통합통신대화기에서 인증체계개발의 한가지 방법

최정혁, 안창혁

SIP는 다매체통신에서 가장 많이 리용하는 신호조종규약이며 현재 SIP에서의 인증실현은 보다 중요한 문제로 나서고있다.

론문에서는 선행방법들[1－3]을 분석한데 기초하여 SIP에 기초한 통신에서의 인증체계들을 해석하였다. 그리고 통합통신대화기에서의 인증체계개발을 새롭게 제기하고 그 실현을 위한 한가지 방법을 제기하였다.

1. 인증처리과정

현재 SIP에서의 인증수법[2]은 HTTP에 기초한 인증이며 그런것으로 하여 여러가지 공격으로 피해를 당하고있다.

여기서는 대표적인 대리인증체계인 NIST[3]에서 정의한 수자인증모형체계를 분석하고 구체적인 인증처리과정에 대하여 서술하였다.

NIST수자인증처리과정을 그림 1에 보여주었다.

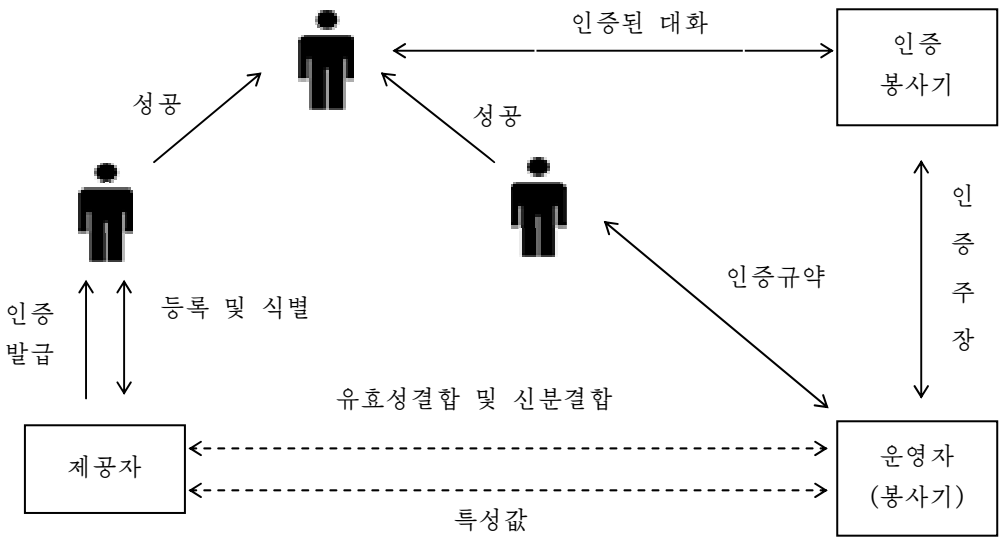

그림 1. NIST수자인증처리과정

이 모형에서 개별적인 사용자들은 제공자에게 먼저 등록을 한다. 일단 제공자가 사용자의 신분을 성공적으로 식별하면 사용자이름과 같은 신원정보들이 제공자와 사용자간에 확립된다.

사용자의 인증이 제공자에 의해서 성공하면 인증봉사기에서 제공하는 인증된 대화내에서 직결처리를 수행할수 있다.

이러한 처리에서 사용자는 운영자의 봉사기로부터 인증자들의 하나 혹은 그 이상의 소유항목들을 검사한다.

봉사기와 인증봉사기는 하나의 같은 봉사기일수도 있고 서로 갈라져있을수도 있다.

만일 봉사기와 인증봉사기가 갈라져있다면 봉사기는 사용자의 인증주장을 인증봉사기에 제공해야 한다.

그다음에 인증봉사기는 처리과정을 초기화하고 인증된 대화를 공유한다.

우의 모형에서 사용자는 제공자에 의해서 직접 인증될수도 있고 제공자가 보내는 특성값들로 인증을 실현하는 봉사기와 인증봉사기에 의해서도 인증될수 있다.

2. 모형화와 구성

우리가 개발한 통합통신체계에서는 사용자가 가입하려고 할 때 입력하는 정보(봉사기주소, 사용자이름, 암호)가 운영자의 봉사기에 전송된다.

사용자에 대한 인증은 운영자가 진행하지만 허가번호만은 제공자로부터 받는다.

통합통신체계의 특성으로부터 제공자와 운영자를 분리하여 운영자에게 봉사기를 부여하고 제공자는 사용자의 인증식별에 직접 관여하지 않는 방법을 새롭게 제안하고 모형화하였다.

제안한 인증모형을 그림 2에 보여주었다.

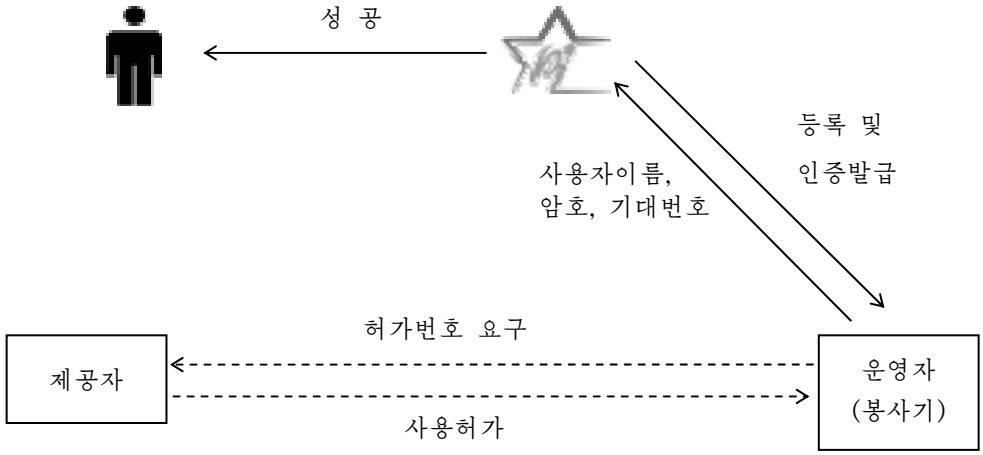

그림 2. 제안한 인증모형

운영자가 사용자의 기대번호를 제공자에게 보내면 제공자는 그 기대번호로부터 허가번호를 생성해준다.

하쉬함수를 리용하여 허가번호와 사용자암호로부터 새로운 암호를 생성하고 그것으로 사용자의 가입을 승인해주는것이 제안한 모형의 특성이다.

인증체계흐름도를 그림 3에 보여주었다.

그림 3에서 보여주는것처럼 제공자는 운영자의 봉사기에 허가번호만을 제공해주며 사용자등록과 인증은 운영자가 진행한다.

우에서 보여준 모형을 실현하기 위한 알고리듬은 다음과 같다.

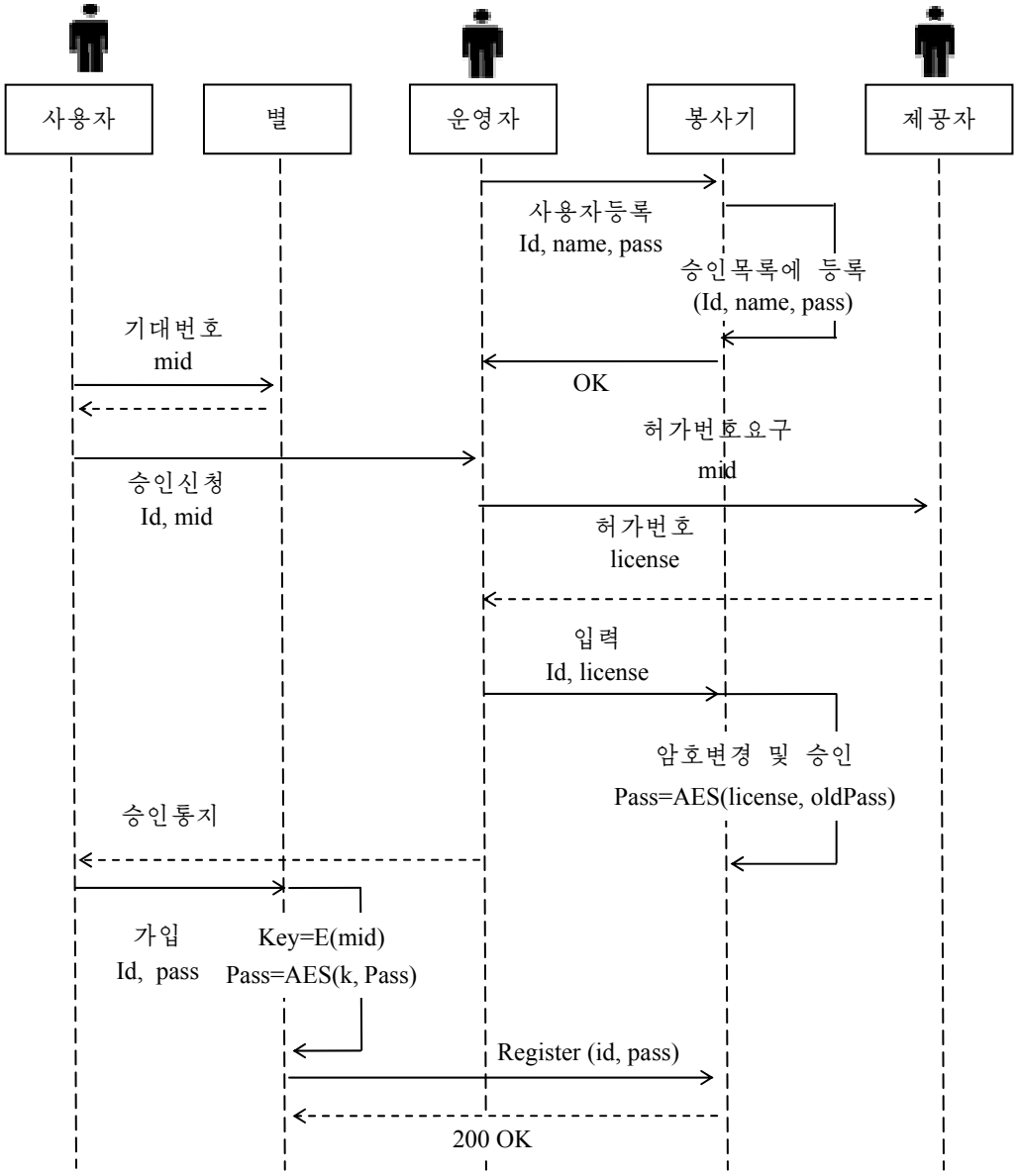

그림 3. 인증체계흐름도

C→AS: $ID_c \| P_c \| ID_v$

AS→V: Ticket1

V→AS: $K_v \| AES$

AS→C: Ticket2

C→AS: $E_v \| key \| R$

AS→C: Ticket3

여기서 C는 의뢰기(사용자), AS는 운영자(봉사기), V는 제공자, ID_c는 사용자의 식별자, P_c는 사용자의 통과암호, ID_v는 사용자의 기대번호, K_v는 허가번호, AES는 암호변경 및 승인, E_v는 열쇠암호, R는 등록, Ticket1은 허가번호요구, Ticket2는 승인통지, Ticket3은 200OK, ‖는

련결이다.

이 구조에서 사용자는 제공자에 가입하지 않고 봉사기에 접근을 요청한다.

사용자가 통합통신체계에 가입하면 자체의 식별자와 암호 그리고 기대번호를 가지고 가입을 신청한다. 운영자는 봉사기에 이러한 정보들을 등록하고 제공자에게 허가번호요구 신청을 한다.

제공자는 운영자에게 허가번호와 함께 암호변경기능을 승인해준다. 다음 운영자는 사용자에게 승인통지를 내려보내며 사용자는 가입을 하게 된다.

3. 결 과 분 석

제안한 방법은 3자인증체계를 통합통신대화기에 적용한것으로서 새로운 특성들을 가진다.

선행방법들과의 성능대비결과는 표와 같다.

표. 성능대비결과

구분	ECC	NIST	제안된 방법
제공자	없다	있다	있다
사용자－제공자 관계	없다	있다	없다
암호강도	낮다	일반	높다
기대번호	리용안함	리용안함	리용함

제안한 방법에서 기본은 사용자의 기대번호로부터 얻어지는 허가번호이다. 허가번호를 암호생성에 리용한것으로 하여 암호강도가 더 높아졌으며 제공자가 통일적으로 허가번호를 생성하여줌으로써 그것이 람발되거나 해득되는 경우를 미리막을수 있게 되였다.

맺 는 말

SIP를 리용하고있는 통합통신대화기에서 인증체계를 개선하기 위한 모형을 제기하고 그것을 실현하였다.

우리가 개발한 인증체계를 도입한 결과 인증과 보안을 우리 식으로 할수 있게 되였으며 개발단위와 운영단위사이 련동을 보장하고 협력하는데 도움이 되였다.

참 고 문 헌

[1] Y. Zhang et al.; Computer Standards and Interface, 31, 286, 2009.

[2] J. Rosenberg et al.; IETF RFC3261, 2002.

[3] Draft NIST Special Publication; Digital Authentication Guideline, 63, 3, 800, 2016.

주체107(2018)년 5월 5일 원고접수

A Method for Development of Authentication System in Integrated Communication Messenger

Choe Jong Hyok, *An Chang Hyok*

In this paper, we propose a method to improve of authentication system on combined communication messenger and evaluate its performance.

Key words: authentication, SIP