부인방지 표준 메커니즘의 분석

서문석*, 이병천*, 백준상*, 김광조*, 김상정**, 이경구**

한국정보통신대학원대학교*
한국정보보호센터**

On the Standard Mechanism for Non-repudiation Services

Moonseog Seo*, Byoungcheon Lee*, Joonsang Baek*, Kwangjo Kim*,
Sangjeong Kim**, Koynggoo Lee**

Information and Communications Univ.*
Korea Information Security Agency**

요 약

본 논문에서는 최근 인터넷 등과 같은 공중 통신로를 통하여 전자적인 서비스를 제공할 경우에 약속된 프로토콜에 위반한 송수신자 쌍방간의 행위에 기술적인 증거를 제공하고, 논쟁 발생 시 법적 근거로 제공할 수 있는 부인 방지 서비스 메커니즘에 대한 최근의 연구 현황 및 국제 표준을 분석하였으며, 분석된 내용을 토대로 기존 메커니즘들이 가지고 있는 문제점들을 도출하여 앞으로 제시될 부인방지 메커니즘의 표준에 대한 가이드라인을 제시한다.

I. 서 론

현 사회가 정보화 사회로 발전함에 따라 정보보호 기술을 이용하여 지금까지는 메시지 기밀성, 사용자 인증성, 정보 무결성 보장, 전자 서명 등의 다양한 보안 서비스를 제공해오고 있었으나, 최근 인터넷 등과 같은 공중 통신로를 통하여 전자적인 서비스를 제공할 때에 약속된 프로토콜을 위반한 송. 수신자 쌍방간의 행위에 기술적인 증거를 제공하고, 논쟁 발생 시 법적 근거로 제공할 수 있는 부인 방지라는 새로운 서비스가 필요하게 되었다. 즉, 암호화 및 전자서명을 이용한 전자 문서 교환 (EDI : Electronic Data Interchange), 전자 계약 (Electronic Contract), 전자 상거래 (Electronic Commerce) 등의 응용분야가 향후 크게 활성화 될 것으로 예상되지만 실제 적용에 있어서는 개인의 행위에 대한 부인의 가능성이 있으며 이를 방지하기 위한 부인방지 서비스의 제공이 필요하다. 더구나 국내에서는 전자서명법의 발효와 더불어 전자 상거래의 활성화를 위한 법적 근거가 마련되었는데 이의 활성화를 위해서도 부인방지 서비스와 같은 부가 서비스가 반드시 제공되어야 한다.

본 연구는 한국정보보호센터 연구비 지원으로 수행되었음.

이러한 부인 공격을 방지하기 위해서는 적절한 부인방지 메커니즘을 이용하여 송신부인방지(NRO : Non-Repudiation of Origin), 수신부인방지(NRR : Non-Repudiation of Receipt), 제출부인방지(NRS : Non-Repudiation of Submission), 전달 부인방지(NRT : Non-Repudiation of Transport) 등의 서비스 제공이 가능하여야 한다. 이러한 부인 방지 메커니즘에 대해서 국외에서는 국제 표준 기구를 통하여 다양한 연구가 진행되어 왔으며, 1998년에는 ISO/IEC IS 13888-1,2,3으로 표준화되어 있다. 정보화 사회가 성숙되어 갈수록 이러한 부인 방지 메커니즘은 더욱 다양한 형태로 구현되어 질 것으로 예상되며, 본 논문에서는 부인방지를 위한 기존의 연구 및 표준화 내용을 분석하여 기존 표준들이 가지고 있는 문제점을 도출하고 앞으로 제시될 부인방지 메커니즘의 표준에 대한 가이드라인을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 부인방지 메커니즘의 다양한 응용분야를 제시하였다. 3장에서는 부인방지 메커니즘과 관련한 연구결과를 분석하였으며, 4장에서는 국제표준인 ISO/IEC IS 13888-1,2,3의 내용을 조사하였다. 기존의 표준이 가지고 있는 문제점 및 새로운 표준이 가져야하는 요구사항 등을 5장에 정리하였으며, 6장에서 결론을 맺는다.

II. 부인방지 메커니즘의 응용분야

인터넷 등과 같은 공중 통신로를 통하여 전자적인 정보를 교환할 경우 송·수신자간에 상호 약속된 프로토콜을 위반하고 자신의 행위를 부인하는 위험성이 상존하게 된다. 예를 들면 인터넷 쇼핑몰을 통해 물건을 구입한 후 정당하게 지불을 완료했으나 상점에서 지불받지 못했다고 부인을 하는 경우 고객은 손해를 입을 수 있다. 부인방지 메커니즘에 근간한 다양한 부인방지 서비스가 실제 제공된다면 대부분의 응용분야에서 이와 같은 논쟁을 미연에 방지하고 적절히 해결할 수 있는 기반구조로 사용될 수 있다. 부인방지 서비스의 적용 가능한 응용분야로는 다음과 같은 것들이 있다.

1. 전자계약

국내에서는 전자서명법이 제정되어 99년 하반기부터 발효되었다. 이에 따라 전자적인 수단으로 이루어지는 계약이 기존의 인감을 이용한 물리적인 계약과 동일한 효력을 인정받게 되며 향후 정보화 사회로의 발전에 큰 역할을 할 것으로 기대된다. 공정한 전자계약이 이루어지려면 프로토콜을 위반하거나 행위를 부인하는 것을 방지할 수 있는 부인방지 서비스가 반드시 필요하다.

2. 전자상거래

최근 인터넷 쇼핑, 온라인 주식거래, 인터넷 은행 등 전자상거래 시장이 크게 활성화되고 있다. 전자상거래는 현금이 오고 가는 상거래로서 만일 행위의 부인이 가능하다면 전자상거래의 기반 자체가 흔들리게 되며, 공정한 전자상거래가 이루어지기 위해서는 부인방지서비스가 필수적으로 사용되어야 한다.

3. 이동통신서비스

IMT-2000 등 차세대 이동통신서비스에서는 음성전화 기능뿐만 아니라 멀티미디어 데이터통신, 인터넷 접속, 전자상거래 단말 등의 다양한 기능을 제공할 것으로 예상되며 이동성의 편리함을 제공하기 때문에 이용이 크게 확산될 것으로 전망된다. 이러한 이동단말시스템은 컴퓨터시스템에 비해 계산능력, 저장용량, 통신용량 등에서 능력이 제한될 수밖에 없기 때문에 적절한 정보보안 서비스를 제공하기 위해서는 많은 시스템적인 고려가 필요하다. 이동통신단말기를 통하여 정보보안 서비스를 이용하기 위해서는 앞에서 기술한 바와 같이 부인방지 서비스가 제공되어야 한다. 여기에서 추가적으로 고려해야 할 것은 부인방지 토큰이 사용될 경우 이동단말에 모든 토큰을 저장하기가 어렵기 때문에 부인방지 서버와의 적절한 역할분담이 필요하다고 생각된다.

4. 온라인 요금납부

최근 인터넷이 발달하면서 기존의 각종 요금 납부 방식이 온라인 방식으로 대체되는 추세에 있다. 즉 전자우편을 통한 요금 청구, 온라인 지불, 전자영수증 등이 가능한 것이다. 이러한 요금납부 방식이 이용되려면 적절한 부인방지 서비스가 제공되어야 한다. 특히 온라인 지불에 대해 전자영수증을 받은 경우 이의 유효성을 부인방지서버가 확인해 주고 사용자 시스템의 고장 시에도 유효성을 증명해줄 수 있도록 부인방지토큰을 저장해 주는 서비스도 필요하다고 하겠다.

5. 배달 또는 내용 증명을 보장하는 등기 우편

국내에는 수천 개의 우체국이 국민의 생활하는 가까운 곳에 위치하고 있으며, 이로 인하여 종이 우편의 각종 서비스를 제공하고 있다. 인터넷의 보급에 따라 국민 모두가 인터넷 주소를 가지게 되고, 정보통신부의 집중 투자로 저렴한 국민 PC가 보급된다면 가까운 시일 내에 모든 국민이 사이버 공간을 이용하는 정보화 시대를 맞이하게 될 것이다. 이를 계기로 사이버 공간을 통한 각종 서비스가 발굴될 것이며 그 중 전자 우체국을 통한 기존에 종이 우편물의 배달 증명 또는 내용 증명을 가능하게 하는 등기 우편 서비스가 보급되리라고 예측된다. 이러한 서비스 구현에는 반드시 전달되는 메시지의 송, 수신의 부인을 방지하는 기법과 전송 정보의 무결성을 확보하여 내용 증명을 할 수 있는 서비스에 부인 방지 서비스가 활용될 수 있다.

III. 관련연구

1. 연구동향

현재 부인방지 메커니즘 개발과 관련하여 연구되고 있는 주요 분야는 국제 표준으로 제시된 메커니즘들이 충족시키고 있지 못한 부분에 대한 보완과 효율성 개선이라는 두가지측면에서 접근이 이루어지고 있다.

표준 메커니즘들이 만족하고 있지 못한 요소로는 수신자의 선택적 수신(selective receipt)문제와 공정성(Fairness)문제가 있다. 선택적 수신 문제는 메시지의 수신자가 메시

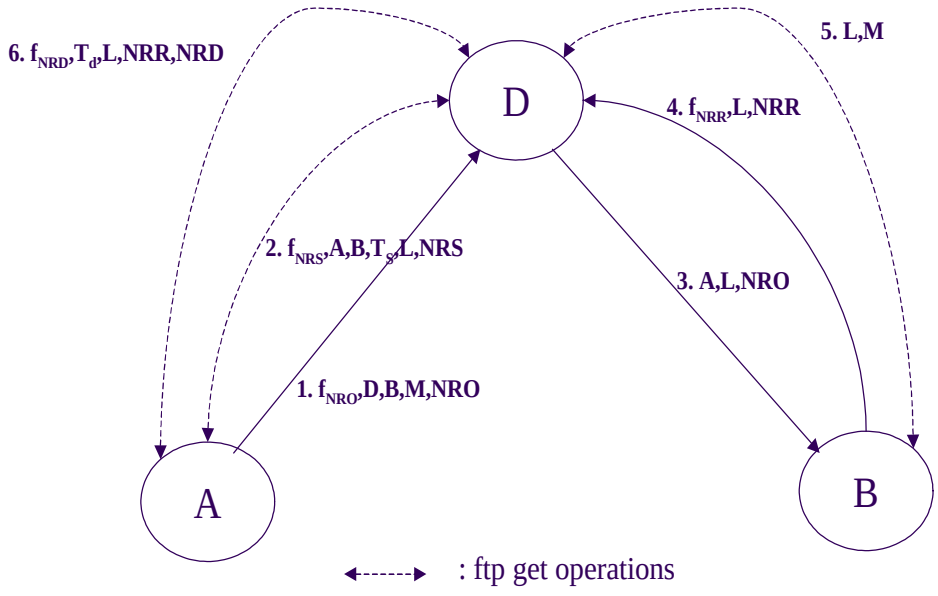
지의 내용은 파악을 하고 메시지 수신사실을 부인하는 경우에 대한 대비책이며, 공정성 문제는 부인방지 메커니즘의 프로토콜을 수행하는 도중 임의의 단계에서 프로토콜이 중단되는 경우 프로토콜 참여자의 정보획득 양이 동등해야하며 어느 한쪽도 유리하지 않아야 한다는 점이다. 이와 관련하여 개선된 부인방지 메커니즘을 제안하기 위해 J. Zhou와 D. Gollmann등이 연구를 수행하고 있다[1,2,4,9].

효율성 개선과 관련한 연구로는 주로 기존의 부인방지 메커니즘이 크게 의존하고있는 제3의 신뢰기관인 TTP(Trusted Third Party)의 의존도를 줄이는 방향으로 연구를 수행하고 있다. 부인방지와 관련한 모든 서비스를 제공하기 위해 TTP를 항시 개입하기보다는 필요시에만 TTP에 의존하는 방식에 관한 연구가 이루어지고 있으며, 또한 프로토콜 수행을 위한 통신량을 줄이는 방법에 대한 연구도 병행하여 이루어지고 있다. 이와 관련한 연구로는 Server-Supported Signature에 근간하여 부인방지 토큰 생성을 지원하도록 하는 서버를 채택한 N. Asokan의 부인방지 메커니즘 연구 및 프로토콜의 공정성과 효율성을 동시에 만족시키기 위한 J. Zhou 등의 최근 연구가 있다[3,4].

2. 주요연구결과

가. J. Zhou와 D. Gollmann 기법(이하 "ZG기법"이라 함)

[1]에서 제시한 ZG기법은 선택적 수신(selective receipt)문제 및 메시지 전송 시간과 관련된 분쟁의 해결을 위해 채택되어지는 것으로 납기시점이 중요한 요소로 작용되는 Electronic Bill Payment System에 적용이 가능한 시간 정보를 포함하는 공정한 부인방지 프로토콜을 제시하고 있다. [1]에서 제시된 프로토콜의 구성은 (그림 1)과 같다.



(그림 1) 공정한 부인방지 프로토콜

프로토콜에 사용된 주요 기호의 정의는 다음과 같다.

L: D에 의해 메시지 M에 부여하기 위해 선택되어진 유일한 레이블

Ts : D가 A의 제출 내용을 수신한 시간

Td : 메시지 M이 배달되어 수신자 B가 이용 가능한 시간

NRO= $sS_A(f_{NRO}, D, B, M)$: 메시지 M의 송신 부인방지

NRS= $sS_D(f_{NRS}, A, B, T_s, L, NRO)$: 메시지 M의 제출 부인방지

NRR= $sS_B(f_{NRR}, D, A, L, NRO)$: L로 레이블된 메시지 M의 수신 부인방지

NRD= $sS_D(f_{NRD}, A, B, T_d, L, NRR)$: 메시지 M의 배달 부인방지

나. K. Kim, S. Park, J. Baek의 기법(이하 "KPB기법"이라 함)[2]

KPB기법에서는 ZG기법이 B가 A로부터 받은 암호문을 지워버려 A가 D로부터 키 확인 인증서를 받은 경우에도 B는 암호문을 복호화할 길이 없는 경우를 방지하기 위하여 키 확인 인증서에 시간 제한(time limit) T를 두어 해결한다. 또한 ZG기법이 A와 B가 주고받는 메시지들에 대한 비밀성을 보장하지 못하는 단점을 보완한 기법을 제시하였다.

다. N. Asokan의 기법

[3]에서 N. Asokan은 Server-Supported Signature라고 불리는 방식을 이용한 송수신 부인방지 기법을 제시하고 있다. Server-Supported Signature는 일방향 해쉬 함수와 전통적인 전자서명에 의존하고 있으며, 효율성은 대칭키 암호시스템을 이용한 경우와 대등하다고 할 수 있다. 여기서는 부인방지 토큰 생성을 지원하는 서명서버라고 불리 우는 제삼 참여자의 사용에 의존하여 ISO의 대칭키 기술과는 달리 서명 서버들은 검증 가능하다 즉, 만약 그들이 잘못 행동한다면 희생자는 분쟁해결 시점에서 그러한 사실을 증명할 수 있다.

각 사용자 P는 비밀키 K_P를 생성하고 K_P를 기초로 해쉬 체인(hash chain)인 $K_P^0 = K_P, K_P^i = h_P^i(K_P) = h_P(K_P^{i-1})$을 계산한다.

여기서 $K_P^0 = K_P, K_P^i = h_P^i(K_P) = h_P(K_P^{i-1})$이다. $V_P = K_P^n$로 P의 루트 검증키이며, 이것이 P로 하여금 n개의 메시지를 인증할 수 있도록 해 준다.

송수신 부인방지를 Server-Supported Signature를 이용한 프로토콜은 (그림 2)와 같다. 여기서 대괄호([])는 그 안에 포함된 메시지가 기밀성이 유지되는 채널을 통해 전달됨을 의미하며, NRO 토큰은 $(Sig_S(O|m|d|K_O^i), K_O^{i-1})$로 구성되며, NRR토큰은 $(Sig_S(R|NRR:m|d|K_R^i), K_R^{i-1})$로 구성된다. 이 프로토콜은 NRO토큰 또는 NRR토큰이 선택적으로 사용될 수 있도록 한다.

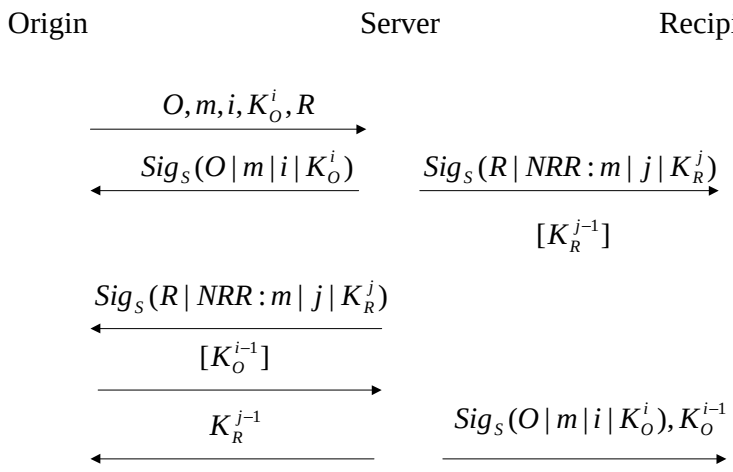
송신부인에 대한 분쟁이 발생한 경우 수신자 R은 (x, y)쌍을 중재자에게 보내 그들이 송신자 O의 i번째 토큰 검증키를 이용해서 메시지 m에 대한 NRO를 구성하고 있다고 주장한다. 중재자는 다음의 과정을 수행하여 부인여부를 검사한다.

1) 검증키 K_O^n과 V_s를 추출하여 그들이 CA(Certificate Authority)에 의해 인증되었음을 검증한다.

2) 토큰에 대한 Server의 서명이 유효한지를 검증한다.

이러한 검사가 성공하면 송신자는 CA나 Server가 거짓을 하고 있다는 것을 증명함으로

써 토큰을 부인할 기회를 갖게 된다. 이는 동일한 토큰 공개키에 해당하는 다른 부인방지 토큰을 보임으로써 가능하다.



(그림 2) 송수신부인방지를 제공하는 프로토콜

라. J. Zhou, R. Deng, F. Bao의 기법(이하 “ZDB기법”이라 함)

[4]에서 J. Zhou, R. Deng, F. Bao등은 TTP에의 의존성을 최소화하는 기법을 제안하였다. 즉 일반적인 문제해결은 당사자들(송신자 O와 수신자 R)끼리 해결하고 분쟁이 발생하였을 때에만 TTP에 문제해결을 요구하는 방식이다. 여기에서는 메시지 M을 비밀키 K와 이것으로 암호화한 암호문 C로 나누어 보내는 방법을 이용하고 있다.

ZDB기법이 충족하고 있는 공정한 메시지 전달 프로토콜의 요구사항으로는 다음과 같은 것들이 있다.

- o 효율성(Effectiveness) : 두 당사자가 정확하게 행동하면 그들은 TTP의 도움 없이 원하는 메시지를 얻을 수 있다.
- o 공정성(Fairness) : 프로토콜 수행 후 두 당사자는 기대했던 정보를 얻거나 또는 어떤 유용한 정보도 얻을 수 없다.
- o 임의 중단성(Timeliness) : 프로토콜 수행 중 어느 순간이라도 참가자는 공정성을 잃지 않고 프로토콜 수행을 중단할 수 있다.
- o 부인방지(Non-repudiation) : 어떤 메시지가 송신자 O로부터 수신자 R로 전달되었다면 O는 송신 사실을 부인할 수 없고 R은 수신 사실을 부인할 수 없다.
- o 제3자 부정의 검증성(Verifiability of third party) : 제3자의 부정한 행위로 참여자의 공정성이 침해되었을 경우 참여자는 그 사실을 증명할 수 있다.

ZDB기법은 교환(exchange), 중단(abort), 해결(resolve)의 세 가지 하부 프로토콜로 구

성되어 있으며, 여기에서는 송신자 O와 수신자 R 사이의 채널은 기밀성(confidentiality)이 보장되며, TTP와 당사자(O 또는 R)와의 채널은 메시지 전달이 보장된다(resilient)고 가정한다. 본 논문에서는 교환 프로토콜만을 제시하며 사용된 기호는 해당 논문을 참조하기 바란다.

o 교환 프로토콜

1) $O \rightarrow R$: $f_1, f_5, R, L, C, TTP, eP_{TTP}(K)$, EOO_C, sub_K

IF R gives up THEN quit ELSE

2) $R \rightarrow O$: f_2, O, L, EOR_C

IF O gives up THEN abort ELSE

3) $O \rightarrow R$: f_3, R, L, K, EOO_K

IF R gives up THEN resolve ELSE

4) $R \rightarrow O$: f_4, O, L, EOR_K

IF O gives up THEN resolve

3. 각 연구 결과의 비교분석

본 장에서 검토한 부인방지 메커니즘 관련 각 연구 결과들에 대한 제공기능 및 효율성 등의 장단점에 대한 비교를 [표 1]에 요약하였다.

[표 1] 각 연구결과의 비교

연구결과 / 비교항목	ZG 기법	KPB 기법	Asokan 기법	ZDB 기법
부인방지 제공 서비스	송신/수신/배달 (배달시간 증명 가능)	송신/수신/배달	송신/수신	송신/수신
TTP의 주요 역할	DA*	DA	공증서버	부분적DA
TTP 의존도	높음 (In-Line)	높음 (In-Line)	중간 (토큰 생성 지원:In-Line)	낮음 (필요시에만 개입:On-Line)
프로토콜 통신량	높음	높음	낮음	낮음
선택 수신 방지 여부	○	○	×	○
Fairness 충족 여부	○	○	×	○

* DA : Delivery Authority

IV. 부인방지 국제표준 분석

1. 표준화 동향

현재 부인방지 메커니즘과 관련하여 표준화가 이루어져 있는 부분으로는 OSI 환경에서의 송수신 부인 방지 서비스를 규정하는 Open System Interconnection-Security Framework in Open Systems - Part 4 : Non-Repudiation 과 ISO/IEC 13888의 Part 1,2,3가 있다. 본 논문에서는 다양한 부인방지 메커니즘을 제시하고 있는 ISO/IEC 13888의 Part 1,2,3를 토대로 제공되는 다양한 부인방지 메커니즘을 분석한다. ISO/IEC 13888은 암호기술을 이용하여 부인방지 메커니즘을 규정하는 일반적인 모델을 정의하고, 다양한 부인방지 서비스에 대한 일반적인 부인방지 메커니즘을 설명하고 있는 ISO/IEC 13888-1 Information technology - Security techniques - non-repudiation - Part 1: General, 전자 봉투와 부가 데이터로 구성되어 분쟁 발생 시에 이용이 가능한 부인방지 토큰을 대칭 암호 기술을 이용하여 제공하고 있는 부인방지 메커니즘을 규정하는 ISO/IEC 13888-2 Information technology - Security techniques - non-repudiation - Part 2 : Mechanisms using symmetric techniques와 비대칭 기술을 사용해서 특정 통신관련 부인방지 서비스를 위한 메커니즘을 명시하고 있는 ISO/IEC 13888-3:1997(E) Information technology - security techniques - Non-repudiation - Part 3: Mechanisms using asymmetric techniques로 구성된다.

2. ISO 13888 - Part 1,2,3

가. Part 1

[5]에서 제시되고 있는 부인방지 메커니즘의 일반 모델은 다음과 같다. 각 메커니즘에 사용된 용어는 표준의 내용을 준용한다.

o TTP 보안토큰을 사용한 부인방지

이 방법에서 증거는 TTP에게만 알려진 비밀키로 감추어진 보안토큰으로 구성된다. TTP는 송신자 혹은 수신자의 요구에 의해서 보안토큰을 생성하고 증거사용자나 중재자를 위해서 검증할 수 있다. 이 경우 TTP는 증거 생성자인 동시에 검증자가 되며, 송신자와 수신자는 TTP에 보안토큰 생성 요구와 함께 데이터를 전송한다. 이러한 요구는 무결성 및 기밀성 보호가 이루어져야 하고, 이러한 유형의 보호 방법을 전자봉투라고 한다.

o 보안토큰과 변조방지 모듈을 사용한 부인방지

이 방법에서 행위에 대한 증거는 증거생성자, 검증자 및 심판관에 의해 소유된 변조방지 암호 모듈에 저장된 비밀키로 감추어진 보안토큰으로 구성된다. 변조방지 모듈은 비밀키에 의해 수행되는 기능을 제한하고 모듈 외부로 키 값을 노출시켜서는 안된다. 증거생성자 모듈은 보안토큰을 생성하기 위해 비밀키가 사용되는 것을 허용하는 반면 검증자 및 심판관에 의해 소유되는 모듈 안의 비밀키는 단지 토큰 검증을 위해서만 사용이 가능하다. 논쟁 발생 시 증거사용자는 봉인된 토큰을 심판관에게 제출하고 증거생성자 모듈에 의해 생성되었음을

주장한다.

o 전자서명을 이용한 부인방지

이 방법에서 증거는 전자적으로 서명된 자료구조로 구성된다. 증거 생성을 위해서는 서명키로 서명을 생성하고 증거 검증을 위해서는 검증키로 서명검증을 수행한다. 송신증명 부인방지를 위해서 증거는 데이터에 대한 전자서명이 된다. 배달 증명을 위해서는 서명된 응답신호(ACKnowledge)가 증거로서 요구되며, 보안정책에 의존해서 송신자나 수신자는 타임스탬프와 같은 다른 증거를 제공할 것을 요구받기도 한다. 만약 심판관이 논쟁 해결을 위해 Time Stamping을 요구할 경우 송수신자와는 다른 신뢰기관으로부터 정보를 얻어내야만 한다. 검증자나 심판관은 증거 검증을 위해서 검증키 값을 얻을 수 있어야 하며, 만일 심판관이 증거 생성자의 공개키를 획득할 수 있다는 것을 보장하지 못할 경우 증거는 검증키를 위한 인증서를 포함하고 있어야 한다.

o Time Stamping을 사용한 부인방지

증거 생성 요구자로부터 신뢰할 수 있는 시간 참조 요구가 있을 때 그리고 전자서명이나 보안토큰을 생성하는 개체에 의해 제공되는 클럭을 신뢰할 수 없을 경우 Time Stamping을 제공하는 TTP에 의존하는 것이 필요하다. 이러한 Time Stamping은 서명키 값이 누출되기 전에 서명되었고 결국 메시지가 위조되지 않았음을 보장하기 위해 사용될 수 있다. TTP의 역할은 Time Stamping 요구를 받았을 때 Time Stamping 정보에 대한 전자서명 또는 보안토큰을 제공한다. Time Stamping은 부인방지 서비스 요청자에 의해 요구되며 부인방지 서비스 요청자의 인증을 요구하지는 않는다. 또한 서명 생성 또는 토큰 생성과 결합된다. 만약 전자서명을 생성하는 개체가 신뢰할 수 있는 개체를 포함하고 있다면 대응서명(counter-signature)은 요구되지 않는다.

o In-line TTP를 사용한 부인방지

In-line TTP 도구는 부인방지 서비스 요청자에 의해 명시적으로 요구될 수 있거나 암묵적으로 제공될 수 있다. In-line TTP는 부인방지 서비스가 요구되고 증거 사용자에게 증거를 제공하는 모든 상호 작동에 있어 중간자로서 행동하며, 모든 경우에 있어서 자료를 중개하고 사건이나 행위를 감시한다. TTP는 사후 논쟁 해결을 위해 기록을 남기며, TTP에 의해 기록 유지되는 증거로서 데이터 또는 데이터에 대한 fingerprint가 될 수 있다.

o 공증에 의한 부인방지

공증 메커니즘은 무결성, 송신지, 시간 그리고 목적지 등과 같은 두 개 이상의 개체간에 통신하는 자료의 속성에 관한 보장을 제공한다[8]. 공증인은 위와 같은 보장을 제공하기 위해 전자서명, 암호화 및 무결성 메커니즘 등을 사용할 수 있다. 증거생성을 위해서 공증인은 증거를 식별하기 위해 사용되어질 수 있는 기록번호를 사용할 수 있다. 증거 검증을 위해서 공증인은 증거의 정당성을 확인해 줄 수도 있다.

나. Part 2

[6]에서 제시된 대칭형 암호기술을 이용한 부인방지 메커니즘은 다음과 같다. 비밀키를 공유하고 있는 두 실체들은 전자봉투(SENV)로 알려진 데이터 무결성을 위한 방법을 이용하여 서로에게 메시지를 전달할 수 있다. SENV는 입력 데이터의 항목들을 비밀키로 보호

하여 형성된다. SENV는 또한 TTP만이 가지고 있는 비밀키를 이용하여 TTP가 증거를 생성하고 검증하는 데 이용될 수 있다.

본 표준에서 사용된 주요 기호의 의미는 다음과 같으며, 명시되지 않은 기호의 의미는 표준문서를 준용한다.

- Imp(y) : 데이터 스트링 y의 각인, y는 (1)데이타 스트링 y의 해쉬코드, 혹은 (2)데이타 스트링 y.
- $SENV_X$: 실체 X의 비밀 키 x로 생성된 전자봉투(secure envelope).
- y||z : 순서대로 y와 z의 연접의 결과.
- A, B :실체의 구별되는 식별자.
- f, f_i : 부인방지 서비스 종류를 의미하는 데이터 항목(플래그)
- $MAC_X(y)$: 실체 X의 키를 사용하여 데이터 y에 계산되는 암호화된 검사값
- Pol : 증거에 적용하는 부인방지 정책 (혹은 정책들)의 구별되는 식별자.
- TSA : 신뢰받는 타임 스탬핑 기관.
- TST : TSA에 의해 생성된 타임 스탬핑 토큰.
- TTP : 제 3의 신뢰기관.

전자 봉투를 만드는 방법은 대칭키의 무결성 기법들을 이용한다. 실체 X의 비밀 키 x는 데이터 z에 첨부된 암호화된 체크 값 $MAC_X(z)$을 계산하기 위해 사용된다. 전자봉투는 다음과 같이 구성된다.

$$SENV_X(z) = z \parallel MAC_X(z)$$

각각의 부인방지 서비스 제공을 위한 토큰의 구성은 다음과 같다.

o 송신 부인방지 토큰(NROT)

NROT는 송신자의 요청으로 TTP에 의해 생성된다.

$$NROT = text \parallel z1 \parallel MAC_{TTP}(z1)$$

$$z1 = Pol \parallel f1 \parallel A \parallel B \parallel C \parallel D \parallel Tg \parallel Q \parallel Imp(m)$$

o 수신 부인방지 토큰(NRDT)

NRDT는 수신자의 요청으로 TTP에 의해 생성된다.

$$NRDT = text \parallel z2 \parallel MAC_{TTP}(z2)$$

$$z2 = Pol \parallel f2 \parallel A \parallel B \parallel C \parallel D \parallel Tg \parallel T2 \parallel Q \parallel Imp(m)$$

o 제출 부인방지 토큰(NRST)

NRST는 배달기관(DA)에 의해 생성된다. 배달기관인 제3의 신뢰기관은 NROT 혹은 NRDT을 생성하는 기관과 같을 수 있다.

$$NRST = text \parallel z3 \parallel MAC_{DA}(z3)$$

$$z3 = Pol \parallel f3 \parallel A \parallel B \parallel C \parallel D \parallel E \parallel Tg \parallel T3 \parallel Q \parallel Imp(m)$$

o 전달 부인방지 토큰(NRTT)

전달 부인방지 토큰(NRTT)은 배달기관(DA)에 의해 생성된다.

NRTT = text|| z4 || MAC_{DA}(z4)

z4 = Pol || f4 || A || B || C || D || E || Tg || T4 || Q || Imp(m)

o 타임스탬핑토큰(TST)

TSA에 의해 제공된 TST는 다음과 같이 정의된다.

TST = text || z5 || MAC_{TSA}(z5)

z5 = Pol || f5 || TSA || Tg || Q || Imp(m)

다. Part 3

[7]에서 제시된 비대칭형 암호기술을 이용한 부인방지 메커니즘은 다음과 같다. 본 표준에서 사용된 주요 기호의 의미는 다음과 같으며, 명시되지 않은 기호의 의미는 표준문서를 준용한다.

- A : 메시지 송신자 A의 식별자
- B : 메시지 수신자 B의 식별자
- DA : 배달기관, 제3의 신뢰기관
- f_i : 유효한 부인방지 서비스 종류를 지시하는 자료 항목
- S_X : 서명 알고리즘과 개체 X의 개인 키를 사용한 서명 기능

o 송신 부인방지 토큰(NROT)

NROT는 메시지 송신자의 허위 부정을 막기 위해 사용되어진다. NROT는 메시지 m의 송신자 A(또는 인증기관 C)에 의해 생성되며 A에 의해 수신자 B에게 보내진다. 수신자 B는 이를 검증 후에 저장할 수 있다.

NROT의 구조는 다음과 같다.

NROT = text1 || z1 || S_A(z1),

z1 = Pol || f1 || A || B || C || Tg || T1 || Q || Imp(m)

o 수신 부인방지 토큰(NRDT)

NRDT는 수신자의 메시지 m의 수신 및 내용의 인지에 대한 허위 부인을 방지하기 위해 사용되어진다. NRDT는 수신자 B(또는 인증기관 C)에 의해 생성되며 B에 의해 메시지 송신자 A를 포함한 하나 또는 그 이상의 개체에게 송신된다. 검증 후에 이들 개체들에 의해 저장된다.

NRDT의 구조는 다음과 같다.

NRDT = text2 || z2 || S_B(z2)

z2 = Pol || f2 || A || B || C || Tg || T2 || Q || Imp(m)

o 제출 부인방지 토큰(NRST)

NRST는 배달기관에 의해 생성된다. 이 경우에 있어서 증거 생성자는 배달기관 DA가 된다. 송신자 A 또는 선행 배달기관 X는 메시지 m을 배달기관 DA로 송신한다. 배달기관 DA는 메시지 m을 수신하고 NRST는 A 또는 선행 전달자 X에게 송신함으로써 메시지가

전방으로 배달하기 위해 제출되었다는 증거를 제공하게 된다.

NRST는 배달기관 DA에 의해 생성되며 DA에 의해 메시지 송신자 A 또는 선행 배달기관 X에게 송신된다. 이것은 검증 후에 A또는 X에 의해 저장된다.

NRST의 구조는 다음과 같다.

NRST = text3 || z3 || S_{DA}(z3)

z3 = Pol || f3 || A || B || C || D || E || Tg || T3 || Q || Imp(m).

o 전달 부인방지 토큰(NRTT)

NRTT는 메시지 m이 배달기관 DA에 의해 B에게 전송되었다는 증거로서 메시지 송신자에 의해 사용된다. 이 경우에 있어서 증거 생성자는 배달기관 DA가 된다. 송신자 A 또는 선행 배달기관 X가 메시지 m을 DA로 송신한다. DA는 메시지 m을 수신자 B 또는 후위 배달기관에 전송한다. 메시지 m을 수신자 B에게 전송한 DA는 또한 NRTT를 메시지 m의 송신자 A에게 송신함으로써 메시지 m이 B에게 전송되었다는 증거를 제공하게 된다.

NRTT는 배달기관 DA에 의해 생성되며 DA에 의해 메시지 송신자 A에게 송신된다. A는 이를 검증 후 저장한다.

NRTT의 구조는 다음과 같다.

NRTT = text4 || z4 || S_{DA}(z4)

z4 = Pol || f4 || A || B || C || D || Tg || T4 || Q || Imp(m)

V. 국제표준의 문제점 및 대책

최근 국내의 정보보안 기술은 크게 발전하고 있으며 인터넷의 확장, 정보화의 진전, 전자상거래 시장의 활성화 등 정보보안 기술의 시장수요는 크게 증가하고 있다. 그러나 정보보안기술이 본격적으로 적용되기 위해서는 공개키기반구조(PKI), ***부인방지서비스*** 등 암호 기반구조를 갖추는 것이 필요하다. 이것은 정보화 사회에서 각 개인의 신분을 인증하고 분쟁발생시의 문제해결 능력을 보유함으로써 정보화 사회의 진전을 가능하게 하는 것이다. 기존의 부인방지 국제 표준이 가지고 있는 보완해야할 문제점으로는 다음과 같은 것들 있다.

- o 선택적 수신(selective receipt)등의 문제를 해결하고 공정성이 부여된 부인방지 서비스를 제공하여야 한다.
- o 부인방지서비스에서 제 3의 신뢰기관(TTP)의 개입을 최소화하여 서비스의 효율성을 향상시킬 수 있어야 한다.
- o 사용자시스템은 고장, 도난, 시스템의 변경 등 장애가 발생할 가능성이 많으며 이러한 경우에도 부인방지 서비스를 제공할 수 있도록 내장애성을 제공해야 한다.
- o 부인방지 서비스는 효율성을 증가시키기 위하여 인증기관, 디렉토리시스템 등의 다른 기반구조와 통합하여 운용될 수 있으며 이러한 통합 운용성을 제공하여야 한다.
- o 부인방지 서비스는 컴퓨터시스템, 이동통신단말시스템, 유·무선 네트웍 등 다양한 환경에서 사용될 수 있으며 이러한 이종의 환경에서도 상호 호환 운영될 수 있어야 한다.

또한, 국내 부인방지 표준을 위해서는 다음과 같은 요구사항을 고려해야 한다.

- o 표준화되는 기술의 안전성을 보증할 수 있어야 한다.

o 사용이 편리하여 널리 사용될 수 있어야 한다.
o 기존의 연구결과로 제시된 문제점 및 그 해결이 가능한 메커니즘을 국제 표준에 반영하여 국제적으로 통용되는 표준들을 제시함으로써 상호 호환이 될 수 있어야 한다.

최근 부인방지서비스와 관련하여 3장에서 기술한 바와 같이 다양한 연구들이 이루어지고 있으나 아직 충분한 검토가 이루어지지는 못한 것으로 보인다. 이러한 기술들을 표준안으로 포함시키기 위해서는 안전성 검증 등을 위한 종합적인 검토가 요구된다.

VI. 결론

본 논문에서는 최근 인터넷 등과 같은 공중 통신로를 통하여 전자적인 서비스를 제공할 경우에 약속된 프로토콜에 위반한 송수신자 쌍방간의 행위에 기술적인 증거를 제공하고, 논쟁 발생 시 법적 근거로 제공할 수 있는 부인방지 서비스 메커니즘에 대해 기존의 다양한 메커니즘의 이론적, 실제적인 사례들을 조사하였고, 현재 부인방지 메커니즘 개발과 관련한 최근의 국내외 연구현황을 분석하였으며, 분석된 내용을 토대로 기존 메커니즘들이 가지고 있는 문제점들을 분석해 보고 표준안 개발을 위해 요구되는 사항들을 정리하였다.

향후 과제로는 부인방지 메커니즘에 가해지는 보안 위협요소에 대한 면밀한 분석을 통하여 안전성이 증명된 부인방지 서비스의 개발이 이루어져야하며 이를 토대로 한 다양한 응용의 개발을 이루어져야 부인방지 표준이 널리 활용될 수 있을 것으로 생각된다.

참고문헌

[1] J. Zhou and D. Gollmann, “Observations on Non-repudiation”, Proc. of ASIACRYPT '96, LNCS 1163, Springer-Verlag, pp. 133-144

[2] Kwangjo Kim, Sangjoon Park, Joonsang Baek, “Improving fairness and privacy of Zhou-Gollman's Non-repudiation Protocol”, IEEE International Workshop on Security, Aizu, Sep.23-24, 1999.

[3] N.Asokan, Fairness in Electronic Commerce, Ph.D thesis, University of Waterloo, 1998

[4] J. Zhou, R. Deng, F. Bao, “Some Remarks on a Fair Exchange Protocol”, to be appeared in PKC2000, Jan. 2000

[5] ISO/IEC 13888-1:1997(E) Information technology - Security techniques - Non-repudiation Part 1: General

[6] ISO/IEC 13888-2:1998(E) Information technology - Security techniques - Non-repudiation Part 2: Mechanisms using symmetric techniques

[7] ISO/IEC 13888-3:1997(E) Information technology - Security techniques - Non-repudiation Part 3: Mechanisms using asymmetric techniques

[8] 김장성, 장영달, 김지홍, “전자공증 서비스에 관한 연구”, 개방형 보안기술과 정보보호응용 워크샵, 제2회, pp.99-116, 1998.11

[9] J. Zhou, Non-repudiation, Ph.D Thesis, Royal Holloway, U. of London, 1997.