Jabber/XMPP기반 분산 워크플로우 시스템의 도메인간 인증

남원식*, 이이섭*
*금오공과대학교 컴퓨터공학과
e-mail:{eruill, eesub}@kumoh.ac.kr

An Inter-Domain Authentication for Jabber/XMPP based Distributed Workflow System

Weon-Sik Nam*, Lee-Sub Lee*
*Dept of Computer Engineering, Graduate School of Industry Kumoh National Institute of Technology

요 약

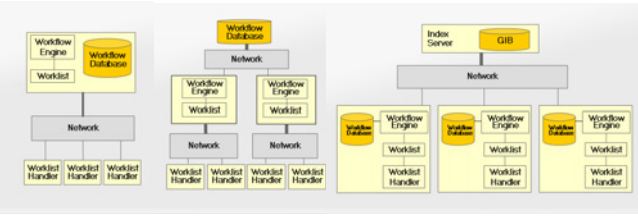
효율적인 업무향상을 위한 워크플로우 표준모델이 WfMC(Workflow Management Coalition)에서 제시해 개발되어지고 있다. 중앙집중식 워크플로우나 분산 워크플로우, P2P기반 워크플로우등 많은 모델이 개발되어 있으나 문제점들이 존재하고 있다. 중앙집중식 워크플로우의 서버에 과도한 업무처리 집중현상이나, 분산 워크플로우의 데이터 병목현상, P2P 워크플로우의 Disconnected현상을 해결하는 방안으로 분산 워크플로우 시스템의 개념을 도입한 Jabber/XMPP기반 분산 워크플로우 시스템의 도메인 간 인증(Inter-Domain Authentication) 메커니즘을 제안하고자 한다.

1. 서론

효율적인 업무향상을 위한 워크플로우 모델 연구가 WfMC(Workflow Management Coalition)에서 표준을 제시해 활발히 진행되고 있다. 워크플로우란 비즈니스 프로세스를 GUI(Graphic User Interface)도구를 이용해 설계하고 설계된 프로세스를 자동으로 운영해 줄 수 있는 환경을 제공하는 기술로써 기업의 업무 처리나 공공단체의 업무처리 등에 쓰이고 있다. 워크플로우 시스템이란 어떤 현상이나 풀고자 하는 문제 자체를 형상화 한 것을 의미 하며, 사용자 혹은 클라이언트가 어떤 일을 해야 할지 직접 찾지 않고 사용자가 처리해야 할 작업들을 시스템이 제시해 준다는 것이 최대의 장점이다.

현재 기업의 업무처리는 워크플로우에 의존해 진행되어지는데, 업무의 증가 또는 새로운 워크플로우 시스템의 증설 등으로 업무처리 시 지연이 생기거나 지원이 안 되는 경우 문제가 발생한다. 기업에 대부분의 업무처리를 워크플로우로 진행하기 때문에 워크플로우의 지연이나 고장 등은 금전적으로나 시간적으로 많은 낭비와 손해를 가져오게 된다. 비록 분산 워크플로우 시스템이나 P2P기반 워크플로우 시스템 등이 업무처리 능력을 향상시키고 보안적으로 안정되어있다고는 하나 나름대로의 문제점을 갖고 있다.

<그림 1>은 워크플로우 모델들을 나타내고 있다. 중앙집중식 워크플로우의 경우 구조상 서버가 존재하여 모든 업무를 서버처리하기 때문에, 업무가 증가할 때 마다 그만큼의 업무처리에 지연이 생긴다. 또한 분산 워크플로우의 경우 n+1개의 서버를 가지고 업무를 각자의 서버에서 실행하기 때문에 작업처리 효율이 뛰어나지만, 데이터베이스에서 관련데이터를 받아 오기 때문에 병목현상이 발생하여 보안성이 떨어지는 Single Point of Failure를 일으킨다. P2P모델의 경우 서버가 없이 Peer들이 업무를 분할하여 처리하므로 업무처리 효율이 분산구조보다 뛰어나지만, Peer가 Disconnected시 관련 업무를 처리를 위한 인증을 할 수가 없어 안정성이 떨어지는 문제점이 있다.



<그림 1> 중앙집중식, 분산, P2P 기반 워크플로우 모델

이에 본 논문은 기존의 워크플로우 시스템들이 가지는 문제점들을 해결하는 방안으로 한 영역의 클라이언트가 다른 영역의 서버에 접근이 가능하게 하는 Jabber/XMPP 기반 분산 워크플로우 시스템의 도메인 간 인증 메커니즘인 IDA(Inter-Domain Authentication)를 제안하고자 한다.

관련 연구는 워크플로우에 쓰이는 PKI 기반 인증방식과 논문에서 제안하는 IDA 기반 인증방식을 비교 정리한다. 마지막으로 본 시스템과 유사한 Kerberos의 IRA에 대해 알아보고자 한다.

2. 관련 연구

2.1 PKI 기반 인증방식

PKI 기반 인증방식은 XML 전자서명에 이용되고 있다. <그림 2>에서 PKI의 기본구조를 살펴보도록 하자. 이 그림에서 수신자의 공개키와 개인키는 인증기관으로부터 제공 받는다. 그림을 통해 알 수 있듯이 PKI 인증 방식은 공개키 값의 안전하고 효율적인 전송을 위해 인증서를 발행, 획득, 조회, 검증 등을 수행하는 인증서 관리 기반 구조를 말한다. 공개키 암호화 알고리즘은 문서를 실제 사용하게 될 수신자의 공개키로 암호화하게 되고 수신자는 자신의 개인키로 축약문을 복호화해서 문서의 변조 여부를 알 수 있다. PKI 인증 방식은 전자서명 애플리케이션에서 무결성, 부인봉쇄, 인증 증의 보안 서비스를 효율적이고 안정적으로 제공하는 것을 목적으로 하고 있다. 또한, PKI 는 비대칭키를 사용하고 있다. 이는 보안성 측면에서 보면 개인키와 공용키를 사용함으로써 강력한 암호화 기능을 제공하고 있다. 비대칭키 알고리즘은 암호화하는 암호화키와 암호문을 원래의 데이터로 바꿔주는 복호화 키가 다른 알고리즘을 의미한다. [3]

<그림 2> PKI 인증 방식

2.2 IDA 인증방식

IDA는 대칭키를 사용함으로써 <그림 3>과 같이 수행된다. 특정 클라이언트만이 복호화할 수 있는 개인키 방식의 암호화를 제공하고 있다. 대칭키 알고리즘은 데이터를 암호화하는 암호화키와 암호문을 원래의 데이터로 바꿔주는 복화화키가 같은 알고리즘을 의미한다.

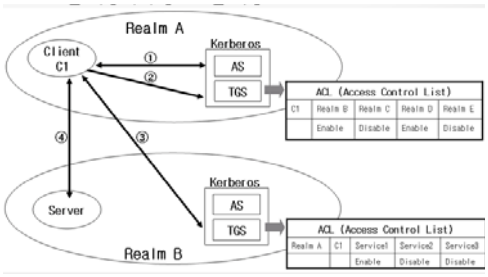
PKI의 암호화 속도는 인증기관에 대해 공개키를 제공받고 암호화하고 복호화 하는 과정으로 인해 암호화의 시간이 오래 걸리며 인증기관의 설치로 인한 비용이 증가되며 별도의 인증기관에서 상호인증을 위한 비대칭키를 사용함으로써 중앙집중식의 문제점인 Single Point of Failure의 문제가 발생하기 때문에 안정성이 문제가 된다. 반면 IDA의 암호화 속도는 PKI에 비해 상대적으로 빠른 암호화를 제공하고 있다. IDA는 특정 클라이언트에 대한 신속하게 접근할 수 있고 인증기관의 미설치로 인한 비용절감과 Single Point of Failure의 관리가 필요 없다. [3]

<그림 3> IDA 인증 방식

2.3 Kerberos의 IRA

현재 Jabber에서 잘 알려진 Kerberos[4]는 IRA(Inter-Realm Authentication) 방식으로 도메인간의 데이터 교환 시 같은 Kerberos 환경이 아니면 정보교환이 어려운 형태로 되어 있다. Kerberos 환경에 대해 살펴보기 위해 <그림 4>과 같이 표현하였다. 다음은 Kerberos IRA 수행과정을 나타내고 있다. 첫 번째 단계로, 클라이언트가 Kerberos에 접속한다. 두 번째 단계로, 클라이언트가 원격 영역에 접속을 위한 티켓을 확보한다. 세 번째 단계로, 클라이언트가 원격 Kerberos로부터 원격 영역의 서비스 사용티켓을 확보한다. 네 번째 단계로, 티켓을 사용하여 서비스에 접속한다. 이에 대하여 어떤 문제점이 있는지를 분석해 보기로 하자. 첫 번째로 지역영역과 원격영역이 모두 Kerberos로 구성되어야 하는 문제점이 있다. 두 번째로 클라이언트가 원격영역에 접속을 위한 티켓을 확보한 경우 영역의 개수가 매우 많기 때문에 모든 도메인이 Kerberos만을 위한 인증 메커니즘으로 사용한다고 가정을 해도, 지역 Kerberos가 모든 클라이언트에 대한 원격영역의 접근 권한 리스트를 유지하기가 어렵다. [5,6] 위의 첫 번째 문제점 해결을 위해 IDA를 적용함으로써 Jabber에 존재하는 다양한 인증 메커니즘 사용에 대한 문제점을 해결할 수 있다.

Jabber 환경에서의 수많은 도메인의 존재로 인해 문제점이 발생하고 있다. 이 문제점을 IDA를 적용하여 필요시 서버 간에 상호인증을 맺음으로 해결할 수 있다.



<그림 4> Kerberos의 IRA

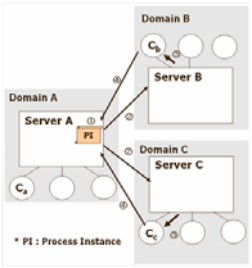
3. Jabber/XMPP기반 분산워크플로우의 IDA 제안

Jabber는 임의의 두 지점 사이에서 메시지와 프리젠스를 실시간 교환하기 위한 XML 기반 오픈 소스 프로토콜이다. Jabber는 인터넷 표준 기술 선정을 관리하는 IETF(Internet Engineering Task Force)의 IESG(Internet Engineering Steering Group)에서 Jabber 인스턴트 메신저와 관련된 인터넷 초안(Internet draft)을 검토하여 XMPP(Extensible Messaging and Presence Protocol)의 핵심부분인 XMPP-core를 Jabber 표준으로 채택하였다. [7]

제안하는 Jabber/XMPP 기반 분산 워크플로우는 P2P 기반 워크플로우의 문제점인 Disconnected를 해결하는 방법으로 Jabber/XMPP의 프리젠스 기술을 사용한다. 또한 업무처리의 효율을 높이기 위해 분산 워크플로우

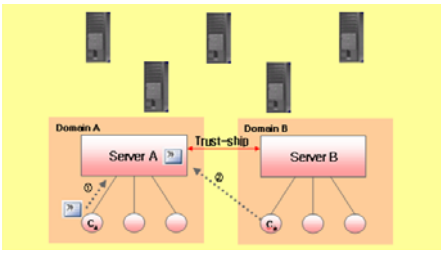
시스템의 골격을 유지하고 안전성과 보안성을 높이기 위해 인증 방식으로 최경선, "재버를 위한 도메인간 인증메카니즘"의 IDA를 제안한다. [3]

기존의 일반적인 Jabber 기반 워크플로우 시스템을 구현한다고 가정해 보자. 분산 워크플로우 시스템의 시나리오는 다음과 같이 표현할 수 있다. Jabber 환경에서 다른 도메인 간의 협업을 위해서 도메인 A의 서버 A는 도메인 B의 서버 B와 도메인 C의 서버 C와 함께 워크플로우 Pi데이터를 교환하여 작업을 수행하고자 한다. 이때 분산 워크플로우 시스템은 <그림 6>과 같이 나타낼 수 있다. 여기에서 C_a, C_b, C_c는 클라이언트를, A와 B 그리고 C는 서버를 의미한다. 또한, Pi는 프로세스 인스턴트를 나타내고 있다. <그림 6>에서 알 수 있듯이 첫 번째 단계로, C_a는 C_b, C_c가 참여하는 Pi를 생성한다. 두 번째 단계로, C_b와 C_c는 A에 저장된 Pi를 직접 접근할 수 없기 때문에 B와 C에 Pi 복사가 이루어진다. 세 번째 단계로, 각 클라이언트 자신이 소속된 서버에 중복된 Pi데이터를 사용한다. 네 번째 단계로, 각 클라이언트가 중복된 데이터를 독립적으로 갱신할 수 있으므로 동기화가 필요하다. 기존 시스템의 문제점은 다음과 같다. 워크플로우 시스템의 경우 파일 전송의 경우와 같이 전송량의 문제와 중복되는 데이터가 저장 공간을 사용함으로써 저장 공간 사용량이 불필요하게 증가 된다. 또한 동기화의 문제로 n개의 Pi가 중복되어 각 클라이언트가 동시변경이 가능하므로 동기화 문제가 발생하게 된다. 그러므로 현재의 워크플로우 시스템을 살펴보면 보안 문제가 발생하고 있음을 알 수 있다. 여러 도메인에 복사된 Pi데이터는 모든 서버에 중복 되어 사용함으로써 보안유지의 어려움이 발생하게 됨을 알 수 있다. [3]



<그림 6> IDA를 적용한 분산 워크플로우 시스템

제안하는 IDA(Inter-Domain Authentication)는 <그림 7>과 같이 한 영역의 클라이언트가 다른 영역의 도메인 서버에 속한 클라이언트와 협업이 가능하도록 하기 위해서, 필요시에 클라이언트가 속한 서버와의 Trust-ship을 통해 집적접근이 가능하다. 이러한 특징을 가지고 있기 때문에 위의 분산 워크플로우 시스템이 가지는 문제점인 데이터 중복의 문제를 해결할 수 있다. 또한 해당서버에 집적 접근함으로써 동기화 문제를 해결할 수 있고, 단일 Pi데이터 관리로 보안에 용이하다. 따라서 IDA를 적용함으로써 훨씬 용이한 분산 워크플로우를 개발 가능하게 되며 프로세스 공유에 있어 발생하는 문제점을 해결할 수 있다.



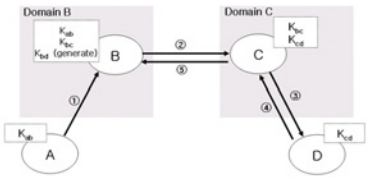
<그림 7> IDA 구성도

4. BAN Logic을 이용한 IDA 검증

IDA를 검증하기위해 BAN Logic을 사용하였다. BAN Logic은 Burrows, Abadi, Needham에 의해서 1989년에 제안된 로직으로 인증 프로토콜을 검증하는 방법으로 자주 사용되고 있다. [8] 정형화된 형태로 인증 시스템을 표현할 수 있는 표기법(Notation)들이 주어지고, 직관적으로 납득이 가는 기본 가정과 규칙을 근거로 인증 시스템의 신뢰성을 검증하게 된다. [9] BAN 논리는 믿음(Belief)에 관한 논리로써 적은 수의 추론규칙을 통해 많은 인증 프로토콜의 목적 유무를 추론할 수 있다. [10]

BAN Logic의 검증절차는 아래와 같다. 첫 번째 단계로, 프로토콜단계에서는 인증프로토콜의 개념을 기반으로 각 메시지를 논리적 형식으로 변환하여 표현한다. 두 번째 단계로, 이상화 단계에서는 프로토콜단계에서 BAN Logic에 적용이 용이하도록 변환하여 표현한다. 세 번째 단계로, 초기가정으로써 메시지가 전송되기 전에 필요한 사전 조건을 기술하며, 이를 통해 검증을 위한 규칙들을 적용한다. 네 번째 단계는 결과로써 초기가정의 메시지를 다양한 규칙을 통해 산출한 결과를 기술하게 된다.

.



<그림 8> Jabber/XMPP기반 분산 워크플로우 모델의 IDA 검증 절차

논문에서 제시하는 Jabber/XMPP기반 분산 워크플로우 모델의 IDA 흐름도는 <그림 8>와 같다. 이를 프로토콜단계로 나타내면 아래와 같은 형태로 표현할 수 있다.

Message 1. A→B:{A, B, C, D {T} K_{ab}}K_{ab}
Message 2. B→C:{A, B, C, D, AD_b, {T} K_{ab}, K_{bd}}K_{bc}
Message 3. C→D:{A, B, C, D, AD_b, {T} K_{ab}, K_{bd}}K_{cd}
Message 4. D→C:{A, B, C, D, AD_d, {T} K_{ab}, K_{bd}}K_{cd}
Message 5. C→B:{A, B, C, D, AD_d, {T} K_{ab}, K_{bd}}K_{bc}

여기에서 AD_x는 참여자$_x$의 물리적 IP주소를 의미하며,

K_{ab}는 참여자 A와 B의 공유키를 표현한 것이다. BAN Logic을 적용하기 위하여 프로토콜 단계를 다음과 같이 이상화 하였다.

Message 1. A→B:{A, C, {T}, K_{ab}}K_{ab}

Message 2. B→C:{A, C, AD_b, {T} K_{ab}, B$\overset{K_{bd}}{\longleftrightarrow}$D}$K_{bc}$

Message 3. C→D:{A, C, AD_b, {T} K_{ab}, B$\overset{K_{bd}}{\longleftrightarrow}$D}$K_{cd}$

Message 4. D→C:{A, C, AD_d, {T} K_{ab}, B$\overset{K_{bd}}{\longleftrightarrow}$D}$K_{cd}$

Message 5. C→B:{A, C, AD_d, {T} K_{ab}, B$\overset{K_{bd}}{\longleftrightarrow}$D}$K_{bc}$

Jabber/XMPP기반 분산 워크플로우 모델의 IDA 초기 가정은 아래와 같다.

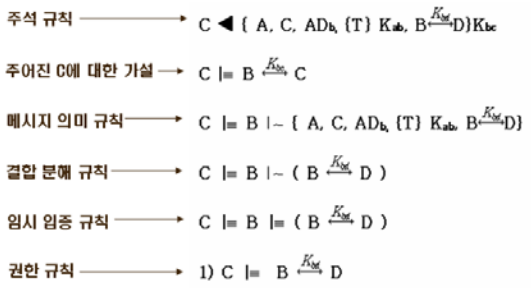
$$A| \equiv A \overset{K_{ab}}{\longleftrightarrow} B,\ B| \equiv B \overset{K_{bc}}{\longleftrightarrow} C,\ B| \equiv A \overset{K_{ab}}{\longleftrightarrow} B$$

$$C| \equiv B \overset{K_{bc}}{\longleftrightarrow} C,\ C| \equiv C \overset{K_{cd}}{\longleftrightarrow} D,\ D| \equiv C \overset{K_{cd}}{\longleftrightarrow} D$$

$$B| \equiv B \overset{K_{bd}}{\longleftrightarrow} D$$

$$D| \equiv (B| \Rightarrow B \overset{K_{bd}}{\longleftrightarrow} D),\ C| \equiv (B| \Rightarrow B \overset{K_{bd}}{\longleftrightarrow} D)$$

제시된 초기가정의 내용을 정리해 보면, Jabber/XMPP기반 분산 워크플로우 모델의 IDA에서 Jabber C2S(Client to Server)인증으로 클라이언트 A는 서버B에 로그온 되어 있고, 클라이언트 D는 서버 C에 로그온 되어 있다. 그리고 각 서버는 자신의 클라이언트를 관리한다. 즉, 서버 B는 클라이언트 A의 권한을 가지며, 서버 C는 클라이언트 D에 대한 권한을 가진다. IDA 적용을 위해서 서버 B는 공유키인($\overset{K_{bd}}{\longleftrightarrow}$)를 생성하게 된다. 클라이언트 A가 서비스를 기동시키고 서버 B가 서비스를 제공하는 주체이기 때문에, B가 서비스의 사용권한(Ticket)을 생성한다. 이를 통해 서버 B와 서버 C의 상호 신뢰함을 증명한다. 초기가정을 통해 다양한 규칙을 적용하여 <그림 9>과 같이 검증한다.



<그림 9>Message 2. B→C:{A, C, AD_b, {T} K_{ab}, B$\overset{K_{bd}}{\longleftrightarrow}$D}$K_{bc}$ 에 대한 검증

<그림 9>과 같은 방법으로 전체 메시지에 대한 검증을 수행하면 서버 B와 서버 C는 상호 신뢰한다는 것을 알 수 있다. 즉 필요시에 Trust-ship을 맺는다.

5. 결론

효율적인 업무향상을 위해 워크플로우 개발이 활발하게 진행되고 있다. 현재 워크플로우의 표준 모델을 WfMC에서 제시하였다. WfMC모델은 5가지 인터페이스를 가지고 있다. 그중 인터페이스 4는 외부의 또 다른 워크플로우 시스템과의 상호운영성을 보장하는 API로써 현재까지 만족할만한 방안은 제시되고 있지 않은 실정이다.

본 논문에서는 분산 워크플로우 시스템을 위한 Jabber/XMPP 기반 분산 워크플로우 시스템의 도메인간 인증(IDA)을 제시해보았다. 기존 분산 워크플로우 시스템이 가지는 병목현상을 IDA를 적용하여 해결함으로써 확장성과 안정성을 제공하였고, IDA를 적용하여 인증기관의 증설이 필요 없고, 관리가 단순화된 워크플로우간 협업모델을 제시하였다. 또한, 본 논문에서 제시한 IDA를 보안검증에 널리 사용되고 있는 BAN Logic을 통해 검증해보았다.

참고문헌

[1] 이이섭, 박수현, 백두권 “A Workflow Enactment Model for Next Generation Service″, 2004. 6, IEICE(SCIE)

[2] 이이섭, “A Hybrid P2P based Workflow Enactment Model″, ACIS SERA 2005

[3] 최경선, “재버를 위한 도메인간 인증 메카니즘”, 공학석사학위논문, 2006. 6

[4] J. G. Steiner, B. C. Neuman, J. I. Schiller, ″Kerberos: An Authentication Service for Open Network System″, Usenix Conference Proceedings, Dallas, texas, February 1988.

[5] M. Steven, ″Limitations of the Kerberos Authentication System″, AT&T Bell Laboratories.

[6] J. T. Kohl, B. C. Neuman, Y. T. Theodore, ″The Evolution of the Kerberos Authentication Service″, Digital Equipment Corporation.

[7] P. S. Andre, ″Extensible Messaging and Presence Protocol (XMPP)″, IETF proposed standard, RFC 3920, October 2004, www.ietf.org/rfc/rfc3920.txt.

[8] J. Mitchell, ″Logic for Computer Security Protocol″, Stanford University.

[9] 두소영, “신뢰성이 있는 사용자 인증 시스템과 안정성 분석”, 2003.

[10] 주성범, 홍주형, 김종훈, “인증 프로토콜 분석을 위한 개선된 BAN 논리”, 2003.