암호학적 프로토콜 분석을 위한 개선된 논리

주성범° 홍주형 김종훈
동아대학교 컴퓨터공학과
{linus°, hongma, jhkim}@donga.ac.kr

An Improved Logic for Cryptographic Protocol Analysis

Sungbeom Ju° Joohyung Hong Jonghoon Kim
Dept. of Computer Engineering, Donga University

요 약

BAN 논리와 같은 논리를 사용한 암호학적 프로토콜의 형식적 검증 방식은 프로토콜들의 다양한 결점들을 분석할 수 있다. 그러나 BAN 논리와 BAN의 확장된 논리들은 명시적 가정과 목적을 통해 프로토콜의 목적 성취 유무만을 추론할 수 있다. 본 논문에서는 기존의 논리들을 비교 분석하여 메시지 의미를 추론하는 규칙에 대한 정확한 해석에 대해 살펴본다. 그리고 암호학적 프로토콜의 보안 요구사항 중 하나인 메시지 무결성(message integrity)을 논리(logic) 범위에서 추론할 수 있는 방법을 제안한다.

1. 서 론

분산 환경에서 암호학적 프로토콜은 둘 이상의 참여개체(principal)에게 안전한 서비스를 제공하기위한 수단으로 사용된다. 안전한 프로토콜 설계는 매우 어려운 작업으로 프로토콜 설계원리나 검증을 통해 프로토콜이 가진 결점을 찾아낸다. 그러나 비형식적인 프로토콜 분석이나 잘 정의되지 않은 설계원리는 이러한 작업을 더욱 힘들게 한다[1].

Burrows, Abadi 그리고 Needham은 인증 프로토콜의 형식적 검증(formal verification)을 위한 믿음에 관한 논리[2]를 제안하였고, 현재까지 다양한 BAN 논리의 확장들이 제안되었다. BAN과 확장된 논리에 의한 형식적 검증은 프로토콜의 초기 가정들과 목적을 명시적으로 기술하고 프로토콜 기술 형태를 분석을 위한 형태로 변환하여 프로토콜이 가진 많은 취약점을 발견하였다[3]. 그러나 기존의 논리들은 추론 논리 자체에 여러 가지 문제점들로 인해 많은 한계점을 가지고 있다. BAN 부류(BAN family)의 추론 구성 방식(inference construction) 방식은 프로토콜에 일어날 수 있는 공격 가능성을 추론하는 것이 아닌 인증과 키 분배와 같은 프로토콜의 목적 성취 유무를 추론함으로서 추가되어야 할 가정과 결점을 찾아낸다[4,5]. 따라서 프로토콜에 잠재된 결점을 명시적으로 추론할 수 없으며 프로토콜의 보안 요구사항을 부분적으로 검증 가능하다.

본 논문에서는 BAN 부류 논리들을 비교 분석하고, 기존 논리에서 모호하게 해석될 수 있는 메시지 의미 규칙에 대해 살펴봄으로써 메시지의 근원지와 무결성의 개념을 분리한다. 그리고 기존의 논리가 검증할 수 없었던 보안 요구사항을 검증할 수 있는 추론 규칙(inference rule)을 새롭게 제안 할 것이다.

본 논문의 구성은 다음과 같다. 2절에서는 BAN 논리와 확장된 논리에 대해 비교 분석하고 기존 논리들의 개선점에 대해 짚어본다. 3절에서는 기존 논리들을 보완할 수 있는 개선된 논리를 제안하고, 마지막으로 결론 및 향후 연구방향에 대해 제시한다.

2. BAN 논리와 확장된 논리들의 비교 분석

인증 프로토콜의 형식적 검증을 위한 논리적 도구로써 선구자적 역할을 한 BAN 논리는 단순하며 적용이 쉽지만 논리에서 많은 가정을 요구하는 한계점을 지니고 있다[6]. BAN의 확장 논리들은 이러한 광범위한 가정들을 제거하고 프로토콜의 이상화 방식을 개선[7]하거나 강한 형식적 의미를 제안[8]하는 등 논리의 개선과 확장이 이루어 졌다. 그러나 이러한 검증 논리의 확장은 방대해진 추론 규칙의 수로 인해 분석이 복잡해졌고 추론 규칙의 형식적 의미가 여전히 모호하다.

BAN 논리와 그 확장 논리에 대한 비교는 아래 표 1과 같이 정리할 수 있다.

표 1. 기존 논리의 비교

속 성	BAN90	GNY90	AT91	VO93	SVO96
형식적 의미 유무	O Operational semantics	X	O	X	O Model theoretic semantics
프로토콜 이상화 유무	O	O	O	O	O
키 신뢰에 대한 가정 제거	X	X	O	X	O
계체에 대한 신뢰 가정 제거	X Nonce verification rule	X Jurisdiction rule	O	X Nonce-verification rule	O
추론의 범위	인증 프로토콜	인증 프로토콜	인증 프로토콜	인증/키 교환 프로토콜	인증/키 교환 프로토콜
메시지 소유 유무 (possession)	X	O Possession rule	X	X	O Seeing axiom 8
메시지 인식의 유무 (recognition)	X	O Recognition rule	X	X	O Comprehending axiom 11,12
메시지 무결성 검증 유무	X	X	X	X	△ Axiom12

GNY 논리[7]는 많은 초기 가정들을 제거하고 메시지

의 소유와 믿음을 분리하였으며, AT 논리[8]는 강한 형식적 의미를 제공하였다. 그리고 VO 논리[9]는 단순히 BAN과 GNY 논리에 키 합의 프로토콜을 검증할 수 있는 논리로 확장 하였고, 가장 최근의 SVO 논리[10]는 기존 논리들의 장점만을 통합하였다.

프로토콜 검증을 위한 논리에서 메시지 의미를 추론하는 규칙[2,7,8,9]은 메시지 인증(message authentication)을 위한 추론으로 해석될 수 있다. 그러나 메시지 인증은 메시지 무결성과 메시지 근원지(message source)의 의미를 동시에 포함 하고 있으므로 메시지 의미 규칙을 메시지 인증의 의미로 보기 어렵다. 아래 BAN 논리의 메시지 의미 규칙(M-1)에서 A의 믿음에 대한 메시지 의미는 메시지 X의 근원지만을 추론 하는 의미로 정확히 해석 되어야 한다. 그리고 메시지 인증을 위해서 메시지 무결성에 대한 새로운 추론 규칙이 요구된다.

$$\text{M-1.}\quad \frac{A \text{ believe } A \overset{K}{\Longleftrightarrow} B,\ A \text{ sees } \{X\}_k}{A \text{ believe } B \mid\sim X}$$

SVO 논리의 Axiom-12[10]은 논리 범위에서 메시지의 무결성을 검증할 수 있는 가능성을 제공한다.

SVO의 Axiom 12.

(P received F(X) ∧ P believes P sees X) ⊃
P believes P received F(X)

실제로 메시지 인증에서 데이터 무결성(data integrity)은 메시지 인증 코드(MAC)나 서명(Sig)을 통해 이루어진다. 그러나 Axiom 12의 F(X)를 메시지 X를 입력으로 받는 결정적 함수(MAC(K,M) 또는 $Sig(K^{-1},M)$)로 가정하고, VO 논리에서 키 확신을 나타내는 Confirm(K)과 GNY 논리의 인식(recognition)을 재공식화(reformulate)한다면, 비트 수준의 데이터 무결성 검증이 아닌 좀더 추상적인 수준에서 메시지 무결성이 검증될 수 있다.

3. 개선된 논리의 제안

이 절에서는 암호학적 프로토콜의 보안 요구사항 중 메시지 무결성을 검증할 수 있는 논리를 제안한다. 아래 그림 1은 기존 논리를 통합 개선하기 위한 논리들의 구성을 나타낸다.

<table>
<tr><td rowspan="2">로직의 의미 설명
(model theoretic semantics)</td><td>논리의 확장
(키 합의 프로토콜 추론)</td><td>논리의 개선
(메시지 무결성 추론)</td></tr>
<tr><td colspan="2">GNY논리의 구문 기반
(구문의 단순화)</td></tr>
<tr><td colspan="3">SVO 논리 기반의 계산 모델(computational model)</td></tr>
</table>

그림 1 제안하는 논리의 구성

제안되는 검증 논리는 GNY 논리의 구문과 추론 규칙, SVO 논리의 모델 이론적 의미론(model theoretic semantics)에 기반하며 키 합의 프로토콜의 검증을 위해 VO 논리를 수용한다.

3.1 구문

아래 표 2는 GNY 논리에 사용된 공식을 보안 요구사항 검증을 위해 필요한 부분만을 재작성한 것이다. P와 Q는 암호학적 프로토콜의 참여개체이며 X는 메시지 또는 공식이다. 함수 F(X,K) 는 단방향 일대일 대응 함수이며 암호화($E_K(X)$) 함수와 같은 가역 함수가 존재하는 함수 F(X)는 인자를 생략하여 구분한다.

표 2. 수정된 공식

새로운 표기	GNY 표기	관련 추론 규칙	설 명
P received X	P ◁ X	Receiving rule	P가 X를 받고 조작 가능
P has X	P ∋ X	Possession rule	P가 받았거나 처리,또는 생성한 X를 소유
P believes P has X	$P \mid\equiv \sharp(X)$	Recognition rule	P가 소유한 메시지 X를 인식
P |~ X	P |~ X	Once told rule	P가 X를 말함. 단 무결성은 보장 안함
P ||~ X	없음	Message interpretation rule	P가 X를 말하고 무결함
$\overline{K}$	없음	Message interpretation rule	암호화 키에 대응하는 키
F(X,K)	H(X)/F(X)	Message interpretation rule	단 방향 일대일 함수
PKψ(P,K)/ PKσ(P,K)/ PKδ(P,K)	$P \overset{k+}{\Longleftrightarrow} Q$/ $P \overset{k-}{\Longleftrightarrow} Q$	Key agreement rule	암호화키/ 서명키/ 키 합의 공개키

표 2의 GNY 논리에서 인식을 위한 표기법 $P \mid\equiv \sharp(X)$은 [7] 소유(has)와 믿음(believe)으로 나타내어 단순화 하였다. 그리고 $\overline{K}$는 대칭키 일 경우 $K \equiv \overline{K}$ 이며, 키 합의 프로토콜의 검증을 위해 VO 논리와 같이 공개키 쌍을 암호화와 서명 그리고 키 합의 공개키로 분리하였다.

VO 논리에 제시된 Confirm(K)는 키 합의 프로토콜에서 키 확신(key confirmation)에 사용되지만 키뿐만 아니라 다음과 같이 메시지 X에 대한 확신을 나타내는 의미로 확장할 수 있다.

Confirm(X) ≡ ((P received F(X,K) ∧
P believes P has F(X,K) ∧ #(X))

만약 참여 개체 P가 F(X,K)를 받았다면 P는 X를 소유하게 되고, 소유한 F(X,K)가 인식할 수 있는 메시지이고 메시지 X가 최근 것(freshness) 이라면 P는 메시지 X를 확신 할 수 있다. 이것은 VO 논리에서 명시적 키 인증을 위한 키 확신과 유사하다.

3.2 개선된 추론 규칙

우리는 GNY 논리에 사용된 추론 규칙을 새롭게 구성한다. GNY 논리에서 명시적으로 표현 된 인식에 대한 믿음($P \mid\equiv \sharp(X)$)[7]을 "P believes P has X"로 표기함으로서 인식 자체에 대한 표기를 제거하면 다음과 같다.

MR-1. $\frac{P\ has\ X \wedge Confirm(X)}{P\ believes\ P\ has\ X}$

MR-2. $\frac{P\ |\sim\ X}{P\ believes P\ has\ X}$

MR-1에서 개체 P는 메시지 X를 소유하고 확신하면 인식할 수 있다. 이것은 메시지 X의 소유와 F(X, K)의 인식을 통한 메시지 X의 확장된 인식이다. 그리고 P는 자신이 말한 X를 인식할 수 있다.

GNY 논리의 메시지 해석 규칙(I1)[7]에서 나타난 인식을 제거하여 "P believes Q|~X"로 구성하고(I-1), I3과 I4를 무결성이 고려된 무결성 해석 규칙(I-M)으로 아래와 같이 재구성 할 수 있다.

I-1.

$$\frac{P\ received\ \{X\}_K \wedge P\ has\ K \wedge P\ believes\ P \overset{K}{\leftrightarrows} Q \wedge P\ believes\ \#(X,K)}{P\ believes\ Q\ |\sim\ X, P\ believes\ Q\ |\sim\ \{X\}_K}$$

I-M.

$$\frac{P\ received\ F(X,K) \wedge P\ has\ \overline{K} \wedge P\ believes\ P \overset{K}{\leftrightarrows} Q \wedge P\ belieeves\ P\ has\ X}{P\ believes\ Q\ \ ||\sim X}$$

3.3 제안된 논리의 건전성

본 논문에서 제안한 추론 규칙에 사용된 확신과 인식 그리고 무결성에 대한 참인 상태(true condition)는 SVO 논리의 계산모델과 모델 이론적 의미론[10]으로 다음과 같이 설명할 수 있다. 프로토콜의 모든 실행(r)과 시간(t)에 대한 공식(φ)의 참인 상태를 (r, t) ⊨ φ라 표현한다. 그리고 각 참여 개체 P는 (r, t)에서 받은 메시지의 집합(received message)과 소유한 메시지(seen message)의 집합을 가진다.

메시지 확신

(r, t) ⊨ P confirm(X) iff 모든 실행 (r, t)에서 P는 다음 조건을 만족한다.

(r, t) ⊨ P received F(X, K)

(r, t) ⊨ P believes P has F(X, K)

(r, t) ⊨ #(X)

메시지 인식

(r, t) ⊨ P believes P has X iff 모든 실행 (r, t)에서 P는 다음 조건을 만족한다.

(r, t) ⊨ P has X

(r, t) ⊨ P confirm(X)

무결성과 메시지 기원 인증

(r, t) ⊨ P ||~ X iff 모든 실행 (r, t)에서 P는 다음 조건을 만족한다.

(r, t) ⊨ P believes P has X

(r, t) ⊨ P has $\overline{K}$

(r, t) ⊨ P believes $P \overset{K}{\leftrightarrows} Q$

4. 결론 및 향후 연구과제

본 논문에서는 기존의 논리의 비교 분석을 통해 메시지 의미 규칙의 모호한 의미를 단지 메시지 근원지의 의미로 제한하였다. 그리고 GNY와 VO 논리 기반으로 추상적 암호학적 메시지 수준에서 무결성을 검증하는 추론 규칙을 제안하여 암호학적 프로토콜의 무결성을 논리적으로 설명할 수 있었다.

향후 제안된 논리로 다양한 프로토콜을 검증하여 좀 더 안전한 프로토콜의 설계를 위한 작업과 부인봉쇄와 같은 더 많은 보안 속성을 검증할 수 있는 논리의 개선 작업이 요구된다.

참고 문헌

[1] T.Y. Woo and S. S. Lam. "A semantic model for authentication protocols," In Proceedings of the 1993 IEEE Symposium on Research in Security a nd Privacy, pages 178-194, 1993.

[2] M. Burrows, M. Abadi, and R. Needham. "A logic of authentication". EDC Systems Research Center, Report 39, revised February 22 1990.

[3] Paul Syverson and Iliano Cervesato. "The logic of authentication protocols," In R. Focardi and R. Gor rieri, editors, Foundations of Security Analysis and Design, volume LNCS 2171. Springer-Verlag, 2001.

[4] L. C. Paulson. "The inductive approach to verifying cryptographic protocols", Journal of Computer Security, 6(1-2):85-128, 1998.

[5] C. Meadows. "Open issues in formal methods for cryptographic protocol analysis", In Proceedings of DISCEX 2000, IEEE Computer Society Press, Janu ary 2000.

[6] C. Boyd and W. Mao, "Limitations of logical analysis of cryptographic protocols." In Accepted by EuroCrypto, to appear, 1993.

[7] L. Gong, R. Needham, and R. Yahalom. "Reasoning about belief in cryptographic protocols.", In Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy, pages 234-248, 1990.

[8] M. Abadi and M. Tuttle, "A semantic for a logic o f authentication," proc. of the ACM Symp. of Principle of Distributed computing, pp. 201-216, 1991.

[9] P. van Oorschot, "Extending cryptographic logics of belief to key agreement protocols ", 1st ACM Conference on Computer and Communications Security, ACM Press, 1993, 232-243.

[10] P. F. Syverson and P. C. van Oorschot. "A Unified Cryptographic Protocol Logic", draft available from authors, 1996.