스마트 카드의 보안성에 대한 정형검증 방법 연구

강은영, 최진영
고려대학교 컴퓨터학과
{eykang,choi}@formal.korea.ac.kr

A Study on Formal Verification of Smart Card Security

Eun Young Kang, Jin Young Choi
Dept. of Computer Science & Engineering, Korea University

요 약

인터넷의 급속한 발달과 이를 통한 다양한 서비스가 확산됨에 따라, 인증과 보안은 아주 중요한 분야로 대두되고 있다. 본 논문에서는 Esterel 을 이용하여 최근 정보화 사회에서 개인적 정보 뿐만 아니라 비즈니스 간의 데이터 응용 분야에 이르기까지 폭 넓게 사용되어지고 있는 스마트 카드의 인증과 보안 시스템 대한 모델링 및 정형검증에 대해 논한다.

1. 서 론

인터넷의 급속한 발달과 이를 통한 다양한 서비스가 확산됨에 따라, 인증과 보안은 아주 중요한 분야로 대두되고 있다. 최근 정보화 사회에서 스마트 카드는 개인적인 정보 뿐만 아니라 비즈니스 간의 데이터 응용 분야에 이르기까지 폭 넓게 사용되고 있다. 이에 따른 인증과 보안은 스마트 카드의 시스템의 안정성 및 효율을 크게 좌우한다. 현재 다양한 보안 방법의 메커니즘이 제안되고 있으나 그에 대한 설계 및 이해가 복잡해지고 있는 실정이다. 따라서 다양한 인증 및 보안 메커니즘에 대한 정확성 검증이 매우 중요하다. 그러나 전통적인 테스팅 기법만으로는 시스템에서 발생할 수 있는 예기치 못한 오류들을 정확하게 검출해 낼 수 없다. 이에 본 논문에서는 정형기법[1]을 이용하여 스마트 카드의 보안 인증 부분을 분석, 결정적 reactive 시스템을 프로그래밍하는 동기적(synchronous)언어인 Esterel[2]로 명세함으로써 Esterel 이 갖는 효율성을 증대 시킴은 물론, 테스팅이 갖는 한계점을 극복하기 위해, 모델 체킹 기법을 사용하여 명세된 시스템을 검증함으로써 실제 스마트 카드[3]가 반드시 만족 시켜야 하는 안정성과 신뢰성을 높이고자 한다. 본 논문은 다음과 같이 구성된다. 2 절에서는 정형기법과 Esterel 에 대해 간략히 소개하고, 3 절 부터는 스마트 카드 메커니즘을 설명한 후 이를 모델링하여 검증한다.

2. 정형기법과 Esterel

정형기법[1]은 수학과 논리학에 기반을 둔 방법으로 하드웨어나 소프트웨어 시스템을 명세하고 검증하는 것을 의미한다. 수학적 기호를 사용하여 시스템을 명세하고 검증 또한 논리를 바탕으로 한 수학적 성질을 이용하여 검증함으로 자연어가 내포하는 애매모호함이나 불확실성을 최소화한다. 따라서 설계된 시스템이 처음에 의도한 요구사항과 동일한지를 수학적으로 증명하여, 최소한의 검증된 특성에 대해서는 믿을 수 있고 사용가능하다. 정형 기법은 정형 명세와 정형 검증으로 나뉘는데, 정형 명세는 시스템이 만족해야 할 요구사항과 그러한 요구사항을 만족할 수 있는 설계를 기술하는 것을 말한다. 정형 검증은 명세가 정확한지, 즉 설계가 요구사항을 만족하는지를 검사하는 것이다.

Esterel[2]은 1980 년대 Sophia-Antipols 내에서 정의 되어지고, 현재 프랑스의 INRIA 연구소에서 계속적으로 연구되어 다양한 정형기법 도구를 개발하고 있다. Esterel 은 Reactive 시스템의 동기적 프로세스 시스템(synchronous process system)의 설계와 검증(verify)을 지원하는 tool 로 특별한 구문 - 지연, 선점, 자동화된 시간 유닛(unit)에 따라 특정 시그널의 반복 등 - 을 직관적인 키워드로 사용한다.[4,5] Esterel 은 또한 실시간 시스템(real time system)과 텔레 통신 프로토콜 서비스(telecommunication service protocol)검증에 유용하게 사용된다. Esterel 의 검증 모델은 프로세스 상호작용(process interactions)의 정확성(correctness)에 초점을 둔다. 이 도구를 이용해서 명세(specification)의 일관성(consistency)을 검사할 수 있는데, 데드락 (Deadlock)이나 명세되어 지지 않은 반응(unspecified receptions)등을 보여준다.

이러한 도구 가운데는 Esterel 언어를 각종 언어로 바꾸어 주고 언어의 문법적 오류와 의미적 오류를 찾아내어 수정하게 하는 컴파일러인 Esterel toolset 이 있으며 이에 대한 시뮬레이션 도구로 XES[6]가 있다. 또한 이를 정형 검증하는 도구인 XEVE[7]가 있다. 뿐만 아니라, 바이시뮬레이션(bisimulation)으로 시스템을 검증하게 하는 fc2symbmin 이 있으며 또한 이를 모델 체킹으로 검증하게 하는 VIS[8]라는 도구 역시 이를 검증하고 시뮬레이팅 도구로 알려져 있다. Esterel 은 이러한 다양한 검증 능력과 그 형태의 변형으로 인해 시스템 설계를 하고 명세화 하여 그 정확성을 검증하거나 시뮬레이팅 할 수 있다.

3. Smart Card

본 논문에서의 제안 모델은 단기능 메모리 스마트 카드[3]의 보안적인 면을 강화시킨 것으로써, 프로세서는 내장하고 있지 않고, 메모리 만을 내장하고 있는 카드 형태로, 단일 기능 어플리케이션 만을 위해 사용된다. 데이터의 억세스 관리는 칩 내의 보안 모듈에 의해 관리 되어 지는데, 이는 데이터의 임의의 변경을 방지하고, 접근이 허가 되지 않은 접근은 블록 시킨다.

구체적인 기능으로는 카드와 그 카드를 사용하려는 목적 운영 모드 간의 능동적인 데이터 전송을 하기 이전에 다음과 같은 작업을 수행한다.

카드 메모리 내에 자신만의 비밀코드를 입력하고, 그 카드를 사용할 때 마다 비밀 코드를 재 입력하는 방식으로, 카드의 사용자가 과연 올바른 사용자인가를 체크 한다. 즉, 이미 카드 안에 저장되어진 비밀코드와 사용자의 입력 비밀 코드가 서로 같을 때, 카드의 사용이 허가된다. 모델에 있어서의 입력 시그널과 출력 시그널은 다음과 같다.

Pure input signals

- **PIN** 사용자의 truePIN 을 입력으로 받는다.
- **REPIN** 입력이 falsePIN 일 경우, PIN 을 재입력으로 받는다.
- **REPINWRIGHT** trueREPIN 을 입력으로 받는다.
- **REPINWRONG** falseREPIN 을 입력으로 받는다.
- **WPIN** falsePIN 을 입력으로 받는다
- **CANCEL** 사용 동작을 취소한다.

In relation to output signals

- **RIGHT** 입력 PIN 이 truePIN 을 알린다.
- **FRIGHT** 입력 falsePIN 일 경우, 재 입력한 PIN 이 truePIN 임을 알린다
- **WRONG** 입력이 falsePIN 임을 알린다.
- **GETOUT** 3 번 이상의 falsePIN 입력이 이루어 졌음을 알린다.
- **BEEP** 정확한 fairness 조건의 만족을 알린다.
- **Keepcard** 현재 카드의 프로세싱을 알린다

4. Esterel 을 이용한 모델링

아래의 그림은 Esterel 로 설계된 스마트 카드에 대한 명세와 이를 Esterel 검증 도구인 XES[6]를 이용하여 시스템의 validation 을 시행하여 유한 상태 기계로 표현한 것으로 사용자의 인증 허가 여부를 결정하는 모델이다.

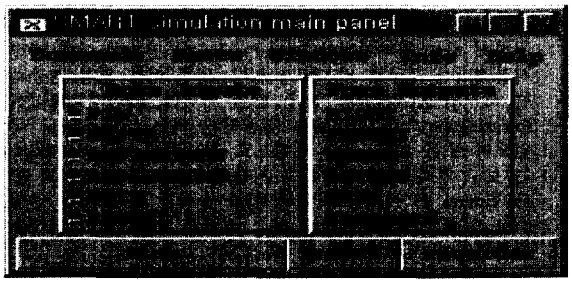

그림 1. 스마트 카드의 검증 모델

기본적으로 각 모듈은 프로세스로 구현되며 모듈간의 연결은 Esterel 의 동기적 가설(synchronous hypothesis)을 기반으로 하여 평행(parallel)하게 구현된다. 모듈들은 시그널을 통하여 각각의 모듈끼리 혹은 외부 세계와 통신을 하며, 그러한 시그널은 전체 모듈에게 broadcasting 된다. 이러한 동기적 가설을 충족시키도록 시그널의 출력과 입력은 시간적 소모가 없는 것으로 간주 된다.

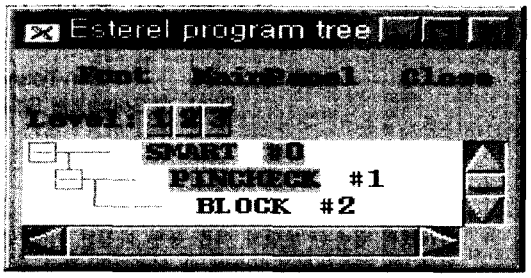

그림 2. 메인 패널에 따른 서브 모듈

SMART 모듈은 <그림_2>와 같이 1 개의 메인 모듈과 2 개의 서브 모듈들로 구성된다. 메인 모듈 SMART 에서는 PIN 입력을 받을 때 까지 아무런 일도 수행하지 않는다. 즉 PIN 버튼을 눌러야만 작동이 가능하다. 이는 다시 잘못된 PIN 이나 CANCEL 입력이 들어 오기 전까지 Keepcard 인 상태로 계속하여 작동한다. 잘못된 PIN 이 들어오면 WRONG 시그널을 발생하고 PIN 을 다시 검사 하기 위한 PINCHECK 서브 모듈을 실행한다. PINCHECK 모듈은 3 번(3 times)의 재 PIN 입력을 허가 하며, 재 입력한 PIN 이 인증된 PIN 일 경우 메인 모듈을 다시 정상적으로 수행하고 그렇지 않을 경우, 카드 사용 금지 모듈인 BLOCK 서브 모듈을 실행한다. BLOCK 서브 모듈은 재입력한 PIN 이 3 번 이상 거짓일 경우 GETOUT 이라는 시그널을 발생하고 작동을 중지한다. 이에 대한 자세한 검증은 다음 절에서 다루겠다. 구체적인 Esterel 코드는 지면 관계상 생략한다.

5. Esterel 을 이용한 검증

본 논문에서는 XES[5]를 이용하여, 시스템의 validation 을 시행한 스마트 카드[3]가 만족해야 할 *safe properties* 를 XEVE[7]를 통하여 검증하여 오류가 없음을 확인 한다. 이번 절에서는 오류의 검증 단계로 모델이 만족해야 하는 safety properties 를 tl2strl[6]이라는 검증 툴을 이용하여 다음과 같이 줄 수 있다.

```
SA1 := { WPIN -> WRONG}
SA2 := { RIGHT -> (Not (WPIN | CANCEL) )
SA3 := { (Not ( WPIN | CANCEL ) ) -> BEEP }
RespondsTo {RIGHT} In 1 PIN
```

SA1 은 만약 거짓 PIN 이 발생하면, WRONG 시그널을 발

생한다는 것이고, SA2 는 정확한 메커니즘이 일어 났을 때는 WPIN 이나 CANCEL 은 반드시 발생하지 않는다는 조건을 둔 것이며, 마지막 SA3 는 한번만의 정확한 PIN 입력이 일어났을 경우에는 WPIN 은 결코 발생하지 않고 CANCEL 또한 입력 값으로 받아 들이지 않으며, 정확한 fairness 의 알림 표시로 BEEP 를 시그널로 띄우는 조건을 두었다. 아래의 <그림_3>에서 나타난 바와 같이 Esterel 의 XEVE 로 검증한 결과 위의 요구사항을 만족시킴을 알 수 있다.

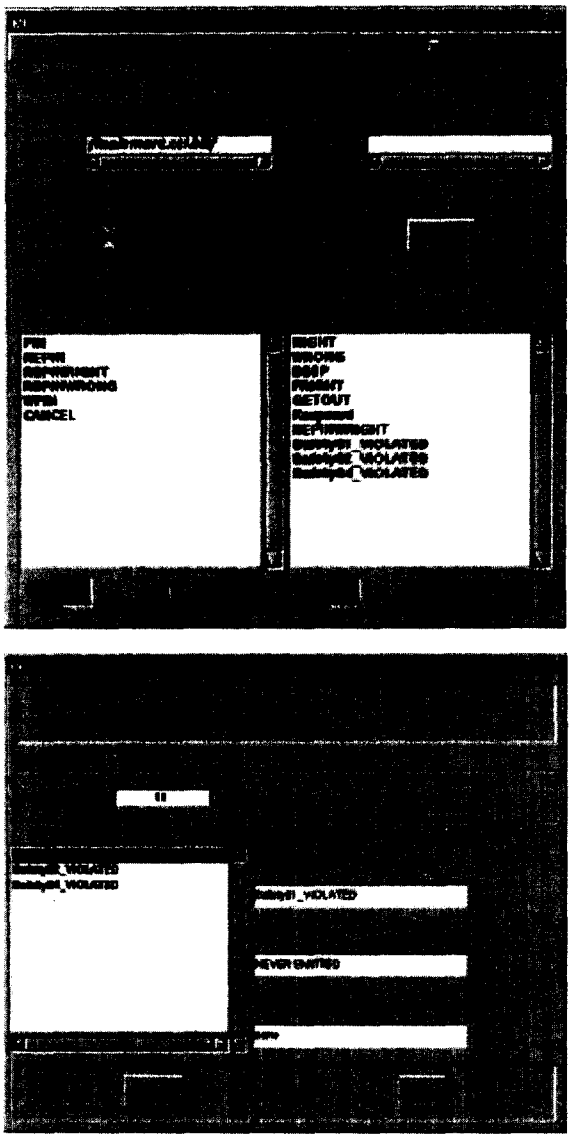

그림 3. XEVE 를 이용한 검증 결과

6. 결론

인증과 보안은 스마트 카드의 시스템의 안정성 및 효율을 크게 좌우한다. 현재 다양한 보안 방법의 메커니즘이 제안되고 있으나 그에 대한 설계 및 이해가 복잡해지고 있는 실정이다. 따라서 다양한 인증 및 보안 메커니즘에 대한 정확성 검증이 매우 중요하다.

본 논문에서는 정형기법 도구인 Esterel 을 이용하여 스마트 카드의 보안 모듈을 명세하고, 이를 다시 XES 를 이용하여 모델링 하였으며, 최종적으로 XEVE 를 이용하여 스마트 카드 내 보안 사항의 인증 모듈이 반드시 갖추어야 할 필수 사항들을 정형 검증하여 시스템의 안전성과 신뢰성을 도모 하였다.

7. 참고문헌

[1] Edmund M. Clarke and Jeannette M. Wing, "formal Method : State of the Art and Future Direction", ACM Computing Surveys, pp.626-643

[2] G. Berry and G. Gonthier. The ESTEREL synchronous programming language: design, semantics, implementation. Science of Computer Programming, 19:87-152, 1992.

[3] 기술정보센터 정보조사분석팀, "스마트 카드 기술 시장 보고서", p65-79, 한국전자통신연구원, 1999

[4] David L. Dill, John Rushby, Acceptance of Formal Methods : Lessons from Hardware Design, IEEE Computer, April 1996, Vol. 29, No. 4, pp.16-30.

[5] S. T. Cheung. "Compiling Verilog into automata" Tech. Rep. UCB/ERLM94/37, May 1994

[6] G.Berry and The Esterel Team. The Esterel v5_21 System Manual. INRIA. France. March. 11. 1999

[7] Amar Bouali. XEVE: An Esterel Verification Environment(V1_3). INRIA. France. 1997

[8] Rovert K. Braton, Crry D. Hachtel et al, "VIS: A System for Verification and Synthesis", in the Proceedings of the Conference on Computer Aided Verification, New Brunswich, MJ, July, 1996