김일성종합대학학보
정보과학

주체109(2020)년
제66권 제4호

이동식구름계산에서 자료기지봉사의 보안을 위한 인증모형설계

리윤미, 황철진

콤퓨터망의 리용과 그 응용범위가 넓어지고있는 오늘날 콤퓨터망의 확대와 그를 통한 자료의 리용이 활발해지고있으며 특히는 웨브를 통한 자료처리가 중요한 문제로 나서고있다. 특히 콤퓨터망의 발전과 함께 리용되고있는 구름계산은 방대한 자료의 처리를 진행할수 있으며 이것은 자료들을 보관하고 리용하는 자료기지에 대한 보안을 강화할것을 요구하고있다.

론문에서는 Needham-Schroeder규약[1]이 가지고있는 위장공격에 대한 취약성을 분석한데 기초하여 이러한 취약점을 극복하기 위한 개선된 Needham-Schroeder규약을 설계하여 이동식구름계산에서 자료기지봉사(DBaaS)를 보호하기 위한 보안모형에서의 사용자인증을 진행하였다.

1. 개선된 Needham-Schroeder규약

자료기지봉사를 안전하게 하는 방법들은 보안봉사의 내용들인 기밀성, 인증, 무결성, 부인방지, 접근조종의 내용들을 포괄하여야 하며 이러한 방향에서 연구되고있다.

론문에서는 자료기지의 보안을 위하여 자료기지에 대한 리용과정을 계층화하고 개별적계층에서의 기능을 정의하였다. 또한 자료기지안의 내용들에 대한 암호화를 진행하여 자료기지안의 자료의 내용을 보호하는 방법들에 대하여 론의하였다. 그리고 자료기지의 리용과정에서의 사용자인증을 진행하기 위한 방법을 제안하였다.

자료기지에 대한 보안모형은 4개의 계층구조를 리용하며 여기서 개별적인 층은 구름층들의 자료보안을 담보하기 위한 기능[2, 3]을 수행한다.(그림 1)

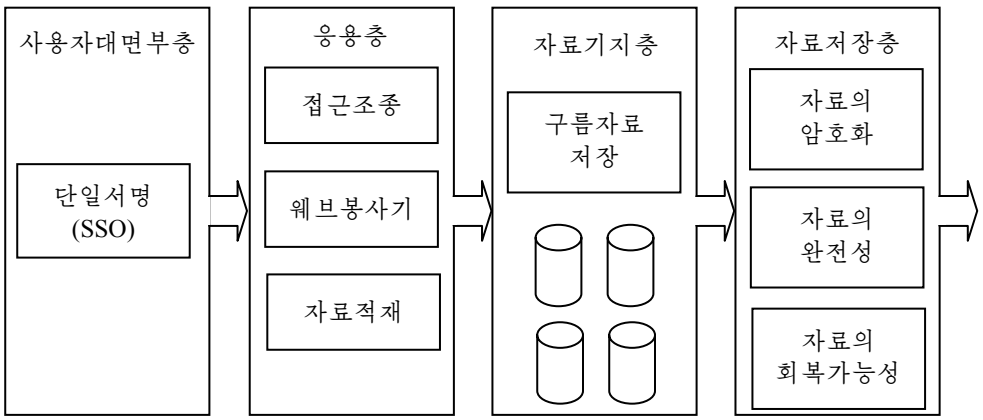

그림 1. 구름계산에서의 자료기지봉사의 보안모형

첫번째 층(사용자대면부층)은 한번의 암호인증을 통하여 사용자인증을 진행한다. 이

층은 인터네트를 통하여 봉사기에 접근하는데 리용된다. 이것은 사용자로 하여금 구름계산의 하부구조에서 확장가능하고 신축성있는 자료기지봉사들을 쉽게 리용하도록 한다.

두번째 층(응용층)은 구름계산에서 쏘프트웨어봉사와 기억공간을 호출하는데 리용된다. 사용자들은 하드웨어자원의 지원이 없이도 이러한 봉사를 리용할수 있다.

세번째 층(자료기지층)은 구름계산에 존재하는 자료기지를 관리하는 효과적이고 믿음성있는 봉사를 제공한다. 그것은 기억기에 존재하는 질문명령문들의 재사용을 가능하게 한다.

실례로 자료를 질문하고 적재하기 위한 시간을 절약하기 위하여 해당 질문명령문들의 재리용을 가능하게 한다.

네번째 층은 자료가 저장과 검색단계에서 각각 암호화되고 복호화되는 자료저장층이다. 이 층에서는 자료의 무결성과 자료회복가능성을 제공한다.

이러한 기능들을 수행하는 자료기지봉사에 대한 리용에서 중요한 문제는 자료기지봉사를 리용하는 사용자들에 대한 인증을 보다 원활하고 능동적으로 진행하면서 그 리용성능을 최대한 높이는것이다. 이 층에서 자료기지에 접근하는 사용자들에 대한 인증을 실현하기 위해 Needham-Schroeder규약을 리용한다.

초기의 Needham-Schroeder규약은 KDC(Key Delivery Center)와 2명의 참가자들을 포함하는 가장 일반적인 인증규약들중 하나이다. 이 규약은 2명의 통신자들에게 통신열쇠(비밀열쇠암호화에서의 비밀열쇠)를 배포하는것과 함께 사용자인증을 진행한다. 여기서는 사용자가 KDC에 봉사기의 식별자를 요청하면 KDC는 봉사기의 식별자와 함께 두 통신자사이의 통신열쇠를 보내주며 사용자는 그 통신열쇠를 다시 봉사기에 보내준다. 즉 봉사기는 KDC와 접속하지 않고 사용자가 접속하여 통신열쇠를 봉사기에 다시 보내준다.

보다 발전된 Needham-Schroeder규약은 KDC대신에 인증국(CA)의 도움으로 2명의 통신자들사이 인증을 진행하기 위해 공개열쇠암호화를 리용한다. 이 규약은 사용자(U), 봉사기(S), 인증국(CA)사이 련결을 안전하게 하기 위해 리용된다. 인증국은 통신에 포함되는 모든 참가자들에 의해 신뢰성이 보장된다고 본다.

CA는 공개열쇠와 비밀열쇠쌍 (P_{CA}, S_{CA}) 를 가지며 대화(Session)열쇠는 사용자들(U)과 봉사기(S)가 각각 K_U 와 K_S 로 공유한다.

증명서와 대화열쇠는 가입기간 매 사용자에게 발급된다. 증명서는 대화열쇠가 변화되여야 할 때 CA에 의해 서명된 봉사기에 대하여 ID와 일부 정보들을 포함한다.

만일 봉사기가 인증국에 의하여 믿음성이 담보된 조건에서 인증국이 사용자와 봉사기사이의 인증을 위한 중계적역할을 하면 이러한 규약에서는 사용자와 봉사기사이의 인증이 담보된다고 말할수 있다.

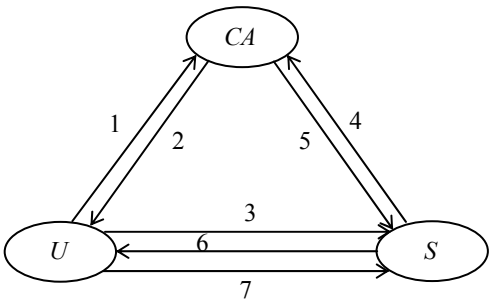

그림 2. 개선된 Needham-Schroder규약

이 규약은 침입자 T 에 의해 위장되는 약점[1]이 있다.

개선된 Needham-Schroder규약은 다음과 같다.(그림 2)

① $U \Rightarrow CA: \{T_U, P_S, U_{n1}\}\ P_{CA}$

② $CA \Rightarrow U: \{(U_{n1}, K_S, P_S)S_{CA}\}\ K_U$

③ $U \Rightarrow S: \{U_{n2}, P_U\}\ K_S$

④ $S \Rightarrow CA: \{T_S, S_{n1}, P_U\}\ P_{CA}$

⑤ $CA \Rightarrow S: \{(S_{n1}, K_U, P_U)S_{CA}\}\ K_S$

⑥ $S \Rightarrow U: \{T_S, U_{n2}, S_{n2}\} K_U$

⑦ $U \Rightarrow S: \{S_{n2}\} K_S$

여기서 리용하는 기호들의 의미는 다음과 같다.

U : 사용자

S : 봉사기

CA : 인증국

P_{CA} : 인증국의 공개열쇠

S_{CA} : 인증국의 비밀열쇠

K_U : 사용자와 인증국사이 공유된 대화열쇠

K_S : 봉사기와 인증국사이 공유된 대화열쇠

P_S : 봉사기의 공개열쇠

P_U : 사용자의 공개열쇠

U_n : 사용자에 의하여 생성된 임의의 통보문

S_n : 봉사기에 의하여 생성된 임의의 통보문

단계 ①과 ②는 그것들이 CA 의 공개열쇠와 U 와 CA 사이 공유열쇠(K_U)로 암호화되였기때문에 T 로부터 U 를 방어할수 있으며 따라서 T 는 S 의 ID를 볼수 없으며 S 에게 통보문을 전송할수 없다. 사실 통보문이 P_{CA} 대신에 T 의 공개열쇠로 암호화되였어도 T 는 열쇠가 U 와 CA 사이에만 공유되였기때문에 K_U 를 만들어낼수 없다. 단계 ⑤, ⑥, ⑦에서 통보문은 S 와 U 에 의해 복호화될수 있으므로 T 가 통보문을 얻을수 있다 해도 그 내용을 복호화할수 없다.

2. 개선된 Needham-Schroeder규약의 안전성평가

제안된 규약에 대한 해석을 보안규약분석도구인 BAN론리로써 다음과 같이 진행한다.

① 규약의 예상목표모임을 $\Gamma \supseteq \gamma$ 라고 할 때 이 예상목표는 통신쌍방사이에 공격자의 중간공격을 막고 사용자인증을 진행하는 안전한 통로를 확립하는것이다.

② 초기가설모임

$$CA|\equiv\#\{T_U, P_S, U_{n1}\}$$
$$U|\equiv\#\{(U_{n1}, K_S, P_S)S_{CA}\}$$
$$S|\equiv\#\{U_{n2}, P_U\}$$
$$CA|\equiv\#\{T_S, S_{n1}, P_U\}$$
$$S|\equiv\#\{(S_{n1}, K_U, P_U)S_{CA}\}$$
$$U|\equiv\#\{T_S, U_{n2}, S_{n2}\}$$
$$S|\equiv\#\{S_{n2}\}$$

초기가설모임과 론리규칙을 리용하여 최종목표모임(Γ)추론을 진행하자.

개선된 규약의 통보문 1을 론리언어로 표시하면 다음과 같다.

$$CA \triangleleft \{T_U, P_S, U_{n1}\}$$

우의 론리언어의 문법정의로부터 다음의 식이 성립한다.

$$CA|\equiv U|\sim\{T_U, P_S, U_{n1}\}$$

초기가설 $CA|\equiv\#\{T_U, P_S, U_{n1}\}$ 과 $CA|\equiv U|\sim\{T_U, P_S, U_{n1}\}$ 로부터 림시값검증규칙이 도출된다.

$$CA|\equiv U|\equiv\{T_U, P_S, U_{n1}\}$$

마찬가지로 통보문 2에 대해서도

$$U\lhd\{(U_{n1}, K_S, P_S)S_{CA}\},\ U|\equiv CA|\sim\{(U_{n1}, K_S, P_S)S_{CA}\}$$

이면

$$U|\equiv CA|\equiv\{(U_{n1}, K_S, P_S)S_{CA}\}$$

이고 통보문 3에 대해서

$$S\lhd\{U_{n2}, P_U\},\ S|\equiv U|\sim\{U_{n2}, P_U\}$$

이면

$$S|\equiv U|\equiv\{U_{n2}, P_U\}$$

이며 통보문 4에 대해서 $CA\lhd\{T_S, P_U, S_{n1}\}$, $CA|\equiv S|\sim\{T_S, P_U, S_{n1}\}$ 이면

$$CA|\equiv S|\equiv\{T_S, P_U, S_{n1}\}$$

이다.

통보문 5에 대해서 $S\lhd\{(S_{n1}, K_U, P_U)S_{CA}\}$, $S|\equiv CA|\sim\{(S_{n1}, K_U, P_U)S_{CA}\}$ 이면

$$S|\equiv CA|\equiv\{(S_{n1}, K_U, P_U)S_{CA}\}$$

이고 통보문 6에 대해서 $U\lhd\{T_S, U_{n2}, S_{n2}\}$, $U|\equiv S|\sim\{T_S, U_{n2}, S_{n2}\}$ 이면

$$U|\equiv S|\equiv\{T_S, U_{n2}, S_{n2}\}$$

이며 통보문 7에 대해서 $S\lhd\{S_{n2}\}$, $S|\equiv U|\sim\{S_{n2}\}$ 이면

$$S|\equiv U|\equiv\{S_{n2}\}$$

이다.

③ 최종목표모임도출

$$CA|\equiv U|\equiv\{T_U, P_S, U_{n1}\}$$
$$S|\equiv U|\equiv\{U_{n2}, P_U\}$$
$$CA|\equiv S|\equiv\{T_S, P_U, S_{n1}\}$$
$$U|\equiv S|\equiv\{T_S, U_{n2}, S_{n2}\}$$
$$S|\equiv U|\equiv\{S_{n2}\}$$

즉 $\Gamma\supseteq\gamma$ 이다.

따라서 이 규약은 안전하다.

맺 는 말

이동식구름환경에서 DBaaS를 보호하기 위한 보안모형을 제안하고 Needham-Schroeder 규약의 약점을 극복한 개선된 Needham-Schroeder규약을 리용하여 사용자인증을 진행하였으며 규약의 안정성을 해석하였다.

참 고 문 헌

[1] A. Alhaj et al.; Int. J. Cloud Appl. Comput., 3, 1, 34, 2013.
[2] M. ALzain, E. Pardede; Proceedings of 44th Hawaii International Conference on System Sciences, 1, 2011.
[3] N. Nagar, U. Suman; Int. J. Cloud Appl. Comput., 6, 1, 1, 2016.

주체109(2020)년 8월 5일 원고접수

Authentication Model Designing for the Security of Database Service in Mobile Cloud Computing

Ri Yun Mi, *Hwang Chol Jin*

In this paper, we designed a new security model for DBaaS(database as a service) in MCC(mobile cloud computing) and analyzed the weakness of the key distribution protocol Needham-Schroeder.

Then we designed the improved Needham-Schroeder protocol and authenticated user in security model.

Keywords: mobile cloud computing, database as a service