한국산학기술학회논문지
Vol. 9, No. 5, pp. 1271-1278, 2008

협업 기반 워크플로우 관리시스템의 보안 프로토콜 설계

최명길[1], 이동호[2], 황원주[3*]

Design on Security Protocols Reflecting Collaboration in Workflow Management Systems

Myeonggil Choi[1], Dongho Lee[2], and Won-Joo Hwang[3*]

요 약 워크플로우 관리시스템이 폭넓게 사용됨에 따라 조직간의 협업이 증가하고 있다. 워크플로우 시스템의 협업이 증가함에 따라 보안의 중요성이 강조되고 있다. 사용자 인증·워크플로우 시스템간의 안전한 통신 기능 등의 보안 기능은 인터넷상에서 워크플로우 관리시스템의 운영에 영향을 미치고 있지만, 워크플로우 시스템은 협업을 기반으로 보안 프로토콜이 제공되지 않은 실정이다. 따라서 본 논문은 워크플로우 관리시스템의 협업기반 보안 프로토콜을 제안한다. 협업 기반 보안 프로토콜의 제안을 위해서 본 논문은 워크플로우 관리시스템의 보안요구사항을 분석하고, 보안요구사항을 바탕으로 보안 아키텍쳐와 보안 프롵토콜을 제시한다.

Abstract As the collaboration of WFMS(workflow management systems) in enterprises increases, security protocols could be considered a critical factor affecting secure operation of WMFS. The security protocol of WFMS could not reflect the nature of collaboration in WFMS, resulting to collaboration of WFMS on Internet causing the operation problems of WFMS. This study suggests collaboration based security protocols based on the collaboration of WFMS on Internet. To reflect the nature of collaboration in WFMS, this study analyzes security requirements for WFMS. Based on security requirements, this study suggests a security architecture and security protocols for WFMS using security agents.

Key Words : Workflow Management System, Agent, Security Requirements, Architecture, Security Protocols

1. 서론

프로세스 중심의 업무처리의 효율성 등으로 인하여 보건, 국방, 전자상거래 등과 같은 영역에서 워크플로우 관리시스템(workflow management systems: WFMS)이 채용되고 있다. 특히 WFMS가 인터넷에서 원거리 조직간에서 협업이 가능해짐에 따라 안전한 워크플로우 관리시스템의 운영이 중요하다[4,8]. 특히 상이한 IT 환경과 기술적 선호도로 인해 조직마다 다른 보안체계를 가진 WFMS를 도입하고 있는 실정이다[1,8]. 특히 인터넷의 발달은 조직간 협업을 증가시키고 있으며, 협업의 증가는 WFMS의 보안 취약성을 심화시키고 있다. 이와 더불어 WFMS를 구성하는 서브시스템(sub-systems)은 물리적으로 분리된 지역에서 운영됨으로 WFMS의 효과적인 보안대책 수립이 필요하다[6,7,13].

WFMS의 보안 프로토콜은 다음과 같은 두 가지 방향으로 개발한다. 첫째, 본 연구는 WFMS의 협업의 특성을 반영한 협업 기반의 보안 프로토콜을 제안한다. WFMS는 동시에 많은 사용자가 협업을 수행하지만, WFMS의 보안 프로토콜은 협업의 특성을 반영하지 못하고 있다. 결과적으로 기존의 보안 프로토콜은 WFMS의 협업을 어렵게 한다. 둘째, 본 연구는 다른 개발자가 공급한 WFMS간 상호 연동이 가능한 보안 아키텍쳐를 제안한다. 다른 공급자가 개발한 WFMS는 다른 시스템 구조를 가지고 있어 상호 연동이 어렵다[5]. 따라서 본 연구는 이종 WFMS간 상호 운영성을 확보하기 위하여 에이전트 기반(agent-based)의 보안 아키텍쳐를 제안한다. 에이전트는 이종 WFMS 환경에서 쉽게 구현이 가능하여, WFMS

[1]중앙대학교 조교수 (주저자)
[2]경상대학교 조교수
[3]인제대학교 조교수
*교신저자: 황원주(ichwang@cau.ac.kr)
접수일 08년 08월 18일 수정일 08년 10월 14일 게재확정일 08년 10월 16일

보안 프로토콜에 적합한 방식이다. 본 연구는 협업 기반의 보안 프로토콜 및 아키텍처를 개발하기 위해서 WFMS의 보안요구사항을 분석한다.

본 연구는 WFMS의 협업 프로토콜을 그룹 커뮤니케이션(group communication)으로 간주한다. 개별 WFMS를 그룹 커뮤니케이션에 참여하는 구성원과 동일하다. 즉 그룹 커뮤니케이션은 동적으로 구성원이 커뮤니케이션에 참여하고, 탈퇴할 수 있으며, 참여와 탈퇴를 위해서는 보안 프로토콜이 필요하고, 그룹 커뮤니케이션에서 특정 구성원들간의 통신은 비밀이 유지된다는 특성을 가지고 있기 때문이다. 협업과 그룹 커뮤니케이션을 수행하는 동안 발생하는 보안문제를 자세히 살펴보면 다음과 같다. 첫째, 그룹 커뮤니케이션과 협업에 참여하는 개별 WFMS는 반드시 인증을 받아야 하고, 참여자의 행위는 모두 기록(audit)되어야 한다. 둘째, 그룹 커뮤니케이션에 참여하는 모든 구성원간의 통신이 안전하게 이루어져야 하는 것과 같이 협업에 참여하는 WFMS간의 통신은 안전해야 한다. 셋째, 객체와 컨텐츠에 대한 접근은 사용자의 접근 권한에 따라 이루어진다. 넷째, 그룹 커뮤니케이션과 마찬가지로 WFMS간의 협업은 동적으로 가입, 탈퇴, 협업이 이루어진다. 따라서 본 연구는 WFMS의 협업을 그룹 커뮤티케이션이라 가정하고 있으며, 협업 기반 보안 프로토콜을 그룹 커뮤니케이션 보안 프로토콜 및 아키텍처로 제안하고 있다.

2. 관련 연구

WfMC(workflowmanagement coaliton)은 보안 서비스와 워크플로우시스템의 보안모델을 제시하고 있으며, 이 연구는 보안의 기본적인 요소와 워크플로우 관리시스템의 보안 필요성을 제시하고 있다[12]. Elisa Bertin and Elena Ferrari는 워크플로우 관리시스템의 허가 제약조건과 허가의 일관성을 검증할 수 있는 방법을 제시하고 있다[2].

Myeonggil Choi, et al.는 워크플로우 관리시스템의 허가 제약조건과 허가의 일관성을 검증할 수 있는 방법을 제시하고 있다[8]. Yang Le, et al.는 워크플로우 관리시스템의 보안요구사항을 도출하고, 워크플로우 관리시스템에 보안요구사항을 적용하는 방법을 보여주고 있다[6].

위의 관련 연구는 워크플로우 관리시스템의 보안문제를 인식하고, 워크플로우 시스템의 기본적인 보안 프로토콜을 제시하고 있다. 즉 WFMS 사용자의 권한 부여 및 역할에 따른 접근 통제에 초점을 두고 있다. 그러나 협업 시에 발생하는 보안 프로토콜 및 이종 WFMS간의 협업에 따른 보안 아키텍처와 관련된 보안 프로토콜을 제시하고 있지 않다.

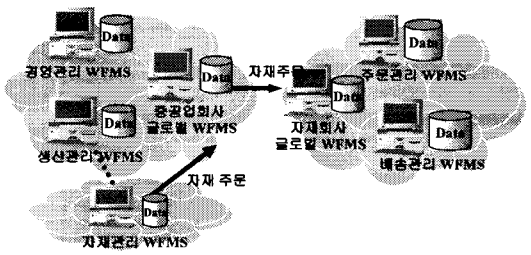
3. WFMS 개 요

WFMS를 살펴보기 전에 워크플로우(workflow)에 대해서 간단하게 살펴보자. 워크플로우는 공통된 경영 목적을 달성하기 위한 활동이며, 조직 프로세서의 다양한 활동들을 잘 정의된 업무로 분화시키는 프로세스이다.

WfMC는 WFMS를 프로세스 정형화, 구체화, 관찰, 조정, 소프트웨어의 작동을 통해서 워크플로우 프로세스의 관리를 지원하는 시스템이라 정의하고 있다[11,12,13]. WFMS는 이종 분산화된 환경에서 거래 처리와 같은 고도화된 기능을 지원이 할 수 있는 보안성, 신뢰성 및 높은 성능을 갖춘 소프트웨어이며, 다른 소프트웨어 및 이종 워크플로우 관리시스템과 연동할 수 있는시스템이다[1].

<그림 1>은 중공업 회사의 WFMS와 철강 회사의 WFMS간의 협업을 보여준다. 중공업 회사는 경영관리 WFMS, 글로벌 WFMS, 생산관리 WFMS는 동일한 지역에서 운영하고 있지만, 자재관리 WFMS는 다른 WFMS와 지리적으로 분리된 지역에서 운영하고 있다.

자재관리 WFMS는 자재 주문을 위해서 자재 주문서를 글로벌 WFMS에 발송한다. 중공업 회사의 글로벌 WFMS는 철강회사의 글로벌 WFMS에 자재 주문서를 발송한다. 철강회사의 글로벌 WFMS는 자재 주문서를 주문관리 WFMS와 배송관리 WFMS에 발송한다. 주문관리 WFMS와 배송관리 WFMS가 자재 주문서를 수신하면, 이 두 WFMS는 중공업 회사의 자재 주문서를 처리한다.



[그림 1] 워크플로우관리시스템간 협업

4. 보안서비스

WFMS의 보안요구사항을 분석하기에 앞서 WFMS에

도입될 수 있는 일반적인 보안서비스를 살펴보면 아래와 같다[12].

4.1 인증(authentication)

대부분의 도메인에서 인가된 사용자에 한해서 데이터와 업무에 대한 접근을 허락하는 것은 중요하다. 특정 사용자가 WFMS에 접근을 위해서는 사용자 인증을 거쳐야 함으로 사용자 인증은 중요하다. 사용자 식별 및 인증을 위해 패스워드, 바이오메트릭, 디지털 서명 등이 사용된다. WFMS가 다른 이종 WFMS와 협업을 수행하기 위해서는 일련의 식별 및 인증을 통해 양방향 인증을 거쳐야 한다. 특히 WFMS가 비동기적으로 운영될 때 상호 운영 프로토콜을 제공해 주어야 한다. 인증은 일반적으로 암호 알고리즘을 이용하여 이루어진다. WFMS의 인증 방식은 인터넷 환경에 적합하게 설계한다.

4.2 접근통제(access control)

인가된 사용자에 한해서 주어진 업무나 데이터에 접근할 수 있다. 인가된 사용자만이 업무나 데이터에 접근할 수 있다. 접근통제는 인가되지 않은 사용자의 접근을 허락하지 않고, 인가된 사용자의 접근을 허락한다. 접근통제는 접근통제리스트(access control list:ACLs), 역할기반 접근통제(role based access control:RBAC)과 다단계접근통제(multilevel access control: MLS) 등의 방식을 사용한다.

이종의 두개의 WFMS간 협업이 발생하면, 워크플로우 프로세스는 사전에 정의된 규칙을 통해 정보를 해석할 수 있어야 한다. 따라서 프로세스 정의 내에 있는 모든 접근통제 정보는 각 워크플로우 도메인내에 식별·인증 정보와 연관시켜 정의되어야 한다.

4.3 기밀성(confidentiality)

대부분의 네트웍 기반 정보시스템에서는 메시지의 도청방지와 변조방지가 중요하다. 메시지는 민감한 정보를 가질 수 있기 때문에 효과적인 도청방지와 변조방지를 위해서는 효율적이고, 강력한 암호 알고리즘을 사용해야 한다. 강력한 암호 알고리즘의 사용은 네트워크를 통해 전송되는 데이터 해독을 방지할 수 있다. 강한 알고리즘을 사용하여 메시지를 암호화 하는 방식과 시스템의 성능은 반비례(trade-off)한다. 즉 강한 알고리즘을 사용하여 암호화를 수행할수록 시스템의 성능이 저하된다. WFMS 기밀성은 악의적인 3자가 송수신 중인 암호화된 데이터의 복호화 시도를 막을 수 있다는 점에서 중요하다. 안전한 통신은 네트웍을 통해 송수신 되는 데이터를 가로채어 메시지의 의미를 알아내는 것을 막고, 메시지 송신자의 신원(identity)을 신뢰성 있게 전송한다.

4.4 무결성(integrity)

암호화된 메시지를 도청하여도 메시지의 내용을 파악할 수 없기 때문에 의미가 없지만, 악의적인 3자는 여전히 메시지 도청과 관련된 문제를 발생시킬 수 있다. 만약 악의적 사용자가 메시지를 중간에 가로채어 수정하여 재송신한다면, 수신자는 유효하지 않은 메시지를 수신한다. 따라서 메시지 변경을 방지하기 위해서 메시지의 무결성을 확보해야 한다.

5. WFMS의 설계고려사항

WFMS의 보안 프로토콜에 대한 요구사항 도출을 위해서는 보안 프로토콜의 고려 사항이 있다. 보안 프로토콜의 고려사항은 보안기능의 확장성, 관리의 편리성, 상호운용성 등이 있다[3,7]. WFMS의 보안 프로토콜은 인트라넷에서만 사용하는 WFMS보다 많은 사용자를 수용할 수 있어야 한다. WFMS는 전역적으로 분산된 WFMS와 협업을 수행함으로 사전에 예측된 사용자보다 사용자 숫자가 많을 수 있다. 따라서 증가할 수 있는 사용자를 지원하기 위해서 WFMS의 보안프로토콜은 쉽게 확장될 수 있어야 한다. 두 번째의 고려사항은 보안 프로토콜의 관리 편리성이다. 모든 워크플로우 프로세스를 지원하는 WFMS는 내재적으로 복잡한 기능을 가지고 있다. WFMS 관리자는 WFMS의 복잡한 기능도 익숙하게 관리할 수 있지만, 보안 기능을 관리하기는 쉽지 않다. 따라서 보안 프로토콜을 효과적으로 운영하기 위해서는 보안 프로토콜을 관리하기 쉬워야 한다. 세째 고려사항은 WFMS간의 상호 운영성이다. 기업 환경과 정보 인프라스트럭처가 상이함으로 조직은 특성에 맞는 보안정책을 수립하고, 보안 프로대책을 도입한다. 즉 정보자원을 효과적으로 보호하기 위해서 조직은 조직의 특성에 알맞은 식별 및 인증 방식, 암호 알고리즘 및 안전한 통신 방식을 채택한다. 이종(heterogeneous) 보안대책을 가진 조직들간의 안전한 협업을 위해서 상호 운영성이 반드시 확보되어야 한다.

이러한 고려 사항을 바탕으로, 본 연구는 WFMS의 4가지 보안요구사항을 도출한다. 첫째, 보안아키텍쳐는 WFMS 기능 변화에 따른 영향을 최소화 할 수 있어야 한다. 조직의 워크플로우를 반영하는 WFMS는 자주 변화됨으로 보안 아키텍쳐는 WFMS와 독립적으로 설계 및

개발되어야 한다. 보안 프로토콜이 WFMS와 독립적으로 수립되면 WFMS의 사용자 증가와 요구되는 성능을 지원할 수 있다.

둘째, 보안 아키텍쳐는 유연하게 설계되어야 한다. WFMS의 서브 시스템은 지리적으로 분산되어 있고, 조직의 워크플로우 변화는 WFMS의 서브 시스템에 영향을 미칠 수 있다. 유연한 보안 아키텍쳐는 WFMS의 변화에 영향을 덜 받기 때문에 효과적인 WFMS 보안 프로토콜을 지원할 수 있다.

셋째, WFMS의 성능이다. WFMS는 신속하게 처리해야만 하는 중요한 데이터를 처리한다. 만약 WFMS가 사용자의 요구를 신속하게 처리하지 못하면, 조직은 비즈니스 기회를 잃어버릴 수 있다. WFMS에 보안 프로토콜을 구현하게 되면 WFMS의 성능이 이전보다 저하될 수 있다. 따라서 WMFS의 보안 아키텍쳐는 비지니스와 WFMS의 성능을 고려하여 설계해야 한다.

넷째, WFMS의 보안 아키텍쳐는 외부의 보안 인프라스트럭처와 독립적으로 설계해야 한다. 각 조직은 다른 체계를 가진 인증 인프라, 공개키 인프라 등으로 구성된 보안 인프라를 채용하기 때문에 다른 보안 체계를 가진 WFMS간 상호 운영성 확보를 어렵게 한다.

6. WFMS 보안 아키텍쳐 설계

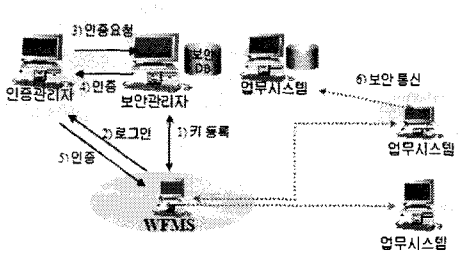
WFMS의 보안 아키텍쳐는 보안 프로토콜과 보안대책이 효과적으로 결합된 구조를 가져야 한다. 논문은 WFMS의 보안요구사항을 반영하기 위해서 에이전트 접근법(agent approach)을 채용

한다. 에이전트는 시스템 환경에 영향을 받지 않고 독립적으로 작동할 수 있는 특성을 가지고 있다. 따라서 이종 시스템 환경에서 쉽게 구현이 가능하다. 에이전트는 WFMS의 플랫폼과 독립적으로 구현이 가능함으로 이종 WFMS간의 협업을 가능하게 한다. 논문은 인증관리자(login agent), 업무시스템(task agent), 보안관리자(security agent) 등 3개의 에이전트를 채용한다.

WFMS에 접근을 위해 사용자는 인증관리자에 인증을 요청한다. 인증관리자는 보안관리자에게 사용자의 인증 및 접근 여부를 문의한다<그림 2>. 사용자는 인증을 받은 후 허락된 권한에 따라 업무시스템과 협업을 수행한다. 업무시스템간에 이루어지는 협업을 보호하기 위해서 통신 채널은 암호화 한다.

보안관리자는 사전에 사용자의 키(key)를 등록하고 인증 정보를 저장한다. 보안관리자의 성능향상을 위해 여러 개의 보안관리자를 사용하고, 인증관리자는 관련 인증 정보를 저장(cache)할 수 있다. 보안관리자는 인증 정보, 로그정보, 사용자 권한 등의 정보를 저장하고, 사용자 인증과 동시에 업무시스템에게 사용자 권한을 전송한다.

보안관리자의 중요한 기능은 사용자 키 관리이다. 키 생성, 분배, 파기 등을 적절하게 관리하지 않고는, 보안은 효과적일 수 없다. 보안관리자는 WFMS 관리자에게 키를 관리할 수 있는 도구를 제공해야 한다. 논문은 키 생성, 배분 과정은 다루지 않는다. 업무시스템은 워크플로우 프로세스를 수행하고, 다른 WFMS와 협업을 수행한다. 업무시스템은 워크플로우 프로세스를 실제로 수행하는 WFMS로 물리적으로 분산된 지역에 위치한다.



[그림 2] 워크플로우 관리시스템의 보안 프로토콜

7. WFMS 보안 프로토콜 설계

본 연구는 WFMS 인증, 협업참여, 키 및 협업 재설정, 안전한 통신, 협업실패 탐지와 협업이탈 등의 보안 프로토콜을 제안한다. 본 논문이 제안하는 보안 프로토콜은 안전한 그룹 통신 보안 프로토콜을 채용하여 WFMS의 협업에 적합하도록 설계한다[10].

WFMS의 보안 프로토콜 설계는 다음과 같은 사항을 가정하고 있다. 보안관리자는 신뢰할 수 있는 3자(Trusted Third Party:***TTP***)의 역할을 수용하고, 인증관리자는 협업에 참가하려는 WFMS를 인증하는 프로토콜을 제공한다. 협업에 참가하려는 업무시스템(***A***)은 보안관리자와 키(K_A)를 공유한다. 비밀키 K_A는 각 WFMS가 협업에 참여하기 전에 보안관리자가 생성하여 등록한다. 협업에 참여하는 모든 잠재적인 업무시스템은 인증관리자의 신분을 사전에 알고 있다. 본 연구는 비밀키 생성·등록 방법과 인증관리자의 신분을 협업 참여자에게 알리는 내용은 다루지 않는다.

보안 프로토콜이 사용하는 노테이션은 다음과 같다.

AG(Authentication aGent)는 인증관리자의 신분을, ***SG(Security aGent)***는 보안관리자의 신분을, ***TG(Task aGent)***는 업무시스템의 신분을 의미한다. $\{X\}_k$는 메

시지 X를 비밀키 k로 암호화한 것을 의미하고, g는 세션 식별자로 협업의 세션을 나타낸다. SK_g는 세션 g의 세션키(비밀키), SK_{g+1}는 다음 세션의 세션키를 의미한다. I 는 임의값(nonce value)을 의미한다.

Leighton-Micali의 키 분배 프로토콜에 바탕을 둔 pair key인 π_{AB}는 협업에 참여하는 업무시스템(TG_1)과 업무시스템(TG_2)간의 비밀통신을 위해 사용된다. 인증관리자(AG)와 업무시스템(TG)은 pair key에서 유도한 공유 비밀키 $\sigma_{AG,\,TG}$를 공유한다.

인증관리자는 비대칭키 쌍인(P_{uG}, P_{rG})를 초기에 생성한다. 공개키(public key)인 P_{uG}는 인증 프로세스 동안 업무시스템에 전달된다. 공개키는 인증관리자가 안전하게 신호(heartbeat)를 송신하는 노력을 감소시키기 위해 사용된다. 보안 프로토콜은 비대칭키 쌍인 (P_{uG}, P_{rG})의 생성·분배를 위해 인증서를 사용하지 않는다. 논문이 채용한 보안 프로토콜은 업무시스템은 세션키를 노출하지 않고, 업무시스템은 보안관리자가 세션키를 노출하지 않다고 신뢰한다고 가정한다.

7.1 인증 프로토콜

인증 프로토콜은 잠재적인 협업 참가자인 WFMS를 인증한다. 인증 프로토콜은 두 가지 목적을 가진다. 첫째, 인증관리자가 잠재적인 업무시스템을 인증한다. 둘째, 협업에 참여하는 업무시스템간에 공유 비밀키를 협상한다. 공유 비밀키(shared secret key)는 업무시스템간의 비밀통신 채널을 만들때 사용한다. 인증 프로토콜은 협업참여 프로세스와 공유 비밀키 유도를 위하여 Leighton-Micali 키 분배를 알고리즘을 사용한다[5]. Leighton-Micali의 장점은 비용이 저렴하는 점이다. 즉 이 알고리즘은 공개키 시스템과 관련된 모듈라 연산을 수행하지 않는 대칭키를 사용한다. 비대칭키는 대칭키와 비교하면 계산량이 많아 컴퓨팅 자원과 시간을 많이 필요하다. 인증 프로토콜은 다음과 같다.

•프로토콜 1: 인증요구

$TG \rightarrow AG$: TG, I_0

•프로토콜 2: pair key 요구

$AG \rightarrow SG$: AG, TG, I_1

•프로토콜 3: pair key 유도

$SG \rightarrow AG$: $\{[\pi_{AG,TG} = \{TG\}_{K_{AG}} \oplus \{AG\}_{K_{TG}}], I_1\}_{K_{AG}}$

•프로토콜 4: 인증

$AG \rightarrow TG$: $AG, TG, \{g, TG, I_0, I_2, P_{UG}\}_{\sigma_{AGTG}}$

잠재적으로 협업에 참여할 수 있는 업무시스템은 인증관리자에게 자신의 신원(identity)과 임의값(nonce value)를 전송하여 인증을 요구한다(프로토콜1). 인증관리자는 pair key인 $\pi_{AG,\,TG}$를 보안관리자로부터 획득한다(프로토콜2, 프로토콜3). 두 개의 신원(identity)과 관련된 세션키로부터 획득된 공유 비밀키는 안전한 통신 프로토콜에서 사용할 수 있다. 재송신 공격(replay attack)을 방지하기 위하여 인증관리자는 보안관리자가 암호화하여 송신한 무작위값 I_1을 검증한다.

보안관리자는 업무시스템(TG)이 비밀통신에 사용하는 공유 비밀키를 다음과 같이 계산한다. 인증관리자는 $TG_{K_{AG}}$를 생성하고, 이 값은 보안관리자로부터 수신된 pair key $\pi_{AG,\,TG}$와 XOR 연산을 수행한다. XOR 연산 결과 공유 비밀키인 $AG_{K_{TG}} = \sigma_{AG,\,TG}$를 획득한다. 획득된 공유 비밀키는 인증관리자와 업무시스템간의 비밀 통신 채널을 형성하는데 사용된다. 각 업무시스템은 공유 비밀키를 획득하기 위해서 보안관리자 직접적으로 통신할 필요 없이, 직접 계산을 통해서 획득할 수 있다. 업무시스템(TG)은 공유 비밀키(shared secret key)를 복호화하고, 임의값(nonce value)을 검증할 수 있다.

공유 비밀키를 획득하고, 인증관리자는 인증을 실시한다 (프로토콜 4). 인증은 인증관리자와 업무시스템의 신원(identity)을 공유 비밀키 $\sigma_{AG,\,TG}$ 를 사용하여 암호화하여 이루어진다. 암호화된 값은 세션 뷰(g), 업무시스템의 임의값(I_0), 공개키(P_{uG}) 등이다. 이 메시지를 수신하면, 수신자는 내용을 복호화하고, 임의값 I_0를 검증한다.

7.2 협업 참여 프로토콜

협업 참여 프로토콜은 업무시스템이 협업에 참여하게 한다.이 프로토콜은 협업참여의 신뢰성을 제공한다. 잠재적으로 협업에 참여하려는 업무시스템(TG)은 인증관리자에게 (프로토콜 5)를 송신한다. 인증관리자는 메시지를 수신하면 검증된 임의값 I_2를 인증 프로세스 동안 업무시스템에 송신한다. 만약 임의값(nonce value)이 유효하지 않으면, 협업참여 요청은 무시된다. 만약 임의값(nonce value)이 유효하면, 업무시스템은 협업 그룹에 참여할 수 있다.

•프로토콜 5: 협업 참여

$TG \rightarrow AG$: $TG, \{AG, I_2\}_{\sigma_{AG,\,TG}}$

업무시스템(*TG*)과 인증관리자(*AG*)는 보안관리자(*SG*)와 공유된 비밀값 검증을 통하여 상호 인증을 수행한다. 잠재적인 업무시스템은 업무시스템(*TG*)과 공유 비밀키를 결정하기 위해 보안관리자와 공유하는 비밀값을 반드시 소유해야 한다. 업무시스템은 최초 인증 요구 메시지에 첨부된 임의값 I_0를 검증하면, 인증 성공 여부를 알 수 있다.

7.3 키 및 협업 재설정 프로토콜

키 및 협업 재설정 프로토콜은 협업 참여자의 신원과 세션키를 분배한다. 세션키 재설정(session rekeying)과 세션키 분배간에는 차이가 있다. 세션키 재설정은 모든 현존하는 협업 참여자가 새로 생성된 세션키를 수신하는 것을 의미하고, 세션키 분배는 인증관리자가 세션키를 모든 협업 참여자에게 분배하는 것을 의미한다.

세션키 분배, 키 및 협업 참여자 신원 배분, 세션 재설정 프로토콜은 모든 협업 뷰(*g*), 가장 최근의 인증관리자의 일련번호(S_{SL})와 전체 메시지를 해쉬 함수로 계산한 MAC을 포함한다. 그룹 뷰(*g*)와 일련번호는 현재 협업 상태를 나타낸다. MAC은 메시지의 무결성을 나타낸다.

세션키는 세션키 블록 $(TG, \{g, SK\}_{\sigma_{AG,TG}})$을 통하여 분배된다. 협업에 참가하려는 업무시스템(*TG*)의 블록은 업무시스템의 신원(identifier)에 의해 식별된다. 블록의 나머지 부분은 공유된 비밀키 $\sigma_{AG,TG}$를 사용하여 암호화 된다. 만약 협업자 신원(identity)이 수신자에 의해 정상적으로 복호화되면, 업무시스템은 인증관리자가 블록을 만들었음을 확신할 수 있다.

•프로토콜 6: 키 분배

$$AG \rightarrow TG: g, S_{AG}, \left(TG, \{g, SK_g\}_{\sigma_{AGTG}}\right)$$

$$\left\{H\left(g, S_{AG}, \{TG, SK_g\}_{\sigma_{AGTG}}\right)\right\}_{SK_g}$$

•프로토콜 7: 협업자의 키 및 아이디 분배

$$AG \rightarrow TG: g, S_{AG}, (TG, \{g, SK_g\}_{\sigma_{AGTG}}, TG_1, TG_2, TG_3, \cdots,$$

$$\left\{H\left(g, S_{AG}, \{TG, SK_g\}_{\sigma_{AGTG}}, TG_1, TG_2, TG_3, \cdots\right)\right\}_{SK_g}$$

•프로토콜 8: 세션키 재설정

$$AG \rightarrow \text{협업그룹}: g, S_{AG}, \left(TG, \{g+1, SK_{g+1}\}\right)_{\sigma_{AGTG}},$$

$$\left(TG_1, \{g+1, SK_{g+1}\}_{\sigma_{AGTG_1}}\right), \cdots,$$

$$\left\{H\left(g, S_{AG}, \{TG, g+1, SK_{g+1}\}_{\sigma_{AGTG}}\right), \cdots\right\}_{SK_{g+1}}$$

(프로토콜 6)은 하나의 업무시스템의 세션키 블록을 포함한다. (프로토콜 7)는 하나의 업무시스템의 세션키 블록을 가지고 있으며, 현재 업무시스템 (TG_1, TG_2, TG_3,....)을 나열한다. (프로토콜 8)에서 보듯이 세션키 블록은 각 업무시스템을 위해 생성되고, 협업 참여자 신원은 세션키 블록에서 도출된다.

세션키 재설정은 (프로토콜 8)과 같이 이루어진다. 인증관리자는 공유 비밀키를 저장(cache)하고, (프로토콜 9)를 신속하게 생성한다. 저장된 공유 비밀키를 사용하면, 메시지 수신자는 세션키 블록에서 세션키를 추출할 수 있고, 빨리 사용할 수 있다. 메시지의 크기는 협업참여자의 수에 따라 선형적으로 증가한다.

7.4 안전한 통신 프로토콜

안전한 통신은 응용 수준에서 통신 트래픽을 보호한다. 메시지 형태는 메시지 암호화 정책에 따라 변화될 수 있지만, 메시지 인증코드(Message Authentication Code:MAC)를 사용하면 무결성을 확보할 수 있고, 세션키를 사용한 암호화는 기밀성을 확보할 수 있다. (프로토콜 9)는 무결성, (프로토콜 10)은 기밀성, (프로토콜 11)은 무결성과 기밀성을 제공한다.

송신자는 메시지의 해쉬값을 암호화한 MAC을 생성할 수 있고, 수신자는 해쉬값을 복호화하여 검증함으로 MAC의 진위 여부를 확인한다. 만약 해쉬값이 일치하면, 수신자는 메시지가 외부의 3자에 의해 수정되지 않음을 확신할 수 있다.

•프로토콜 9: 무결성

$$TG \rightarrow \text{협업그룹}: g, TG, [M], \{H(g, TG, M)\}_{SK_g}$$

•프로토콜 10: 기밀성

$$TG \rightarrow \text{협업그룹}: g, \{TG, [M]\}_{SK_g}$$

•프로토콜 11: 무결성/기밀성

$$TG \rightarrow \text{협업그룹}: g, \{TG, [M], H(g, TG, M)\}_{SK_g}$$

7.5 협업 중단 탐지 프로토콜

WFMS는 악의적인 공격자가 인증관리자로부터 협업에 참여하는 업무시스템에게 키 재설정과 관련된 메시지 전달을 방해하는 공격을 감내할 수 있어야 한다. 이와 같은 공격이 발생하더라도, 특정 업무시스템은 이전의 세션키를 가지고 있을 수 있다. 이 경우 세션키가 파괴되면 보안 위험이 발생할 수 있다. 정확한 협업 참여자의 신원

(identity)를 알기 위해서 인증관리자는 업무시스템의 협업 중단을 탐지해야 한다. 협업 중단 탐지 프로토콜은 안전한 신호(secure heartbeat)를 협업 중단 탐지 프로토콜로 사용한다. (프로토콜 12)이 나타내듯이 인증관리자는 협업 참여자가 보내는 신호(heartbeat)를 계속적으로 수신하면 협업 프로세스의 중단 여부를 발견할 수 있다. 인증관리자가 업무시스템의 신호(heartbeat)를 수신하지 못하면, 업무시스템이 협업을 중단하거나 협업그룹에서 추방된 것으로 여길 수 있다. 협업에 참여하는 업무시스템은 인증관리자의 신호(heartbeat)를 수신함으로 인증관리자가 운영 중임을 알 수 있다(프로토콜 13). 인증관리자의 신호(heartbeat)가 수신되지 않는다면, 업무시스템은 인증관리자가 중단되었다고 여길 수 있다.

•프로토콜 12: 협업참여자 신호

$TG \rightarrow AG$: $TG, g, S_{TG}, H(g, S_{TG})_{\sigma_{AG:TG}}$

•프로토콜 13: 세션 신호

$TG \rightarrow$ 협업그룹 : $g, S_{AG}, H(g, S_{AG})_{P_{AG}}$

•프로토콜 14: 키 전송

$TG \rightarrow AG$: g, TG

신호(heartbeat)는 두 가지 역할을 수행한다. 업무시스템은 신호(heartbeat)를 사용하여 중단 탐지와 협업 상태가 최신 세션뷰에서 진행되는지 여부를 확인한다. 인증관리자의 일련번호는 신호(heartbeat)가 최근의 수신한 신호임을 나타낸다. 협업 참가자는 협업 뷰를 통해 자신이 가장 최신 세션키를 사용하고 있음을 확신한다. 암호화되어 전송되는 신호(heartbeat)는 공격자가 신호(heartbeat)를 위조하지 못하도록 한다. 이러한 프로토콜이 없다면, 공격자는 새로운 세션키 분배를 막고, 협업 참가자가 이전의 세션키를 사용하여 전송하도록 속인다.

현재 세션키와 협업 신원 정보를 수신하지 못하는 업무시스템은 키 전송 요청 메시지를 송신함으로 복구할 수 있다 (프로토콜 14). 키 전송 요청 메시지는 업무시스템이 가장 최근 키/협업참여자 신원 분배를 원한다는 것을 인증관리자에게 보여준다. 이 경우 프로세스는 가장 최근 세션키와 협업참여자 신원을 분배한다. 협업 중단 탐지 프로토콜은 인증관리자의 협업 중단 탐지 뿐만 아니라 협업 중단시에 협업에 다시 복구할 수 있게 한다.

7.6 탈퇴 프로토콜

탈퇴 프로토콜은 업무시스템이 협업에서 자연스럽게 탈퇴할 수 있도록 한다. 업무시스템은 (프로토콜 15)을 전송하여 자신의 협업 탈퇴를 나타낸다. 탈퇴 프로토콜은 다른 목적으로도 사용된다. 업무시스템은 다른 업무시스템의 협업 탈퇴를 요구할 수 있다. 협업탈퇴를 요구하기 위해서, 탈퇴 요구자는 블록($\{g, K_1\}_{SK_R}$)에 K_1의 신원(identity)를 삽입한다. 인증관리자는 이 형태의 메시지를 수신하고 업무시스템(TG_1)을 보안정책에 따라 탈퇴시킨다.

•프로토콜 15: 협업 탈퇴

$TG \rightarrow AG$: $TG, \{g, TG, \{g, TG_1\}_{SK_0}\}_{\sigma_{AG:TG}}$

8. 결 론

보안이 필요한 도메인에 워크플로우를 효율적으로 운영하기 위해서는 WFMS는 기존의 보안 기법을 결합할 필요가 있는데, 이를 통해 비용을 최소화하고, 사용자의 이용을 극대화하면서 바람직한 보안수준에 도달해야 한다.

본 논문은 WFMS의 보안요구사항을 분석하고, 이를 바탕으로 WFMS의 보안 아키텍처와 보안 프로토콜을 제시하고 있다. WFMS의 보안 아키텍처와 보안 프로토콜 설계를 위해서 논문은 에이젼트 중심의 접근법을 채용하였다. 에이젼트는 이종 시스템 환경에서 설계 및 구현이 가능한 특성을 가지고 있다. 논문은 WFMS의 보안요구사항을 수용하기 위해서 인증관리자, 업무시스템, 보안관리자를 채용하고, 각 에이전트의 역할을 설계하여 보안 프로토콜에 반영하였다.

논문이 제안한 보안 프로토콜은 분리하여 사용할 수 있는 모듈 형태의 프로토콜이다. 특히 WFMS의 협업 전 과정에 사용할 수 있는 보안 프로토콜을 제시하고 있다. 논문이 제안하는 보안 프로토콜은 이종의 WFMS의 협업에서도 사용이 가능한 유연한 구조를 가지고 있다. 유연한 보안 프로토콜은 인터넷을 기반으로 다른 IT 환경과 인프라스트럭쳐를 채용한 인터넷 기업의 보안을 효과적으로 수행하게 함으로 기업간의 협업을 효율적으로 증진시킬 수 있다. 향후에는 논문이 제시하는 인증 프로토콜과 WFMS를 둘러싸고 있는 기업 보안 환경과의 관련성을 분석하여 기업 전산자원을 고려한 WFMS 보안대책의 구현이 필요하다.

참고문헌

[1] Mike Anderson, "Workflow Interoperability-Enabling E-Commerce", WfMC White Paper, 1999.

[2] Elisa Bertin, Elena Ferrari, "The Specification and Enforcement of Authorization Constraints in Workflow Management Systems," *ACM Transactions on Information Systems and System Security*, Vol. 2, No. 1, 1999, pp. 65-104.

[3] Mary Ann Davidson, "Security for E-Business," *Information Security Technical Report*, Vol. 6, No. 2, 2001, pp. 80-94.

[4] Ehud Gudes, Martin S. Oliver and Reind P. van de jet, "Modeling, Specifying and Implementing Workflow Security in Cyberspace," *Journal of Computer Security*, Vol. 7, No. 4, 1999.

[5] *T.Leighton, S.Micali, "Secret-Key Agreement without Public-Key Cryptography," Proceedings of Crypto 94, 1994, pp.456-479.*

[6] Le Yang, M.G.Choi, Y.S.Choi, S.M. Shin, "FWAM: A Flexible Workflow Authorization Model using Extended RBAC," Proceeding of Computer Supported Cooperative Work in Design, 2008.

[7] D. Liu, M. Wu and S. Lee, "Role-Based Authorizations for Workflow Systems in Support of Task-Based Separation of Duty," *The Journal of Systems and Software*, Vol. 73, 2004, pp. 375-387.

[8] Myeonggil Choi, Urlong Jin, Y.S.Choi, and S.M. Shin, "Development of a Flexible Access Conrol Design by Extending RBAC," Proceedings of First International Conference on Communications and Networking in China, 2006.

[9] Patrick McDaniel, Peter Honeyman, "Antigone: Flexible Framework for Secure Group Communication", *Proceedings of the 8th USENIX Security Symposium*, 1999, pp. 99-114.

[10] S. Tinderle, M. Teichert and P. Dadam, "Correctness Criteria for Dynamic Changes in Workflow Systems," *Data & Knowledge Engineering*, Vol. 50, 2004, pp. 9-34.

[11] *Workflow Management Coalition, "Workflow Reference Model", Technical Report, 1994.*

[12] Workflow Management Coalition, "Workflow and Internet: Catalysts for Radical Change," *White Paper*, June, 1998.

[13] Workflow Management Coalition, "Workflow Security Considerations," *White Paper*, 1998.

최 명 길(Myeonggil Choi) **[정회원]**

- 1993년 : 부산대학교 학사
- 1995년 : 부산대학교 석사
- 2004년 : 한국과학기술원 박사
- 1995년~2000년 : 국방과학연구소 연구원
- 2000년~2005년 : 한국전자통신연구원 국가보안기술연구소 선임연구원
- 2005년~2007년 : 인제대학교 조교수
- 2008년~현재 : 중앙대학교 조교수

<관심분야>
보안성평가, 홈네트워크 보안, 정보보호정책 및 관리

이 동 호(Dongho Lee) **[정회원]**

- 1996년 : 부산대학교 경영학사
- 1998년 : 부산대학교 경영학 석사
- 2004년 : 부산대학교 경영학 박사
- 2004년~2005년 : 부산대학교 경영경제연구소 전임연구원
- 2005년~2006년 : 동명정보대학교(현 동명대학교) 전임강사
- 2006년~현재 : 경상대학교 조교수

<관심분야>
e-비즈니스, 유통정보시스템, 정보보호정책 및 관리

황 원 주(Won-Joo Hwang) **[정회원]**

- 1998년 : 부산대학교 컴퓨터공학과 학사
- 2000년 : 부산대학교 컴퓨터공학과 석사
- 2002년 : 오사카대학 정보시스템공학과 박사
- 2002년~현재 : 인제대학교 정보통신공학과 조교수

<관심분야>
홈네트워크, 정보보호