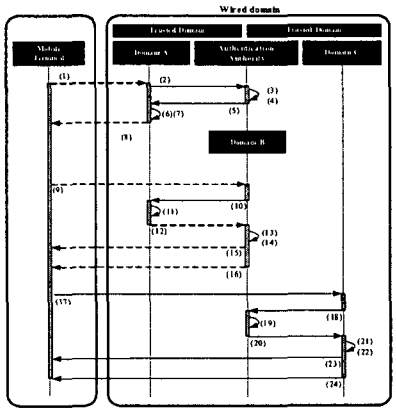

그림 5 artifact를 교환하는 단일인증 profile

그림 5는 그림 4의 전체적인 과정 즉, 인증정보에 대한 전자적인 서명과 암호화 및 복호화를 유선환경(Wired domain)에 모두 전가 시키고 모바일 기기는 단지 인증정보를 포인팅하는 artifact만을 교환한다. 그림 5의 단일인증 profile은 그림 4의 단일인증 profile보다 더욱 많은 처리 과정을 거쳐야하지만 높은 컴퓨팅 능력을 요구하는 처리과정은 모두 유선서비스 환경의 Authentication Agent에서 처리하게 된다.

3.2 위협모델과 보안대책

3.2.1 profile의 스텝별 위협요소 분석과 대책 [4]

그림 5의 artifact교환 단일인증 profile에서 예상되는 위협은 다음과 같다.

- step 2: 사용자 보안정보 보호가 필요하다.
- step 8, 11, 16, 19, 24: artifact와 artifact를 수신할 목적지 정보의 보호가 필요하다.
- step 7, 15, 23: artifact의 재사용을 방지하고 Assertion을 불법적인 위변조로부터 보호해야한다.
- step 13, 21: XML기반의 응답 메시지에 대한 기밀성과 무결성이 보호되어야한다.

표 1 각 스텝별 위협요소와 대책

step	위협요소	대책
2	confidentiality	SSL, TLS 또는 WTLS
8,11, 16,19, 24	confidentiality	SSL, TLS 또는 WTLS
7,15, 23	reuse confidentiality integrity	one-time use, XML encryption, SOAP protocol
13,21	confidentiality integrity	XML Signature SSL, TLS 또는 WTLS

3.2.2 Artifact와 Assertion 도난에 대한 대책 [4]

- 단말기와 Domain간에 통신보안 프로토콜을(예를 들면, SSL3.0, TLS1.0, or WTLS)을 구축하여 artifact의 기밀성을 유지한다.
- Artifact의 lifetime을 제한한다.
- Assertion의 발행시간 및 사용자인증시간을 명시한다.
- Assertion에 사용자의 인증 위치를 알 수 있는 IP address를 명시하고 비교한다.
- 목적지에서 출발지로 전송된 Assertion의 유효기간을 체크한다.

4. 결론

본 논문에서는 사용자 인증정보에 대한 전자서명 및 암/복호과정을 기존의 유선환경에서 구축된 단일인증 시스템에 전가시키고 모바일 디바이스에게는 사용자 인증정보를 참조하는 artifact만을 부여하는 방법을 제공함으로써 모바일 디바이스의 성능적인 제약을 극복할 수 있는 방안과 제안된 profile의 적용 시 고려해야할 보안 위협 사항과 이에 대한 대책을 제시함으로써 보다 안전하고 효율적인 단일인증 구현을 위한 가이드라인을 제공하고 있다.

참고문헌

[1]http://www.eastandard.net/financialstandard/commentary/comm01.h
[2]Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1: http://www.oasis-open.org/committees/security/
[3]Pfitzmann, B., Waidner, B.: Token-based web Single Signon with Enabled Clients. IBM Research Report RZ 3458 (#93844), November (2002)
[4]Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) V1.1: http://www.oasis-open.org/committees/security/
[5] WAP White_Paper1.pdf : http://www.wapforum.org/what/WAPWhite_Paper1.pdf