2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

계층적 보안 구조를 이용한 인증·부인봉쇄 메커니즘 설계

이재명*, 신미예*, 황윤철*, 이상호**
충북대학교 전자계산학과
e-mail:dlwoaud@cnlab.chungbuk.ac.kr

Design of Non-repudiation Mechanism Using hierarchical Security structure

Jae-Myoung Lee*, Mi-Yae Shin*, Yoon-Cheol Hwang*,
Sang-Ho Lee**
Dept of Computer Science, Chungbuk University

요약

부인봉쇄 서비스의 목적은 송신자와 수신자 사이에서 메시지를 송수신하는 것과 관련하여 부인할 수 없는 타당한 증거를 수집하고, 유지하여 이를 이용 가능하도록 만드는 것이며, 신임된 제3자가 필요하다. 이 논문에서는 계층적인 구조를 갖는 조직에서 상위 자가 하위 자를 신임한다는 가정 하에 통신 당사자간에 제3자의 간섭을 최대한 줄여 주는 인증 및 부인봉쇄 서비스를 제공하는 메커니즘을 설계한다.

1. 서 론

컴퓨터의 보급과 인터넷의 사용이 급증하면서 컴퓨터 네트워크를 통한 정보량이 급격히 증가되면서 정보를 전송하는 방식이 다양화되고 이에 따라 합법적인 사용자의 여러 가지 부정 행위에 대해서도 정보에 대한 안전성과 신뢰성을 보호할 수 있는 새로운 정보보호 사항들이 요구되고 있다. 이러한 정보화 사회에서 요구되는 정보보호 문제에 대해서 관용키나 공개키 방식 등을 이용한 여러 가지 대책들이 오래 전부터 연구되어 오고 있다. 정보의 비밀을 보장하기 위한 암호 메커니즘, 인가되지 않은 자원에 대한 접근을 제어하기 위한 접근 제어 메커니즘, 송수신 사실에 대한 부인을 방지하기 위한 부인봉쇄 메커니즘 등이 이에 해당된다. 특히 분산환경 시스템에서 메시지 송신자나 수신자는 각각 메시지의 송수신을 거부할 수 있으므로 신임된 제 3자는 이러한 부인봉쇄 서비스를 제공하기 위해 인증, 공증, 분배, 판결자로서 필요하다.[2] 메시지의 송신자는 수신자에게 메시지를 전송하기 전에 신임된 제 3자로부터 인증을 위한 키를 획득한 후 수신자에게 메시지를 송신하고, 또한 수신자는 메시지를 수신했음을 신임된 제 3자에게 알려야 한다. 사용자를 인증하는 방법은 이렇게 다양 하지만 그 중에서 계층적인 인증 구조는 많은 인증서 체인이 존재한다는 보안상 허점이 있음에도 불구하고 사실상 표준으로 남아 있다.[1] 계층적인 인증 구조 환경에서는 상위 자는 하위 자의 신임장을 갖고 있으므로 신원은 확인할 수 있지만 전송되는 메시지의 송수신자 임을 증명할 수는 없다. 따라서 이 논문에서는 부인봉쇄 서비스 제공을 위한 분산 환경에서의 일반적인 부인봉쇄 프로토콜을 2장에서 알아보고, 3장에서는 계층적인 조직 구조에서의 인증 메커니즘을 알아본다. 4장에서는 계층적인 조직 구조에서 작성되는 신임장을 이용한 부인봉쇄 서비스 프로토콜을 제한하며, 끝으로 5장에서 결론을 맺는다.

2. 분산환경에서의 일반적인 부인봉쇄 메카니즘

부인은 사회적 혹은 전자적 환경에서 존재하는 것으로 보안처리 가능한 것 중 하나로, 송신자는 수신

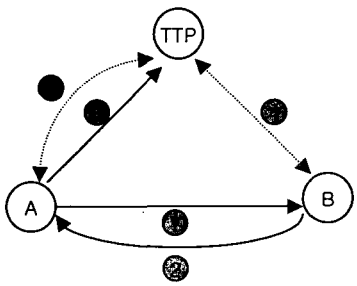
에 대한 증거를 얻기 위해 수신자에게 수신을 했다는 것을 증명할 수 있는 간단한 인식을 요구한다.[2] 이러한 인식은 통신 채널에 대한 신뢰성과 통신에 참여하는 사람들의 신뢰성 문제로 인해 제기되며, 부인봉쇄 프로토콜을 디자인하는데 많은 영향을 끼친다.

부인봉쇄 서비스는 서명, 암호화, 인증, 데이터 무결성 메카니즘과 같은 메커니즘의 사용을 통하여 제공되며, 생성의 증거, 전송과 저장의 증거, 입증의 증거, 논쟁의 해결로 구성된다.

부인봉쇄의 프레임워크와 메커니즘은 ISO/IEC에 의해 표준화되고 있으며, 본 논문에서는 프로토콜의 메시지를 표현하기 위하여 다음과 같은 기호를 사용한다.[3]

- X,Y : concatenation of two message X and Y
- H(X) : a one-way hash function of message X
- eK(X) and dK(X) : encryption and decryption of message X with key K
- sK(X) : digital signature of message X with the private key K
- P_A, S_A : the public and private key of pricipal A
- A -> B : X : principal A sendes message X to Principal B
- A <-> B : X : principal A featches message X from principal B using a "ftp get" operation

[3]에서는 신임된 제3자를 기본으로 하는 해결 방안을 제안하고, 실행 될 때 포함되는 부분을 최소화하려했다. 이를 그림으로 표현해 보면 아래 그림1과 같다.



[그림 1] A fait Non-repudiation Protocol

(1) f_{NRO}, B, L, C, NRO

(2) f_{NRR}, A, L, NRR

(3) f_{SUB}, B, L, K, con_K

(4) f_{CON}, A, B, L, K, con_K

(5) f_{CON},A, B, L, K, con_K

- A : originator of the non-repudiation exchange
- B : recipient of the non-repudiation exchange
- TTP : on-line trusted third party providing network services accessible to the public
- M : message sent from A to B
- C : commitment(cipher text) for message M, e.g. M encrypted under a key K
- K : message key defined by A
- NRO = $sS_A(f_{NRO}, B, L, C)$: Non-repudiation of Origin for M
- NRR = $sS_B(f_{NRR}, A, L, C)$: Non-repudiation of Receipt for M
- sub_K = $sS_A(f_{SUB}, B, L, K)$: proof of submission of K
- con_K = $sS_A(f_{CON}, A, B, L, K)$: confirmation of K issued by TTP

이 프로토콜은 Commitment(cipher text)와 Key을 분리하여, Commitment는 A, B사이에서 교환되어지고 Key는 신임된 제 3자 TTP에게 맡겨진다. 여기서 A, B , TTP는 모두 자신의 비밀 서명키와 공용키를 모두 갖추고 있다고 가정한다. 유일한 레이블 L은 특별한 프로토콜의 모든 메시지를 연결한다. 플래그는 서명된 메시지를 나타내기 위해 사용한다. 위의 그림을 기호를 사용해 표현하면 아래와 같다.

(1) A <-> B : f_{NRO}, B, L, C, NRO

(2) B -> A : f_{NRR}, A, L, NRR

(3) A -> TTP : f_{SUB}, B, L, K, sub_K

(4) B <-> TTP : f_{CON} , A, B, L, K, con_K

(5) A <-> TTP : f_{CON}, A, B, L, K, con_K

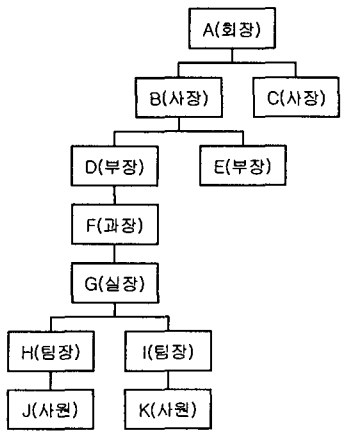
서명된 메시지 안에는 생성자와 수령자의 식별값이 포함되며, 메시지 M은 key K를 가지고 복호화함으로써 얻어진다. 또한 신임된 제3자는 전달 Agent로써 활동하지 않고 메시지 key를 위한 인증 Agent로써의 역할만 한다.

3. 계층구조에서의 인증 메커니즘

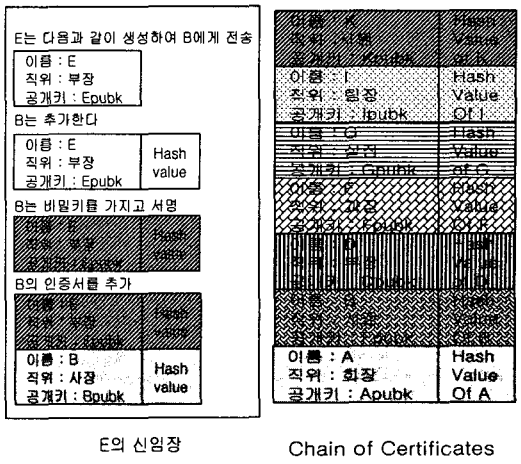
보안 모델에 접근하는 방법으로는 평평한 구조 방법과 계층적 구조 방법이 있다. 평평한 구조 접근 방법은 전체 보안 공간의 효율적인 사용이 가능하고 인터넷 환경에서 보안 정책 복제로 능률을 유지할 수는 있다. 그러나 분산된 보안 정책 변화에 따른 갱신의 어려움이 존재한다. 계층적 구조는 중앙 집중 방식이 아닌 분산 방식으로 보안 정책 변화에 따른 갱신이 쉽다. 따라서, 엔터프라이즈 네트워크, 더 나아가 글로벌 네트워크 환경에서 적합한 보안 모델의 접근 방법은 계층적 구조의 보안 모델이 적합할 것이다. 이와 같은 장점을 가지고 있는 계층적 구조의 모델을 적용하기 위해 한 회사의 조직 체계를 예로 들어본다.[4]

큰 회사의 조직 체계는 몇 개의 계열사를 가지고 있으며, 각 계열사들 내에는 여러 개의 부서로 이루어져 있다. 또한 각 부서들 하위에 프로젝트를 수행하는 팀과 팀을 구성하는 팀원들로 이루어져 있다. 최상의 회장은 이름이나 얼굴 등으로 회사내의 모든 직원들을 알기가 어렵다. 그러나 회사의 최고경영자인 회장은 각 그룹의 사장들을 알 수 있으며, 각 계열사의 사장은 부장들을 알 수 있다. 이와 같이 회사 내에서 계층적으로 상위 직원은 하위 직원을 알 수 있다.

계층적인 인증 보안정책을 적용함에 있어 위와 같은 조직내의 특성을 이용하여 회장이 모든 직원의 신원을 인증하는 것이 아니라 해당 직원의 바로 위의 상사가 부하직원의 신원을 인증한다.



[그림 2] 회사의 조직 체계도



[그림 3] E의 신임장 및 Chain of Certificates

위의 [그림 3]의 E의 신임장을 생성하기 위해서는 다음과 같은 메커니즘을 따른다.

[단계1] E는 자신의 특성을 나타내는 이름, 직위와 자신의 공개키를 생성하여 상위에 있는 B에게 전송한다.

[단계2] B는 E에서온 메시지에 hash value를 추가한다.

[단계3] B는 hash value를 추가한 후에 메시지와 hash value를 자신의 비밀키를 가지고 암호화시킴으로서 서명을 한다.

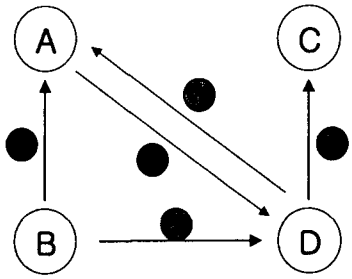
[단계4] 마지막으로 B는 자신의 인증서를 추가함으로서 E의 신임장을 생성한다.

조직의 계층구조가 깊을 경우 위와 같은 절차를 반복적으로 적용함으로서 하위직원의 신임장이 [그림 3]과 같이 생성됨을 볼 수 있다.

4. 계층적 보안구조의 인증·부인봉쇄 메커니즘

조직적인 계층 구조에서 상위 관계자가 기지고 있는 신임장은 분산환경의 부인봉쇄 서비스에 포함되는 신임된 제3자의 역할 중 인증 기능뿐만 아니라, 공개키를 포함하고 있다. 따라서 통신을 하고자 하는 당사자간에 메시지를 전송했다는 증거 및 수신했다는 증거를 남기는 기능을 추가함으로써 통신 당사자 이외의 상위 관계자는 메시지(인증 및 부인봉쇄 서비스에 관련된 메시지) 분배의 역할을 하지 않아도 된다. 즉, 통신에 직접 관계하지 않는 제 3자의

포함 관계를 최소화할 수 있으므로 분산환경에서의 부인봉쇄 서비스 프로토콜보다 더 효율적이다. 이런 메커니즘을 표현하면 아래 [그림 4]와 같다.



[그림 4] 인증·부인봉쇄 메커니즘

위의 [그림 4]를 기호화하여 표현해 보면 아래와 같다.

(1) B -> A : B, D, $_{B}H(M)$
(2) B -> D : B, c(M), $_{B}H(M)$
(3) D -> C : D, B, flag-r
(4) D -> A : $_{B}H(M)$, B, D, C
(5) A -> D : $_{B}P_{K_{a}}$, B

위의 표시된 내용을 단계별로 기술하면 다음과 같다.

[단계1] B는 상위 A에게 D와 전송하고자 하는 message의 hash 값을 전송한다. 그러므로 전송부인을 할 수 없다.

[단계2] B는 D에게 B, message의 암호화 값, message의 hash값을 전송, D는 현재까지 아무런 정보를 B로부터 얻을 수 없다.

[단계3] D는 B와 통신을 하며, 수신자임을 밝히는 증거를 C에게 전송 수신을 거부할 수 없다.

[단계4] D는 A에게 $_{B}H(M)$, B, D와 본인을 인증해 줄 수 있는 C를 전송한다.

[단계5] A -> D : $_{B}P_{K_{a}}$, B, A. D는 B의 공개키를 이용하여 MESSAGE를 복원 할 수 있다.

5. 결론

부인봉쇄 프로토콜은 두 가지 방법으로 세워진다. 하나는 안전한 교환을 동시에 이루거나, 아니면 신임된 제3자의 서비스를 빌려서 하는 방법이다. 본 논문에서는 두 번째 접근 방법을 따랐으며, 부인봉쇄 프로토콜은 통신 채널이나, 통신에 관여하는 사람들의 신뢰성에 의존하지 않아야 하며, 프로토콜이 실행되는 관점에서는 어느 누구도 이익이나 우위를 가지게 해서는 안되며, 제3자의 역할을 최소화되게 설계되어야 한다. 이런 관점에서 본 논문에서는 조직적인 계층 구조에서 상위 관계자가 가지고 있는 신임장은 분산환경의 부인봉쇄 서비스에 포함되는 신임된 제3자의 역할 중 인증 기능을 제공할 뿐만 아니라, 공개키를 포함하고 있다. 따라서 통신을 하고자 하는 당사자간에 메시지를 전송했다는 증거 및 수신했다는 증거를 남기는 기능을 추가함으로써 통신 당사자 이외의 상위 관계자는 메시지(인증 및 부인봉쇄 서비스에 관련된 메시지) 분배의 역할을 하지 않아도 된다. 즉, 통신에 직접 관계하지 않는 제3자의 포함 관계를 최소화할 수 있으므로 분산환경에서의 부인봉쇄 서비스 프로토콜보다 더 효율적인 것임을 보였고, 또한 제3자는 인증, 공증, 판결자로서의 역할을 모두 할 수 있음을 보였다. 본 논문은 단지 개념적인 차원에서 계층적 구조를 이용한 인증·부인봉쇄 메커니즘을 설계한 것으로 향후 이것을 더욱 세분화하여 설계하고 구현함으로써 실질적으로 기존에 존재하는 부인봉쇄 서비스보다 통신 당사자간에 데이터 전송횟수를 얼마나 감소시키는지에 대한 연구가 필요하다.

[참고문헌]

[1] 이재광, 정진욱, 변옥환 역, "자바 보안과 암호화", 한빛 미디어, 2000

[2] J Zhou and D. Gollmann, "Observation on Non-repudiation", Lecture Notes in Computer Science 1161, Advances in Cryptology Proceeding of Asiacrypto'96, pages 133-144, Kyongju, Korea, November 1996

[3] Zhou. and D.Gollmann. "A fair non-repudiation protocal". Proceedings of 1996 IEEE Symposium on Security and privacy, pages 55-61, Oakland, California, May 1996.

[4] Charles P. pFleeger, "Security in Computing", p135-140, Prentice-Hall International, Inc, 1997

[5] "Securing the Web Server : Windows NT vs. Unix" in procedding of the Electronics Commerce Conference, Auust 4-5, 1997, Arington, VA pp. A2-3 to A2-17