情 報 保 護 學 會 誌
第17卷 第5號, 2007. 10

모바일 및 유비쿼터스 서비스 환경을 지원하는 XML기반의 단일인증 설계

손민우*, 정종일**, 신동일***, 신동규****

요 약

모바일 및 웹 어플리케이션의 통합으로 인해 모바일 사용자들이 접근할 수 있는 서비스의 수는 크게 증가했지만 사용자들은 여러 개의 사용자 이름과 패스워드를 관리해야하는 어려움을 가지고 있다. 이와 유사한 상황은 다양한 종류의 개인 장비, 무선 센서, 서버, 서비스 그리고 댁내에서 네트워크화 된 기기들로 구성된 홈 네트워크 환경으로 확장될 수 있다. 최근 디지털 홈 워킹 그룹 (DHWG: Digital Home Working Group)은 보안 강화를 위해 사용자와 기기에 대한 호환성 있는 인증 및 인가 메커니즘을 위한 프레임워크를 준비할 것을 권고하고 있다. 인터넷, 인트라넷 그리고 댁내에 분산된 자원들을 사용하기 위해 각 어플리케이션에 대한 사용자의 인증 및 인가는 반드시 필요하지만 이는 보안 관리와 시스템 성능 측면에서는 커다란 부담이 된다. 본 논문에서는 XML기반의 단일인증기술 표준인 SAML (Security Assertion Markup Language)을 이용한 단일인증 아키텍처를 제안한다. 제안된 아키텍처를 기반으로 모바일 및 유비쿼터스 서비스 환경에서 모바일과 홈 기기 간에 서로 다른 개체의 인증 및 인가 프로파일 정보의 교환을 가능하게 하므로 분산 환경에서의 보안 관리를 강화할 수 있다. 특히 제안된 아키텍처에서는 고도의 연산능력을 필요로 하는 보안정보의 전자서명 및 암복호 작업을 유선환경에 구성된 고성능의 기기로 전가하고 모바일 기기는 사용자의 인증을 검증할 수 있는 작은 문자열 형태의 artifact를 보유하고 이를 사용자의 인증에 이용함으로써 낮은 컴퓨팅 능력과 기억용량의 한계 같은 모바일 기기의 성능적인 제약을 극복할 수 있게 한다.

Ⅰ. 서 론

모바일 및 웹 어플리케이션의 통합으로 인해 모바일 사용자들이 접근할 수 있는 서비스의 수는 크게 증가했지만 사용자들은 여러 개의 사용자 이름과 패스워드를 관리해야하는 어려움을 가지고 있다. 이와 유사한 상황은 다양한 종류의 개인 장비, 무선 센서, 서버, 서비스 그리고 댁내에서 네트워크화 된 기기들로 구성된 홈 네트워크 환경으로 확장될 수 있다[1]. 이와 관련하여 디지털 홈 워킹 그룹 (DHWG: Digital Home Working Group)은 보안강화를 위해 사용자 및 기기에 대한 호환성 있는 인증 및 인가 메커니즘을 위한 프레임워크를 준비할 것을 권고하고 있다[2]. 홈 네트워크는 모바일 및 웹 서비스 환경에서의 인증 및 인가를 위한 프레임워크를 기반으로 확장될 수 있을 것으로 기대되지만 모바일 및 웹 서비스는 보안 기반이 분산되고 시스템 전반에 키 기반 구조를 구현해야하는 단점이 있다. 뿐만 아니라 인터넷, 인트라 넷 그리고 댁내에 분산된 자원들을 사용하기 위해 각 어플리케이션에 대해 사용자의 인증 및 인가가 반드시 필요하지만 이는 보안 관리와 시스템 성능에 커다란 부담을 주게 된다[3]. 즉, 사용자가 갖는 보안정보관리에 대한 부담 외에 사용자가 접근을

* 세종대학교 대학원 컴퓨터공학과 멀티미디어 인터넷 연구실 (minwoo15@gce.sejong.ac.kr)
** 세종대학교 대학원 컴퓨터공학과 멀티미디어 인터넷 연구실 (jijeong@gce.sejong.ac.kr)
*** 세종대학교 대학원 컴퓨터공학과 멀티미디어 인터넷 연구실 (dshin@sejong.ac.kr)
**** 세종대학교 대학원 컴퓨터공학과 멀티미디어 인터넷 연구실 (shindk@sejong.ac.kr)

시도하는 각 시스템의 관리자는 수많은 패스워드들을 데이터베이스에서 관리해야하고 공개된 전송망을 통해 사용자의 패스워드 같은 민감한 보안정보들이 빈번하게 교환되기 때문에, 발생할 수 있는 잠재적인 보안문제들에 대한 대책을 마련해야한다.

보안 특징으로써 단일인증은 사용자가 분산 시스템들이 제공하는 다양한 서비스로 로그인 하는 것을 허용하는 반면 사용자는 다양한 서비스로 로그인할 때 단지 1회의 인증만이 필요하거나 적어도 동일한 방법으로 사용자를 인증한다[4]. 현재 공개키 기반, 커버로스, 또는 패스워드-스토어에 의존하는 다양한 단일인증 솔루션들이 제안되었지만 각 솔루션은 사용자 측에 부가적인 기반구조와 새로운 관리단계를 필요로 하는 단점이 있다[5]. 최근 OASIS (Organization for Advance- ment of Structured Information Standards)는 XML기반의 보안 관련 정보를 교환하기 위해 SAML (Security Assertion Markup Language)을 표준으로 승인했다[6]. SAML은 서로 다른 개체들 간에 인증, 인가 및 프로파일 정보의 교환을 가능하게 하여 분산 환경의 보안 서비스들 간에 상호운용성을 제공한다. 특히 모바일 웹 서비스 워킹 그룹의 OMA (Open Mobile Alliance)에서는 사용자 인증과 인가를 위한 기술로서 SAML을 강력히 권고하고 있다[7].

본 논문에서는 모바일 및 홈 네트워크 서비스 환경을 위한 단일인증 아키텍처를 설계하였으며 메시징 시나리오를 제안하고 검증함으로써 제안된 아키텍처를 실험했다. 본 논문의 구성은 다음과 같다. 2.관련연구에서는 단일인증의 개념과 기존 단일인증 기술들의 비교와 SAML에 대해 서술하고 3.모바일과 홈 네트워크 서비스 환경을 위한 단일인증 아키텍처에서는 모바일 및 홈 네트워크 서비스 환경을 위한 단일인증 아키텍처의 설계를 제시하고 제시된 환경에 포함된 구성 요소들 간에 메시지들을 교환하는 실험을 통해 설계된 아키텍처를 검증한다. 또한 메시지 교환과정에서 발생할 수 있는 보안적인 취약성을 분석하고 이에 대한 보안 대책을 제시한다. 4.결론에서는 본 논문에서 제시하는 아키텍처의 특징 및 장점 등을 기술하고 결론을 내린다.

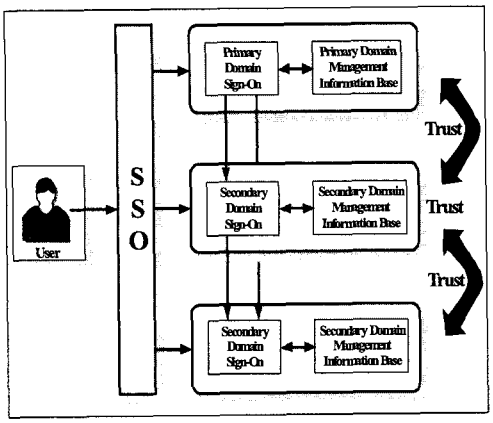
Ⅱ. 관련 연구

모바일 기기들은 사용자 및 서비스 제공자의 위치에 관계없이 홈 네트워크 서비스를 제공할 수 있는 가능성을 제시하고 있는 반면에 낮은 대역폭, 낮은 CPU성능 그리고 적은 메모리 용량 같은 약점들을 갖는다. 이러한 약점들은 모바일 및 홈 네트워크 서비스 환경에서 단일인증 같은 새로운 기술들을 채택하는데 있어 커다란 걸림돌이 되고 있다[8]. 따라서 이를 해결하기 위한 모바일과 홈 네트워크 서비스 환경의 보안을 위해 새로운 접근 방안이 고려되어야 한다. 즉, 분산 시스템이 제공하는 많은 서비스들 중에 특정 서비스에 접근하기 위해서는 일관되고 통합된 접근 방법이 제공되어야 한다. 이러한 목적에 부합하는 유선 인터넷 환경 상의 단일인증에 대한 연구는 활발히 진행되고 있으며 이에 발맞추어 OASIS는 SAML을 유선 인터넷 환경의 웹 서비스 어플리케이션에 단일인증 적용을 위한 표준 명세서로 승인했다. 최근 OMA (Open Mobile Alliance)는 SAML을 모바일 웹 서비스에서 사용자 인증 및 인가를 위한 기술로 강력히 권고하고 있지만 SAML을 적용한 시스템 개발을 위한 실질적인 가이드라인은 제안하지 않고 있다.

2.1. 단일인증

단일인증의 기본적인 개념은 보안 아키텍처의 복잡성을 단일인증 서비스로 전가하는 것이다. 단일인증 서비스는 인증 및 인가 같은 다양한 보안 특징들을 생성해내는 기존의 보안 구조를 포괄하는 역할을 한다[9]. 단일인증을 지원하는 시스템은 최초 사용자 인증 도메인에서 사용자로부터 모든 식별정보와 사용자 정보를 수집한다. 수집된 정보는 사용자가 접근을 시도할 또 다른 도메인에서 사용자 인증을 지원하는데 재사용된다.

[그림 1]은 다양한 목적지를 대상으로 하는 단일인증의 개념을 보여준다. 사용자는 단일인증서비스 (SSO: Single Sign-On)에 사용자를 인증에 필요한 아이디와 암호 같은 정보를 제공하여 최초의 도메인에서 인증을 받는다. 사용자가 신뢰관계를 갖는 다른 도메인에 접근을 할 경우 아이디와 암호 대신 이전 도메인에서 성공적으로 인증 받았음을 증명하는 정보를 제공하여 인증과정을 생략하거나 간소화할 수 있다.



〔그림 1〕 다양한 목적지를 대상으로 하는 단일인증의 개념

2.2. 단일인증 구현을 위한 기존 기술들과의 비교

단일인증을 구현하는 방법은 쿠키 같은 토큰 기반의 프로토콜을 사용하는 방법과 공개키 및 개인키를 기반으로 하는 방법으로 나누어질 수 있다[10]. 토큰 기반의 프로토콜들이 갖는 주된 장점은 주요 서비스 제공자들이 이미 SSL 서버의 인증서를 보유하고 있고 적절한 알고리즘학적인 구현이 브라우저를 통해 모든 클라이언트 기기에서 사용가능하다는 것이다. 뿐만 아니라 서비스 제공자와 동일한 안전한 채널을 통해서 사용자에 관련된 정보를 제공하기 위해 직접적인 관련이 없는 다양한 인증 토큰들을 사용할 수 있다[11]. 그러나 쿠키를 이용한 단일인증의 구현은 다음과 같은 문제점들을 갖는다[12].

- 쿠키들은 때때로 동일한 세션 키를 가지고 암호화되기 때문에 공격자가 단 하나의 쿠키에 대한 세션 키를 찾는다면 시스템 내부의 모든 사용자 쿠키가 취약해질 수 있다.
- 브라우저 내의 쿠키는 플러그-인이나 다른 방법들로 도난당할 수 있다.
- 스푸핑(Spoofing) 공격은 쿠키가 다른 도메인 들로부터 개별적인 서버들에게 보내져야 하는 것임을 기술할 방법이 없기 때문에 쿠키의 목적지 제어를 파괴할 수 있다.

SAML은 단일 인증 후 신뢰 보안 도메인들 사이에서 사이트 접근을 용이하게 하는데 적합한 표준으로 쿠키를 이용한 단일인증 솔루션 구현에 비해 많은 장점들을 갖는다. 토큰의 역할을 하는 artifact는 하나의 보안 도메인에서 만들어지고 다른 보안 도메인으로 전송되어 사용자 인증에 사용된다. 다른 도메인으로 전송된 artifact는 원래의 보안 도메인에 반환되고 사용자 인증 후 제거된다. 따라서 쿠키 기반의 단일인증 솔루션에서 세션 키가 노출되는 문제와 브라우저에서 토큰들이 도난당하는 문제를 해결할 수 있으며 artifact가 URL(Uniform Resource Locator)에 첨부되어 사용자의 정보를 담고 있는 메시지를 목적지로 전송하기 때문에 목적지 제어에 대한 문제점을 해결할 수 있다[13].

단일인증을 구현하기 위한 대표적인 키 기반 기술로는 공개키 기반 (PKI: Public Key Infrastruc -ture)과 커버로스 (Keberos)가 있다. [표 1]은 기존의 단일인증 기술들과 SAML의 차이점을 보여 준다.

〔표 1〕 단일인증 구현 기술들 간의 특징 비교

기술 / 특징	PKI	Keberos	SAML
키 교환 필요	O	O	X
부가적인 기반 구조 필요	O	O	X
사용자 인증 범위 확장의 용이성	어려움	어려움	용이함

공개키 기반과 커버로스는 사용자 인증을 위해 최종 사용자와 인증 도메인 간에 키를 교환하는 반면 SAML을 이용한 단일인증은 키 대신 사용자의 인증 여부를 판단할 수 있는 문자열 형태의 토큰을 교환한다. 공개키 기반과 커버로스 같은 키 기반의 인증 기술은 키를 교환하고 관리하기 위한 부가적인 기반을 형성해야 하는 반면 SAML은 기존에 구성된 인증 기반 기술에서 생성된 사용자 인증 정보를 이용하므로 키 교환과 관리를 위한 별도의 인증 기반을 구성할 필요가 없다. 공개키 기반과 커버로스는 사용자 인증을 위해 공개키 및 개인키를 사용하므로 키 기반의 인증 도메인간의 확장은 가능하지만 키를 지원하지 않는 도메인으로의 확장은 불가능하지만 SAML은 다양한 인증 기술들이 생성해내는 사용자 인증 정보를 포괄하도록 유연성 있게 설계되어 다양한 인증 기술들을 포괄할 수 있어 사용자 인증 범위의 확장성이 매우 높다.

2.3. SAML (Security Assertion Markup Language)

SAML은 시스템 간에 자동적이고 수동적인 상호소통 모두를 위한 단일인증을 제공하도록 설계되었다. 이러한 설계방향은 사용자를 또 다른 도메인으로 로그인하도록 하고 그들이 해당 도메인에서 행할 수 있는 모

든 권한을 정의하고 두 도메인 간에 자동으로 생성된 메시지의 교환을 관리할 것이다. SAML은 사용자, 기기 또는 주체 (subject)[1] 라고 불리는 동일함을 증명할 수 있는 특정 개체에 관련된 인증과 인가 정보를 교환하는 것을 가능하게 하며 XML의 부분집합을 이용하여 SAML은 시스템이 주장[2] 기반의 주체를 수용하거나 거절하는 요구/요청 프로토콜을 정의한다 [13].

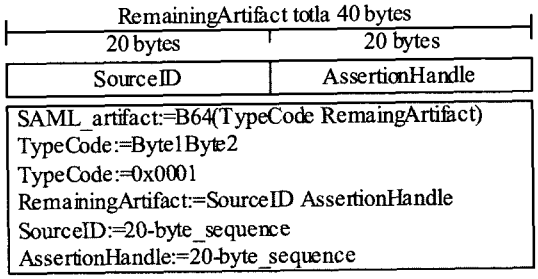
주장은 특정 주체에 대한 정확한 사실의 선언이다. SAML은 주장을 세 가지 타입으로 정의한다.

- 인증 주장 (Authentication assertion): 주체가 이전에 특정한 방법(패스워드, 하드웨어 토 큰 또는 X.509 공개 키 등)으로 인증되었다 는 것을 나타낸다.
- 인가 결정 주장 (AuthorizationDecision asser tion): 특정 주체의 자원 접근 요청을 허용하 거나 거절해야 함을 가리킨다.
- 속성 주장 (Attribute asssertion) : 특정 주체가 특정 속성들과 관련되었다는 의미한다.

SAML은 주장이 어느 위치에 위치해야하는지 지정하지 않는다. 다만 로컬 시스템들은 부정확한 결정에 의한 주장이 발생하면 보안수준과 적용정책들이 충분한지 결정한다. 이러한 SAML의 특징은 주장을 수용하기 전에 신뢰관계를 가질 것을 강력히 권고한다.

2.4. Artifact

SAML은 인가 요청이 HTTP를 재전송하기에 너무 긴 경우 artifact방식을 이용한다. 토큰 역할을 하는 artifact는 하나의 도메인에서 생성되어 사용자 인증을 위해 다른 보안 도메인으로 보내진다.



〔그림 2〕 artifact의 구조

[그림 2]와 같이 artifact는 서버가 주장을 검색하는데 사용하는 AssertionHandle을 위한 20바이트의 임의의 수(random number)와 SourceID를 위한 20바이트의 TypeCode를 포함하는 총 40바이트의 RemainingArtifact로 이루어진 필수의 2바이트 TypeCode를 포함한다[13].

Ⅲ. 모바일 및 홈 네트워크 서비스 환경을 위한 단일인증 아키텍처

모바일 및 홈 네트워크 서비스 환경을 위한 단일인증 아키텍처의 설계 목적은 모바일 사용자가 다양한 인증 정보의 집합을 처리하고 기억해야하는 필수적인 요구사항들을 감소시킴으로써 보안을 개선하고 이를 통해 모바일 사용자가 사용자 인증에 필요한 시간소요를 줄이는 것이다.

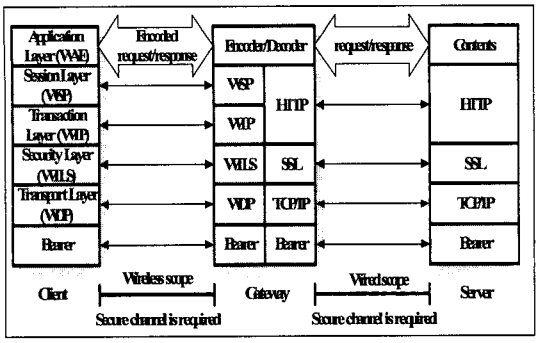
단일인증 서비스를 얻기 위해 모바일 사용자는 적어도 한번은 자신의 인증 정보를 제공해야 하고 이 정보는 결국 유선 서비스 환경의 단일인증 시스템으로 전달된다. 모바일 환경에서 유선 서비스 환경의 인증 서버로 인증정보가 전달되는 과정에서 다음과 같은 사항들이 고려되어야 한다.

- 모바일과 유선 서비스 네트워크 사이에서 사용자의 인증 정보를 전달하기위해 적절한 변환 기능을 갖춘 장비가 필요하다.
- 사용자의 인증 정보가 전송되는 동안 기밀성과 무결성이 보장되어야 한다.
- 단일인증 구현을 위해 사용자인증에 관한 보안정보를 전달하는 프레임워크는 도메인별로 정의된 사용자 인증방법을 모두 수용할 수 있어야 한다.

모바일과 유선 서비스 네트워크를 연결하는데 광범위하게 사용되는 프레임워크들 중의 하나는 OMA의 WAP 프록시로 잘 알려진 WAP (Wireless Application Protocol) 게이트웨이이다[14]. [그림 3]은 WAP 게이트웨이에서 무선구간과 유선구간의 연결을 보여준다. WAP 게이트웨이는 모바일 도메인과 유선 인터넷을 연결하고 프로토콜 게이트웨이 역할을 하며 전송되는 내용을 인코드 하거나 디코드 한다.

1) subject를 주체로 번역함.

2) Assertion을 주장이라고 번역함.

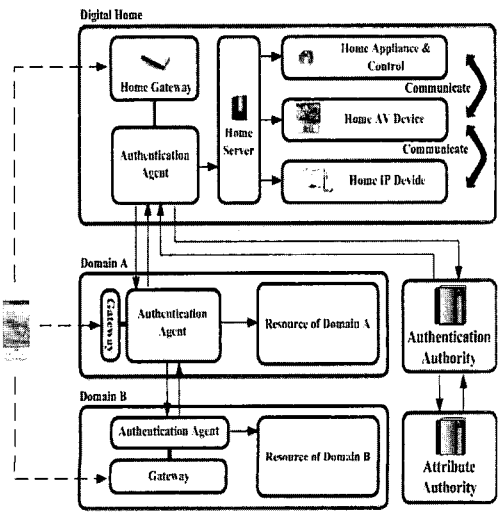


〔그림 3〕 WAP 게이트웨이를 이용한 유무선 환경의 연결

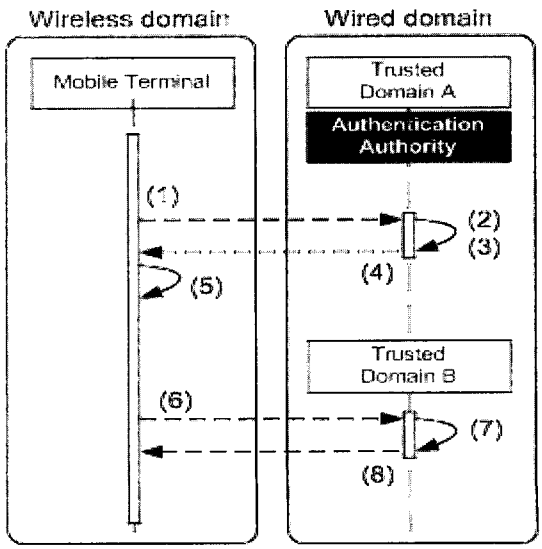
본 논문은 모바일 사용자가 인증을 얻은 후 또 다른 신뢰도메인에 접근하기 위해 자신의 인증에 필요한 정보를 유선환경의 홈 네트워크에 제공하고 홈 네트워크에서 생성된 사용자의 인증정보를 다른 신뢰도메인에서 재사용하는 단일인증 구현 방안을 제안한다. [그림 4]는 본 논문에서 제안한 단일인증 아키텍처에 대한 개념을 설명하고 있다. 모바일 사용자는 디지털 홈에 접근하기 위해 자신의 사용자 이름과 암호를 모바일 기기에 입력한다. 입력된 사용자의 정보는 모바일과 홈 네트워크를 연결하는 홈 게이트웨이를 통해 인증 에이전트에 전송된다. 인증 에이전트는 사용자 인증 요청을 상호신뢰관계를 갖고 있는 인증기관에게 보낸다. 인증기관은 사용자를 인증하고 디지털 홈의 인증 에이전트에게 인증 주장을 반환한다. 디지털 홈에서 성공적으로 사용자인증이 완료된 후 모바일 사용자는 도메인 A의 특정 서비스에 접근한다. 도메인 A는 사용자의 인증정보를 디지털 홈의 인증 에이전트에게 요청하면 인증에이전트는 도메인 A에게 인증 주장을 전달한다. 따라서 도메인 A는 인증기관에서 발행한 인증 주장을 통해서 사용자 인증을 수행한다.

제안된 단일인증 구현 방안에서 사용자 인증 정보는 무결성 보장을 위해 반드시 전자서명 되어야하고 공개된 전송망을 통해 이루어지는 보안정보의 기밀성 보장을 위해 암호화 되어야 한다. 그러나 전자서명 및 암호화 과정은 기능적인 제약이 따르는 모바일 기기에 커다란 부담이 된다. 따라서 본 논문에서는 암호화와 전자서명을 모바일 기기에서 처리하지 않고 연산능력과 메모리 용량이 우수한 유선환경에서 처리하는 방안을 제시한다. 제안된 구현 방안에서 모바일 기기는 기밀성과 무결성 보장을 위해 암호화와 전자서명이 필요한 인증 정보를 갖는 대신에 기기나 사용자 그 자신이 특정방법으로 인증되었음을 검증하는 크기가 작은 문자열 형태의 artifact를 소유한다. 본 논문에서 제시하는 방안은 모바일 기기에서 artifact를 소유하게 하고 이를 사용자 인증정보를 교환하고 검증하는 수단으로 사용함으로써 모바일 기기가 갖는 연산 능력의 한계를 극복할 수 있는 방안을 제시한다.

[그림 5]는 모바일 기기가 유선 도메인으로 사용자의 인증 정보를 가져오는 단일인증의 경우를 보여준다. 인증정보를 교환하는 과정은 다음과 같다.



〔그림 4〕 The Proposed 단일인증 Scheme

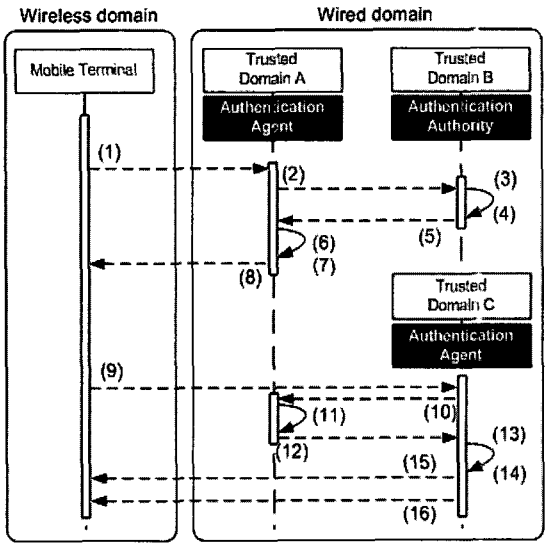


〔그림 5〕 인증정보기반 단일인증 프로파일

(1) 모바일 기기의 사용자 인증 정보는 신뢰관계 가 형성된 도메인의 인증기관으로 전송된다.
(2) 인증기관은 사용자의 인증정보를 이용하여 사용자를 인증함으로써 인증정보를 생성한다.
(3) 인증 정보는 안전한 전송을 위해 암호화되고 전자 서명된다.
(4) 인증 정보는 모바일 기기로 전송된다.
(5) 모바일 기기는 불법적인 위변조로부터 인증정보를 보호하기 위하여 전송된 인증 정보의 무결성을 검사한다.
(6) 도메인 B에게 접근하기 위해 모바일 기기의 인증정보를 도메인 B에게 전송한다.
(7) 도메인 B는 수신된 인증정보의 무결성을 체크하고 복호한다.
(8) 인증정보가 유효하면 모바일 사용자의 접근 이 허용된다.

[그림 6]은 모바일 기기가 암호화 및 전자서명으로 인한 연산 부담을 최소화하기 위해 인증정보인 주장 대신에 artifact를 유지하는 단일인증 절차를 보여준다. artifact를 이용한 단일인증 과정은 다음과 같다.

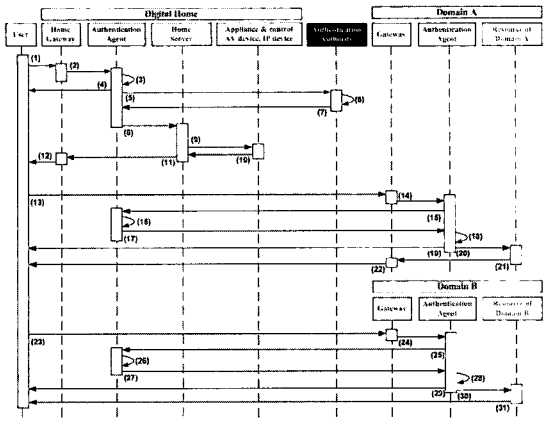
(1) 모바일 기기의 사용자 인증 정보는 도메인 A의 인증 에이전트에게 전달된다.



[그림 6] artifact기반 단일인증 프로파일

(2) 모바일 기기의 인증 정보는 신뢰관계가 형성 된 도메인의 인증기관에게 전달된다.
(3) 인증기관은 사용자의 인증정보를 사용하여 사용자를 인증함으로써 인증 주장을 생성한다.
(4) 안전한 전송을 위해 인증 주장은 암호화 되고 전자서명 된다.
(5) 인증 주장은 도메인 A의 인증 에이전트에게 전송된다.
(6) 도메인 A의 인증 에이전트는 전달된 인증 주장의 무결성을 검사한다.
(7) 도메인 A의 인증 에이전트는 모바일 사용자가 인증기관에 의하여 인증되었음을 검증하는 artifact를 생성한다.
(8) artifact는 모바일 기기로 전송된다.
(9) 도메인 B에게 접근하기 위해 모바일 기기의 artifact를 도메인 B에게 전송한다.
(10) 도메인 B의 인증 에이전트는 모바일 기기로부터 artifact를 받는 동시에 도메인 A의 인증 에이전트에게 artifact를 반환한다.
(11) 도메인 A의 인증 대행자는 받은 artifact에 대한 무결성을 검사한다.
(12) artifact가 유효하면 도메인 A의 인증 에이전트는 도메인 B의 인증 에이전트에게 모바일 사용자의 인증 주장을 보낸다. 이 과정에서 도메인 A의 인증 에이전트에서 보관된 artifact는 제거된다.
(13) 도메인 B의 인증 에이전트는 수신된 인증 주장의 무결성을 검증하고 복호한다.
(14) 도메인 B의 인증 에이전트는 모바일 사용자가 인증기관에 의하여 인증되었음을 검증하는 artifact를 생성한다.
(15) 생성된 artifact는 모바일 기기로 전송된다.
(16) 인증 주장이 유효하면 도메인 B에 대한 모바일 사용자의 접근이 허용된다.

[그림 6]에서 설명된 artifact를 사용하는 단일인증 구현 방안은 [그림 5]에서 설명한 단일인증 구현 방안보다 더 많은 처리 과정을 요구하지만 고도의 연산 능력을 필요로 하는 처리과정은 유선 도메인의 인증 에이전트가 대신하게 된다. 따라서 모바일 디바이스는 작은 문자열 형태의 artifact만을 가지고 있기 때문에 낮은 연산 능력과 작은 메모리 등 모바일 기기가 갖는 단점들을 극복할 수 있다.



〔그림 7〕 단일인증 아키텍처의 시퀀스 다이어그램

[그림 4]에서 설명된 아키텍처를 위한 인증 과정은 [그림 7]에서 시퀀스 다이어그램의 형태로 표현된다. [그림 7]은 상호 신뢰관계를 갖는 디지털 홈과 두 개의 다른 도메인에서 사용자의 단일인증을 적용하는 개체들 간에 교환되는 메시지들을 설명한다. 모바일 사용자가 디지털 홈에 접근할 때 사용자 인증에 관한 artifact가 인증기관에 의해 발행되었기 때문에 도메인 B의 과정들은 도메인 A의 과정과 유사하다. 시퀀스 다이어그램의 각 순서에 대한 설명은 다음과 같다.

(1) 사용자는 디지털 홈에 접근한다.

(2) 사용자는 인증에 필요한 정보를 제공한다.

(3, 4) 사용자를 위한 새로운 artifact가 생성되고 사용자에게 주어진다.

(5) 인증 에이전트는 인증기관에 사용자의 인증을 요청한다.

(6) 인증기관은 사용자를 인증 후 인증 주장을 발행한다.

(7) 발행된 인증 주장을 인증 에이전트에게 반환한다.

(8) 인증 주장이 유효하면 사용자는 홈서버에 접근할 수 있다.

(9) 홈 서버는 사용자를 접근하길 원하는 특정자원으로 접근을 허용한다.

(10, 11, 12) 사용자가 원하는 자원은 디지털 홈의 홈 서버와 게이트웨이를 통해서 사용자에게 제공된다.

(13) 사용자는 도메인 A의 자원에 접근요청을 한다.

(14) 도메인 A의 인증 에이전트는 디지털 홈에 로그인한 사용자의 artifact를 수신한다.

(15) artifact를 수신하고 이를 디지털 홈의 인증 에이전트에게 반환한다.

(16) 디지털 홈의 인증 에이전트는 반환된 artifact의 무결성을 검사한다.

(17) artifact가 유효하면 사용자의 인증 주장을 도메인 A에게 전달한다.

(18), (19) 인증 주장이 유효하면 사용자는 도메인 A의 자원에 접근 할 수 있다. 또한 사용자를 위한 새로운 artifact가 생성되고 사용자에게 주어진다.

(20, 21, 22) 인증 에이전트는 자원을 요청하고 도메인 A의 게이트웨이를 통해 사용자에게 제공한다.

(23) ~ (31)의 과정은 (13) ~ (22)의 과정과 동일하게 이루어진다.

그러나 각 도메인의 사용자 인증 방안은 각 도메인의 특징에 의존하는 것에 따라 달라질 것이다. 따라서 도메인들 사이에서 서로 다른 사용자 인증 방안들로부터 생성된 사용자의 인증과 관련된 보안 토큰들을 전송하기 위해서는 보안 정보의 표현을 제한하지 않는 프레임워크가 필요하다. SAML은 사용자의 인증 정보를 표현하기 위해 Action 엘리먼트를 정의한다. 주장은 사용자의 인증 정보를 표현하기 위해 AuthenticationStatement 엘리먼트와 다양한 사용자 인증 방법들을 지원하기 위한 AuthenticationMethod 속성을 포함하는 AuthenticationStatement 엘리먼트를 포함한다. SAML에서 지원하는 다양한 사용자 인증 방법들은 다음과 같다[13].

- Password
- Kerberos
- Secure Remote Password (SRP)
- Hardware Token
- SSL/TLS Certificate Based Client Authentication
- X.509 Public Key
- PGP Public Key
- SPKI Public Key
- XKMS Public Key
- XML Digital Signature
- Unspecified

```
<element name="AuthenticationStatement"
        type="saml:AuthenticationStatementType"/>
<complexType name="AuthenticationStatementType">
  <complexContent>
    <extension base="saml:SubjectStatementAbstractType">
      <sequence>
        <element ref="saml:SubjectLocality" minOccurs="0">
        <element ref="saml:AuthorityBinding" minOccurs="0"
                 maxOccurs="unbounded"/>
      </sequence>
      <attribute name="AuthenticationMethod"
                 type="anyURI" use="required"/>
      <attribute name="Authentication"
                 Instant type="dateTime" use="required"/>
    </extension>
  </complexContent>
</complexType>
```

〔그림 8〕 주장 스키마

```
<saml:Assertion AssertionID="00cda300-0d5de-8521-83e5-c2d9f6847b91"
                IssuerInstant="2004-04-07T14:12:01Z"
                Issuer="gce.sejong.ac.kr"
                MajorVersion="1" MinorVersion="0"/>
  <saml:Conditions NotBefore="2004-04-07T14:12:01Z"
                   NotOnOrAfter="2004-04-07T18:12:01Z"/>
    <saml:AuthenticationStatement
                   AuthenticationMethod="password"
                   AuthenticationInstant="2004-04-07T14:12:01Z'>
      <saml:Subject>
        <saml:NameIdentifier NameQualifier="gce.sejong.ac.kr">
                   JongilJeong
        </saml:NameIdentifier>
      </saml:Subject>
    </saml:AuthenticationStatement>
</saml:Assertion>
```

〔그림 9〕 인증 주장

[그림 8]은 주장 스키마를 나타내고 [그림 9]는 SAML 기관이 발행한 인증 주장을 포함하는 주장 문장을 나타낸다 ([그림 7]의 (6)을 의미)[9]. 이 메시지는 상호 신뢰관계를 갖는 세 개의 도메인들로 구성된 실험환경으로 검증하였고 실험환경 구축은 이전 논문에서 개발한 SAML 라이브러리를 사용하였다.

3.1. 제안된 단일인증 아키텍처에 대한 보안 위협과 대책

본 논문에서 제안한 단일인증 아키텍처에서 예상되는 보안 위협 모델과 대책은 다음과 같다.

- 메시지 도난

  도청자 (Eavesdropper)는 사용자의 보안정보를 포함하는 메시지를 복사하여 목적지에 접근한다. 이 경우 메시지가 목적지에 도달하기 전에 경유하는 모든 중개자들 간에 교환되는 메시지의 기밀성을 보장한다.

- 메시지 교환에 대한 공격

  메시지의 교환과정에서 다양한 공격이 시도될 수 있다. 예를 들면, MITM(Man-in-the-middle-attack)을 통해 제 3자가 보안 정보를 포함하는 메시지를 가로채어 위조 및 변조를 시도할 수 있다. 이 경우 목적지와 중개자 또는 중개자와 중개자 간 상호인증을 제공하고 메시지의 무결성과 기밀성을 제공한다.

- 사용자 위장

  목적지는 이전 중개자로부터 보안 정보를 포함하는하여 제 3자가 실제사용자로 위장하여 목적지에 접근할 메시지를 얻기 때문에 사용자를 악의적인 목적지로 유도 할 수 있다. 이 경우 목적지는 이전 중개자에게 그 자신이 인증되었음을 증명한다.

본 논문에서 제안한 단일인증 아키텍처의 메시지교환 단계에서 예상되는 보안 취약성과 보안 강화를 위한 보안 대책은 다음과 같이 정리 된다.

〔표 2〕 보안 취약성 구간과 보안 관련기술

위협 모델	보안 취약성 예상단계	보안 취약성 개선 관련기술
메시지 도난	인증에이전트	XML Encryption
메시지 교환에 대한 공격	(5), (7), (17), (27)	XML Signature, XML Encryption
사용자 위장	홈 게이트웨이, 홈 서버	XML Signature

제시된 보안 대책들은 XML 기반의 보안 기술들을 포함하는 응용계층수준의 보안만을 고려한 것으로 보다 안전한 메시지 교환을 위해서는 전송계층 수준의 보안 대책이 함께 마련되어야 한다. 따라서 [그림 7]에서 메시지 교환 개체들인 각 구성요소들을 연결하는 지점 대 지점 (point-to-point)에 대해 기본적으로 SSL/TLS를 이용한 보안 통신채널을 구축하여 전송계층수준의 보안을 만족시키고 있다.

Ⅳ. 결 론

본 논문에서 제안한 SAML기반의 단일인증 아키텍처는 기존의 다양한 인증방법들을 수용하고 각 방법을 통해 생성된 사용자의 인증정보를 교환할 수 있는 방안을 제시한다. 제시된 방안은 모바일 및 유비쿼터스 서비스 환경에서 모바일과 홈 기기 간에 서로 다른 개체의 인증 및 인가 프로파일 정보를 교환할 수 있기 때문에 분산 환경 간 자원 공유 시 반드시 필요한 사용자 인증 및 인가에 관련된 보안 관리를 강화할 수 있게 한다. 특히, 제안된 아키텍처에서는 고도의 연산능력을 필요로 하는 보안정보의 전자서명 및 암복호 작업을 유선환경에 구성된 고성능의 기기로 전가하고 모바일 기기는 사용자의 인증을 검증할 수 있는 작은 문자열 형태의 arti-

fact를 보유하고 이를 사용자의 인증에 이용함으로써 낮은 컴퓨팅 능력과 기억용량의 한계 같은 모바일 기기의 성능적인 제약을 극복할 수 있게 한다.

참고문헌

[1] Q. He, P. Khosla, Z. Su, "A Practical Study on Security of Agent-Based Ubiquitous Computing," Lecture Notes in Computer Science 2631, 2003

[2] Digital Home Working Group, "Digital Home White Paper," http://www.dhwg.org/resources/DHWG_WhitePaper.pdf 2003

[3] A. Volchkov, "Revisiting Sigle Sign-On: a pragmatic approach in a new context," IT Professional, Volume: 3 Issue: 1 , pp. 39-45, Jan/Feb 2001

[4] T.A. Parker, "Single Sign On systems-the technologies and the products," European Convention on Security and Detection, pp. 151-155, 16-18 May 1995

[5] B. Pfitzmann, "Privacy in Enterprise Identity Federation - Policies for Liberty Single Signon," 3rd Workshop on Privacy Enhancing Technologies (PET 2003), Dresden, March 2003

[6] http://www.open-oasis.org

[7] OMA (Open Mobile Alliance) Web Services Enabler (OWSER): Core Specifications Draft Version 1.0 http://member.openmobilealliance.org/ftp/public_documents/mws/Permanent_documents

[8] T. Pilioura, A. Tsalgatidou, S. Hadjiefthymiades, "Scenarios of using Web Services in M-Commerce, ACM SIGecom Exchanges," Vol. 3, No. 4, pp. 28-36, January 2003

[9] B. Pfitzmann, B. Waidner, "Token-based web Single Sign On with Enabled Clients," IBM Research Report RZ 3458 (#93844), November 200)

[10] J.I. Jeong, D.K. Shin, D.I. Shin, K.Y. Moon, "Java-Based Singe Sing On Library Supporting SAML (Security Markup Language) for Distributed Web Services," Lecture Notes in Computer Science 3007, 2004

[11] B. Pfitzmann, B. Waidner, "Token-based web Single Sign On with Enabled Clients," IBM Research Report RZ 3458 (#93844), November 2002

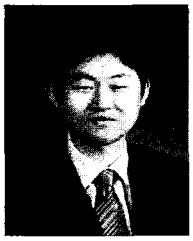
[12] V. Semar, "Single Sing On Using Cookies for Web applications., Proceedings," IEEE 8th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE '99), pp. 158 -163, 1999

[13] Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) V1.1: http://www.oasis-open.org/committees/security/

[14] WAPforum, "Wireless Application Protocol WAP 2.0," http://www.wapforum.org/what/WAP White_Paper1.pdf

〈著者紹介〉

손 민 우 (Son Min Woo)
학생회원
2003년 2월 : 상지대학교 전자계산공학부 졸업 (공학사)
2005년 2월 : 세종대학교 대학원 컴퓨터 공학과 석사
2005년 3월~현재 : 세종대학교 대학원 컴퓨터공학과 박사과정
관심분야 : XML 기반 생체인증, 정보보호, 홈네트워크 미들웨어, 개인화 서비스



정 종 일 (Jeong Jong Il)
학생회원
2002년 2월: 세종대학교 컴퓨터공학과졸업 (공학사)
2002년 8월 : 세종대학교 대학원 컴퓨터 공학과 졸업 (공학석사)
2004년 8월~현재 : 세종대학교 대학원 컴퓨터공학과 박사과정
관심분야 : 정보보호, 바이오인포메틱스, 홈네트워크 미들웨어

신 동 일 (Shin Dong Il)
정회원
1988년 2월 : 연세대학교 전산과학과 졸업 (이학사)
1993년 7월 : M.S. in Computer Science, Washington State University
1997년 8월 : Ph.D in Computer Science, University of North Texas
1997년 9월~1998년 2월 : 시스템공학 연구소 선임연구원
1998년 3월~현재 : 세종대컴퓨터공학 과 부교수
관심분야 : 홈 네트워크 미들웨어, 개인화 서비스 지능형 에이전트, HCI

신 동 규 (Shin Dong Kyoo)
종신회원
1986년 2월 : 서울대학교 계산통계학 과 졸업 (이학사)
1992년 8월 : Illinois Institute of Tech- nology 전산학과 졸업(공학석사)
1997년 8월 : Texas A&M University 전 산학과 졸업(공학박사)
1986년 2월~1991년 1월 : 한국국방 연구원 연구원
1997년 8월~1998년 2월 : 현대전자 멀티 미디어연구소 책임연구원
1998년 3월~현재 : 세종대학교 컴퓨터공 학과 부교수
관심분야 : 정보보호, 바이오인포메틱스, 홈네트워크 미들웨어, XML 기반 생 체인증