UPPAAL을 이용한 전자지불 프로토콜 분석[1)]

문영주0*, 방기석**, 김일곤*, 강인혜***, 최진영*

*고려대학교 컴퓨터학과
{yjmoon0, igkim, choi}@formal.korea.ac.kr,

**한림대학교 정보통신공학부
kbang@formal.korea.ac.kr

***서울시립대학교 기계정보공학과
inhye@uos.ac.kr

Analysis of E-Commerce Protocols Using UPPAAL

Young-Joo Moon0*, Il-Gon Kim*, Jin-Young Choi*
*Dept of Computer Science & Engineering, Korea University

Ki-Seok Bang**
**Division of Information Engineering and Telecommunication
Hallym University

Inhye Kang***
***Dept of Mechanical and Information Engineering, University of Seoul

요약

전자지불 시스템의 활용성 증대와 더불어 상거래의 안전성을 보장하는 문제가 중요한 핵심 사항으로 간주되고 있다. 본 논문에서는 이러한 전자지불 시스템의 암호화 키는 안전하다는 가정 하에 전자지불 프로토콜을 통해 소비자와 상인, 은행간의 상거래의 정확성을 중점으로 NetBill 프로토콜을 명세, 검증했다. 프로토콜의 명세를 위해서는 실시간 개념이 포함되어 있는 UPPAAL을 사용했다.

1. 서론

최근 컴퓨터 기술과 정보통신 기술의 발전에 따른 인터넷의 급속한 발전은 전자상거래의 고도 성장이라는 결과를 유도했다. 올 2005년 통계청의 연구 결과에 따르면 전자상거래의 총 규모는 300조원을 넘어섰고, 전년에 비하여 약 79조원이 증가한 수준이며, 그 중 인터넷을 이용한 전자상거래는 97%가량을 차지하고 있다[1].

이에 따라, 전자지불 시스템의 활용성 증대와 더불어 시스템의 안전성을 보장하는 문제가 핵심 사항으로 간주되고 있다. 현재까지 전자지불 시스템의 안정성에 대한 연구는 각 모듈에서 주고 받는 키 값의 보안 여부에 중심을 두고 이루어졌다. Jan Jürjens는 UML을 이용하여 CEPS 전자지갑 시스템의 기능에 대해 명세하고, 암호화 키 노출에 의한 보안 취약점에 대해 연구하였고[2], Susan Stepney는 Z 정형명세 언어를 이용하여 전자지갑의 기능을 증명했다[3].

본 논문에서는 이러한 전자지불 시스템의 프로토콜의 암호화 키는 안전하다는 가정 하에 전자지불 프로토콜을 소비자와 거래 상인간의 상거래 정확성을 중점으로 NetBill 프로토콜을 검증하고자 한다. 즉, 프로토콜 구성 모듈들이 안전한 통신을 통해 상거래의 기본 요구사항이 올바르게 보장되는지 검증하고자 한다. 프로토콜 의 명세를 위해서 실시간 개념이 포함되어 있는 Timed automata[4]기반의 모델 체커인 UPPAAL[5] 을 사용하였다.

본 논문의 구성은 다음과 같다. 2장에서는 전자지불 프로토콜의 일종인 NetBill과 정형검증도구 UPPAAL에 대해 간략 하게 소개하고 3장에서는 NetBill 프로토콜의 모델링 및 정확성 검증에 대해 설명하고자 한

1) 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성지원사업의 연구결과로 수행되었음

다. 4장에서는 본 논문에 대한 결론을 언급하고, 향후 연구방향을 제시하고자 한다.

2 관련연구

2.1 전자지불 프로토콜

NetBill 프로토콜은 인터넷을 통한 전자상거래를 위해 디자인되었다[6]. 그림 1과 같이 소비자, 상인, 은행의 3부분으로 이루어져있다. 소비자가 상인에게 물품을 요구하는 메시지(Goods Request)를 보내면, 상인은 암호화된 물품 메시지(Encrypted Goods)를 보내고 물품에 해당하는 가치 메시지(Electronic Payment Order)를 받는다. 상인이 받은 가치 메시지를 은행으로 보내면(Endorsed Electronic Payment Order), 은행은 처리 결과(Transaction Result)를 상인에게, 상인은 소비자에게 보낸다. 은행의 처리결과가 정상적으로 완료된 경우, 상인은 암호화된 물품에 대한 키 값을 소비자에게 보낸다. 은행에서 올바르게 처리되지 않거나, 시스템의 시간 만료를 넘어선 경우, 그림 1의 아래 두 단계에서 표현된 것처럼 소비자는 처리 결과에 대한 확인을 위해 은행에서 직접적으로 처리 결과를 알아볼 수 있다.

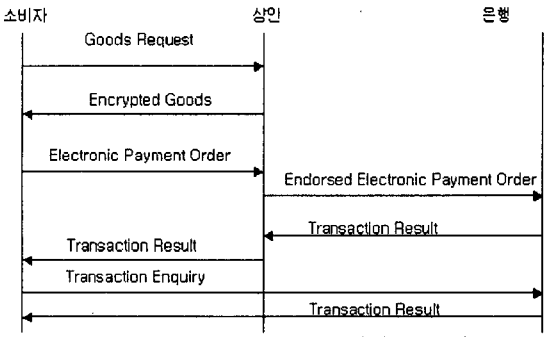

그림 1. NetBill 프로토콜 메시지 순서도

2.2 UPPAAL

UPPAAL은 실시간 시스템의 검증을 위해 개발된 도구로 Timed automata를 기반으로 한다. UPPAAL은 기술 언어, 시뮬레이터, 모델 체커로 구성되어 있으며, 이들은 각각 시스템 에디터, 시뮬레이터, 검증기능을 제공한다. 기술 언어는 각 프로세스를 Timed automata로 표현한 것으로, 시스템 편집기를 이용해서 도식적으로 시스템을 명세하고, 시뮬레이터는 기술 언어로 표현된 시스템의 동적인 실행을 시뮬레이션 해서 시스템의 동작을 확인할 수 있게 해 주며, 모델 체커는 명세된 시스템의 상태 공간을 탐색해서 시스템이 만족해야 할 속성을 만족하는지 검증한다.

UPPAAL에서 시스템은 프로세스의 집합으로 이루어져있으며, 각각의 프로세스는 하나의 Timed automata로 표현되고 채널로 연결된다. 각 채널은 송신 이벤트와 수신 이벤트로 구성되어 있고, 하나의 채널로 연결된 두 개의 프로세스는 송신 이벤트와 수신 이벤트에 의해 동기화가 이루어진다. 각 프로세스는 노드들로 구성되어 있고, 시스템의 동작은 노드들의 전이로 표현된다. 노드의 전이는 동기화 이벤트 외에 한정자(guard)에 의해 영향을 받는다. 한정자는 각 프로세스의 시간 변수에 대해 자연이나 시간 만료와 같은 시간 제약 사항을 표현하는 것으로, 제안된 모델은 시간 제약 사항에 따른 모델 검증이 가능하다.

3. 전자지불 프로토콜의 명세

3.1 전자지불 프로토콜 모델링

프로토콜에 참여하는 소비자와 상인, 은행을 각각 프로세스로, 각 프로세스가 주고 받는 메시지를 송수신 이벤트로 만들어서, 시스템 에디터에서 도식적으로 Timed automata 형식으로 표현함으로써 프로토콜을 명세했다. 그림 2는 명세한 프로세스 중 하나인 소비자의 프로세스이다. 그림 1의 메시지 순서도와 비교해서 보면, 소비자가 상인에게 보내는 상품 요청 메시지는 그림 2에서 송신 이벤트로, 상인이 소비자에게 보내는 암호화된 물품 메시지는 수신 이벤트로 표현했다. 또한 소비자 프로토콜의 시간 만료를 표현하기 위해 로컬 클럭을 정의해서 한정자에서 사용하도록 했다.

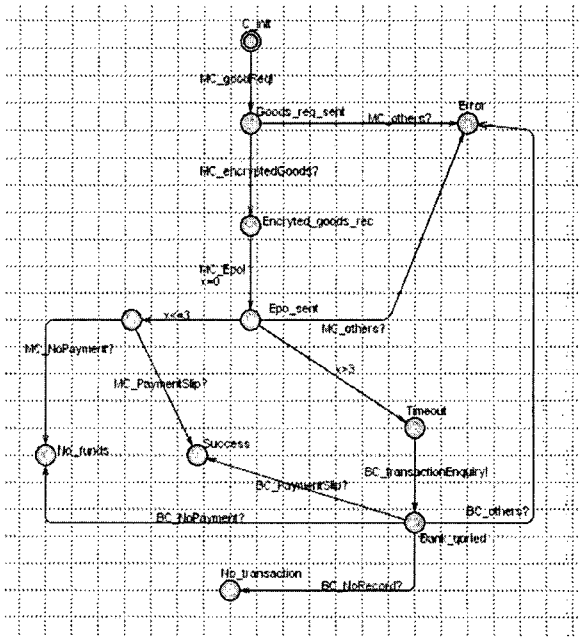

그림 2. 소비자 프로세스 명세

3.2 전자지불 프로토콜 검증

전자지불 프로토콜 행위의 정확성을 표현하는 검증 속성을 UPPAAL에서 사용하는 시제 논리인 CTL을 이용해서 표현하면 다음과 같다.

표 1. CTL로 표현한 검증 속성

E<> merchant1.Get_payment and merchant1.Get_payment imply consumer1.Success
E<> consumer1.Success and Consumer1.Success imply merchant1.Get_payment

즉, 소비자가 원하는 물품에 대해 가치를 상인에게 지불하면(merchant1.Get_payment), 해당 물품을 얻게 되고(consumer1.Success), 상인이 소비자에게 물품을 판매하면(consumer1.Success), 그에 해당하는 가치를 얻게 된다(merchant1.Get_payment)는 것이다. 위의 CTL 식을 UPPAAL의 검증기에서 검증한 결과는 다음 그림 3과 같다. 즉, 명세된 NetBill 프로토콜은 안전한 채널이 보장된 상태에서 소비자와 상인, 은행간의 상호 동작이 정확하게 발생하고 상품 구매 및 대금 지불이 정확하게 이루어짐을 알 수 있다.

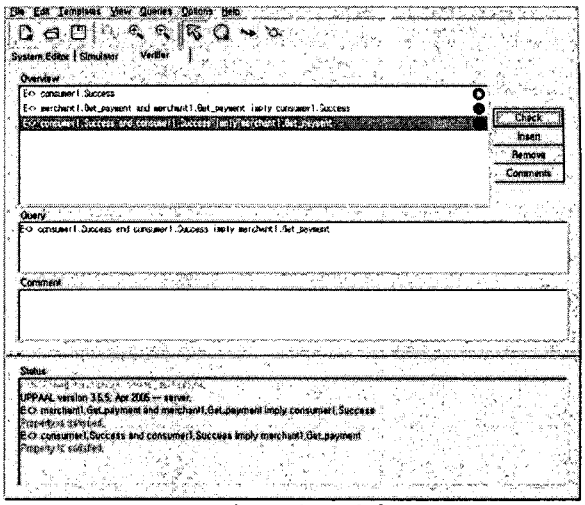

그림 3. 검증 결과

4. 결론 및 향후 연구방향

본 논문에서는 전자상거래에서 사용하는 전자지불 프로토콜의 암호화 키가 안전하다는 가정 하에 프로토콜의 참여 모듈간의 상거래 행위를 중점으로 NetBill 프로토콜을 명세하였다. 전자상거래의 실제 상황에서 일어날 수 있는 시간 만료에 의한 예외 상황을 표현하기 위해 전자지불 프로토콜의 명세는 시간 제한 사항을 표현할 수 있는 Timed automata를 기반으로 하고 있는 UPPAAL을 사용하였다.

전자지불 프로토콜의 암호화 알고리즘이 안전하다는 가정 하에, 프로토콜이 정확하게 동작했다면 소비자는 지불한 가치에 해당하는 물품을, 상인은 판매한 물품에 해당하는 가치를 얻어야 한다. UPPAAL을 사용하여 검증한 결과, NetBill 프로토콜이 상거래의 기본 요구사항을 만족시켜 준다는 사실을 확인하였다.

향후에는 CEPS 전자지갑 표준을 기반으로 한 전자상거래 시스템의 전자화폐 구입 및 충전 기능의 안전성을 검증할 예정이다.

5. 참고문헌

[1] 통계정 서비스업통계과, "2004년 4/4분기 연간 전자상거래 통계조사 결과", http://www.nso.go.kr/newnso/n otice/report_view.html.

[2] J. Jörjens and G. Wimmel, "Security Modelling for Electronic Commerce: The Common Electronic Purse Specificatio," I3E 2001, pp. 489-506, 2001.

[3] S. Stepney, D. Cooper, and J. Woodcock, "An Electronic Purse : Specification, Refinement, and Proof", Technical Report PRG-126, 2000.

[4] R. Alur and D. Dill, "A Theory of Timed Automata", Theoretical Computer Science 126, pp.183-235, 1994.

[5] J. Bengtsson, Kim G. Larsen, F. Larsson, P. Pettersson, and Wang Yi, "UPPAAL in 1995", TACAS 96, pp.431-434, 1996.

[6] B. Cox, D. Tygar, M. Sirbu, "NetBill Security and Transaction Protocol", Proceedings of the First USENIX Workshop in Electronic Commerce, pp.77-88, 1995.