한국정보과학회

KIISE 2007 FALL CONFERENCE

KOREAN INSTITUTE OF INFORMATION SCIENTISTS AND ENGINEERS

2001
2002
2003
2004
2005
2006
2007
2008
2009

- Information
- Table of Contents
- Search This CD-ROM
- CD-ROM Help
- Exit

제 34 회 추계학술발표회

일시 : 2007년 10월 26일 ~ 27일
장소 : 부산대학교

http://www.KIISE.or.kr

2. 정보통신

유비쿼터스 환경에서 프라이버시 보호를 위한 동적 접근 제어 시스템

이제훈° 김상욱
경북대학교 전자전기컴퓨터학부
{newsky°, sykim}@woorisol.knu.ac.kr

A Dynamic Access Control System For Privacy Protection in Ubiquitous Environment

J.Lee° and S.Kim
School of Electrical Engineering and Computer Science
Kyungpook National University

요 약

유비쿼터스 환경에서 개인의 프라이버시를 최대한 보호하면서 개인 정보에 따른 서비스를 제공하는 것은 중요한 문제이다. 다양한 장치들이 유동적으로 움직이며 네트워크 서비스를 받고 다양한 컨텐츠를 제공하는 서비스를 요구하게 된다. 이때 개인의 정보에 따른 동적인 접근 제어와 프라이버시의 보장이 요구된다. 본 논문에서는 유비쿼터스 환경에서 개인의 프라이버시를 보호하면서 상황 인식(Context-Aware)에 따라서 장치와 컨텐츠를 제공하는 프레임 워크를 설계한다. 추가적으로 인증서를 통한 네트워크 통신의 보안을 제공한다.

1. 서론

유비쿼터스 환경에서 서비스의 주체들은 자동화된 기능을 제공하기 위하여 개인 정보를 서로 교류하고 보관하게 되었다[1-3]. 개인 정보보호를 위한 요구사항에는 프라이버시 보호 기능, 개인 정보 특성에 따른 처리, 프라이버시를 보호하는 접근 제어 등이 있다[4]. 이러한 요구 사항을 수용하기 위하여 사용자의 입력은 최소화하고 개인 정보의 전달은 자동으로 처리하면서 개인의 프라이버시를 보호할 수 있는 기술이 필요하다.

기존의 접근 제어 방식은 미리 정의된 정책과 개인이 제공하는 정보를 바탕으로 이루어졌다. 수동적인 접근 제어의 방식으로는 다양한 상황에 맞는 서비스를 제공하기 힘들다. 따라서 동적인 접근 제어 방식을 제공하여야 하며 이때 개인 정보의 관리를 통한 프라이버시의 보호가 중요하다.

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음 (IITA-2007-C1090-0701-0026)

본 논문에서는 자신의 홈 인증 서버를 두고 외부의 다른 도메인으로 이동하였을 때 해당 도메인과 동적인 협상을 통하여 사용자의 접근 제어를 하는 시스템을 제안한다. 이때 개인의 신상정보는 홈 인증 서버와의 미리 정의된 인증 코드를 이용하여 통신한다. 이는 개인이 누구인가를 확인할 수 없도록 하여 프라이버시를 보호한다.

본 논문의 2장은 기존의 접근 제어 방식을 분석하고 3장은 제안된 동적 접근 제어 방식에 대해 설명한다. 4장은 개인 정보 및 정책 전달을 위한 프로토콜을 설명한다. 마지막으로 5장에서는 결론과 향후 연구방향에 대하여 설명한다.

2. 관련 연구

2.1 중앙 집중 접근 제어

중앙 집중 접근 제어 시스템의 경우 하나의 도메인을 관리하는 중앙의 관리자가 존재하고 이 관리자에 등록된 정책에 따라서 접근 제어를 하게된다. 기존의 RBAC(Role-Based Access Control)과 같은 형태의 역할에 기반한 접근 제어가 가능하다[5]. 도메인은 관리하는

중앙의 서버에서 해당 도메인의 각 장치들이나 컨텐츠에 대한 접근 제어 정책을 설정할 수 있어 관리가 편한 장점이 있다. 그러나 이 방식을 통해서는 기존에 등록된 사용자가 그룹 형태의 정책 적용은 가능하지만 유비쿼터스 환경과 같은 다양한 장치와 사용자가 접근하고 컨텐츠 사용을 요구하는 환경에서는 적용이 어려운 문제점이 있다. 또한 개인 정보의 관리가 타 도메인의 중앙 서버에 할당되는 문제점이 발생하여 타 도메인의 관리자의 부실로 인한 개인 정보 유출이 발생할 수도 있다.

2.2 분산 접근 제어

기존의 UPnP처럼 각 장치들 간의 분산 접근 제어 방식은 클라이언트가 각 장치들과의 직접적인 통신을 통하여 사용자 인증을 하고 권한을 확인하는 방식이다[8]. 중앙의 서버를 거치지 않고 장치와 바로 통신하기에 중앙의 서버가 가지는 인증과 접근 제어에 대한 부하와 각각의 장치를 관리해야하는 부담이 줄어드는 장점이 있다. 그러나 이와 같은 방식은 사용자가 인증과 권한을 요청할 때 사용자의 입력이 요구되거나 각 디바이스에 인증과 권한에 대한 정책을 적용해야 하기 때문에 장치에 부하가 걸리고 일관된 정책을 적용하지 못하는 문제점이 발생한다.

2.3 Radius

Radius는 IETF 표준으로 정의된 RBAC의 일종으로 클라이언트 서버 구조의 서비스로 사용자의 인증과 장치에 대한 인증, 접근 권한 등을 제어할 수 있는 방식이다[7]. 이 서비스는 표준에 정의된 다양한 장치들에 대한 인증 방법을 제공한다. 주로 대형의 네트워크 접근 제어에 활용된다. 이후에 확장된 버전인 diameter등이 있다. 하지만 서비스 제공자가 컨텐츠의 접근 제어나 개인의 신상 정보를 이용한 동적인 접근 제어를 하기에 부족한 부분이 많다.

3. 프라이버시를 보호하는 동적 접근 제어 프레임워크

본 논문에서 제안하는 시스템은 사용자가 다른 도메인으로 이동하였을 때 자동으로 도메인에서 제공하는 서비스를 판별하고 미리 인증된 두 도메인간의 신뢰를 기반으로 사용자에게 서비스를 제공한다. 서비스 사용자가 관리하는 인증 및 접근 제어 정보를 관리하는 서버를 두고 개인이 사용하는 장치가 다른 도메인으로 이동하였을 때 동적으로 개인이 보유한 서버와의 협상을 통해 개인에게 맞는 서비스를 제공한다. 개인 정보의 유출은 개인이 누구인지 알 수 있을 때 적용되는 문제로 개인이 정확히 누구인지 알지 못하도록 시스템을 설계하면 해당 사용자가 접근한 접근 기록 등이 의미 있는 데이터가 되지 못한다.

3.1 시스템 구조

그림 1은 제안된 인증과 접근 제어의 시스템 구성도를 나타냅니다.

사용자가 타 도메인으로 이동하였을 경우 해당 네트워크를 사용하는 시스템을 나타냅니다. 하나의 도메인은 보안 관리자를 보유하고 있고 이 서버는 개인의 신상 정보와 접근 제어에 관한 정책을 미리 등록 하고 있다. 제안하는 시스템은 크게 2 부분으로 구성된다. 내부적으로는 개인 정보를 관리하고 인증 정보를 관리하는 기능을 하는 인증 관

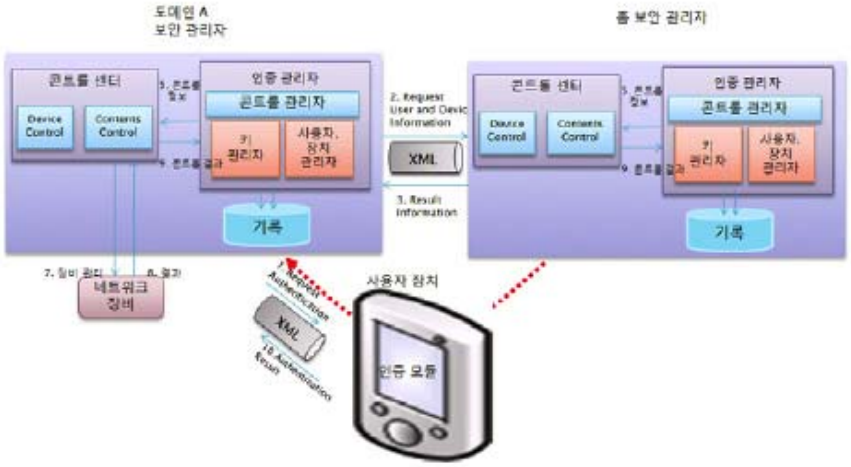

그림 1 시스템 구조도

리자와 해당 도메인이 보유하고 있는 각 장비들과 컨텐츠를 관리하는 콘트롤 센터로 나뉜다. 사용자는 개인의 장치를 통해서 서비스를 제공받고 개인의 장치는 보안 모듈을 통해서 이동한 도메인의 보안 관리자와 통신하게 된다.

보안 관리자의 인증 관리자는 인증 정보와 개인 정책에 관한 정보를 보유하고 다른 서버와의 협상하는 역할을 한다. 사용자의 관리는 사용자의 식별코드와 사용하는 장치의 기기 등록 코드 등의 장치 정보와 성별, 나이 등의 개인 신상 정보를 등록하는 것과 타 도메인의 개인 정보 요청에 따른 정책과 해당 사용자의 사용 허가 범위를 등록하는 것을 뜻한다. 따라서 장치에 따른 인증서를 발급하여 사용자의 인증을 대체한다. 또한 외부의 사용자가 접근을 요청할 때 임시 인증서를 발급하는 역할도 하게 된다. 사용자는 인증서가 만료되기 전까지는 해당 인증서를 통하여 이동한 도메인의 여러 장치나 컨텐츠를 사용할 수 있으며 인증서가 만료되면 다시 인증서 발급 절차에 따라서 발급 받도록 한다.

콘트롤 센터는 보유한 다양한 장치와 컨텐츠의 사용을 조절할 수 있도록 한다. 다양한 장치와 컨텐츠가 존재하기 때문에 인증 서버와 분리하여 다양한 정책에 따른 접근 제어가 가능하도록 한다. 네트워크의 접근 제어나 컨텐츠의 허용 범위에 따른 접근 제어가 요구된다. 네트워크의 접근 제어는 다른 도메인의 네트워크를 통한 DDOS 등의 공격 등을 사전에 막도록 하는데 중요한 기능을 할 수 있다.

3.2 동작

각 도메인의 보안 관리자는 인증 관리자로부터 인증되어 신뢰한다는 것을 가정한다. 그림 2는 사용자가 다른 도메인에서 임시 인증서를 발급받고 자신의 홈 보안 관리자를 통해서 동적인 접근 제어를 받는 과정을 나타낸다.

사용자는 이동한 도메인(A 도메인)에 임시 인증서를 요청하고 발급받은 임시 인증서를 이용하여 암호화된 통신을 하여 네트워크를 통한 정보의 유출을 막도록 한다. 이러한 통신은 이동한 도메인에서 제공하는 서비스 검색 프로토콜을 이용하여 서비스를 판별한다[8]. 이 임시 인증서는 만료기간을 두어 만료 기간 전까지는 해당 인증서를 통하여 접근을 허용 받을 수 있도록 한다. 사용자는 자신의 홈 도메인에서 발급받은 인증서를 포함하는 인증 요청을 통하여 A 도메인에 인증을 요청한다. A 도메인의 인증서버는 해당 인증서를 검증하고 사용자의 개인 정보가 등록된 홈 인증 서버에게 요청한다. 요청을 할 때는 사용자가 보내온 인증 코드로 인증을 요청하게 된다. 따라서 사용을 요청하는 개인이 정확히 누구인지 이동한 도메인은 알 필요가 없게 되는 것이다. 홈 인증 서버는 요청 받은 개인 정보 요청의 인증 코드를 통하여 해당 요청이 정상적인 요청임을 확인하고 요청받은 항목

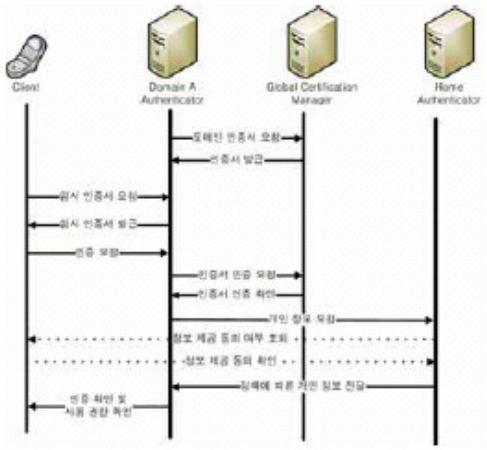

그림 2. 동작 흐름도

에 대하여 정책에 따른 접근 허용 여부를 알려준다. 이때 홈 인증 서버는 인증 요청에 대하여 로그를 남겨서 추후의 자신의 사용 내역 등을 확인 할 수 있도록 한다. 이는 장치의 도용을 통한 불법적인 사용을 막기 위한 정책이다. 또한 이 로그를 통하여 만약 홈 서버에서 발급한 사용자의 인증서가 유출되거나 도용되었을 경우 로그에 기록된 서버들 중 임시 인증서가 만료되지 않은 도메인 서버로 임시 인증서 만료를 알리는 기능을 하도록 한다.

개인 정보 및 접근 정책을 요청받은 홈 인증 서버는 미리 정의된 정책에 따라서 자동으로 정보를 확인해주거나 수동으로 사용자에게 허용 여부를 확인하도록 한다. 이는 사용자가 원치 않은 정보를 요청하였을 때는 거부할 수 있도록 하기 위함이다. 사용자는 자신의 정보를 전달해도 괜찮은 곳의 리스트나 정책을 미리 홈 인증 서버에 등록한 사용자의 입력 없이도 자신의 정보를 전달해줄 수 있다. 전달 받은 개인 정보와 정책, 그리고 해당 도메인의 정책에 따라서 장치나 컨텐츠의 서비스를 제공한다. 이때 고려해야하는 요소는 성별, 나이, 환경, 목격 등에 따른 접근 정책이 적용되어야 하며 우선순위 등을 두어 처리할 수도 있어야 한다.

이 시스템에서 개인의 정보를 확인하는 것은 개인이 보유하고 있는 장치에 발급된 인증서를 통하게 된다. 하지만 이 장치가 분실이나 도난 되었을 때는 홈 인증 서버를 통해서 인증서를 만료하고 사용을 중지 시킬 수 있어야 한다. 또한 로그를 확인하여 원격의 도메인에서 발급된 임시 인증서도 같이 만료 시킬 수 있도록 한다.

4. 개인정보 및 정책 전달 프로토콜

본 시스템에서는 개인 정보와 정책의 요청은 그림 3과 같은 XML 문서를 정의하여 처리한다.

```
<?xml version="1.0" encoding="utf-8"?>
<Client>
    <AuthCode>4302c7ea82602e88d91a3d5..</AuthCode>
    <ExpireDate>2007-07-31 23:59:59</ExpireDate>
    <RequestAge>true</Request>
    <RequestPermission>true</Request>
</Client>
```

그림 3. 정책 요청 프로토콜

정보의 요청은 해당 도메인에서 필요로 하는 정보에 대하여 질의하고 해당 질의에 맞추어 기존에 등록된 정책에 따라서 확인해준다. 위와 같은 형식을 통하여 향후 확장된 인증 서비스를 제공할 수 있도록 한다.
그림 4는 요청된 개인 정보와 정책에 대해서 Home Authenticator 가 전달하는 정보이다. 개인의 신상을 확인 할 수 있는 내용은 포함하지 않도록 하여 프라이버시 문제를 해결하도록 한다. 개인을 식별하는 것은 Home Authenticator이므로 미리 생성한 인증서와 사용자키를 이용하도록 한다. 접근 허용에 대한 정책은 성인 컨텐츠의 경우에는 나이 접근 제한 등에 대하여 설정하여 미성년자의 사용을 막도록 한다. 또한 유효 기간을 두어 Home 서버에서도 해당 일시 인증서의 유효 기간을 인지할 수 있도록 한다.

```
<?xml version="1.0" encoding="utf-8"?>
<Server>
    <AuthCode>4302c7ea82602e88d91a3d5..</AuthCode>
    <Age>19</Age>
    <Permission>
        <Video>allow</Video>
        <Audio>deny</Audio>
    </Permission>
</Server>
```

그림 4. 정책 응답 프로토콜

5. 결론 및 향후 연구

본 논문에서 유비쿼터스 환경에서 프라이버시를 보장하는 동적 접근 제어를 위한 프레임워크를 설계하였다. 다양한 장치들에서 사용자의 상황에 따라 동적인 권한을 할당받아 접근 제어를 할 수 있다. 이때 미리 인증된 도메인 서버들 간의 협상을 통하여 사용자가 누구인지를 다른 도메인 서버는 알 필요가 없도록 하여 개인 정보 유출을 막는다. 또한 사용자가 허용하는 범위를 정책을 통해서 입력해둠으로써 유비쿼터스 환경에서 편리성과 보안성을 제공하게 된다. 또한 네트워크 통신은 암호화를 통하여 개인 정보가 네트워크를 통해 유출되는 것을 막는다.

향후에는 이 설계를 바탕으로 유비쿼터스 환경에서 UPnP를 이용한 컨텐츠 이용 등에 적용시킬 계획이다. 또한 개인 정보와 위치 정보 등의 상황을 이용하여 동적인 협상하고 이를 서비스 제공에 반영할 수 있는 기술 개발을 해야 한다.

6. 참고 문헌

[1] R.Butler, V.Welch, D.Engert, I.Foster, S.Tuecke, J.Volmer, C.Kesselman, "A national-scale authentication infrastructure," Computer, Vol 33, Issue 12, pp. 60-66, Dec. 2000
[2] E. Gustafsson and A. Jonsson, "Always best connected," IEEE Wireless Communication., Vol. 10, no. 1, pp. 49-55, Feb. 2003
[3] S.Frank ,"Security for Ubiquitous Computing", WILEY, March 2002
[4] 송유진, 이동혁, 남택용, 장종수, "유비쿼터스 환경에서 프라이버시보호의 기술적 요구사항과 프레임워크", 정보보호학회지, 16권, 2호, pp. 56-61, 2006
[5] R.S. Sandhu, E.J. Coyne, "Role-Based Access Control Models," Computer, Vol 29, Num 2, pp.38-47, Feb. 1996
[6] UPnP, http://www.upnp.org
[7] RADIUS, http://www.ietf.org/rfc/rfc2865.txt