고등급 보안 시스템 개발을 위한 정형기법[1)]

유희준[1U] 김영미[1] 최진영[1] 서동수[2] 노병규[3]
고려대학교 컴퓨터학과 정형기법연구실[1]
성신여자대학교 전산학과[2]
한국정보보호센터[3]
{hyoo, ymkim, choi}@formal.korea.ac.kr
dseo@cs.sungshin.ac.kr
namy@kisa.or.kr

Formal Methods for Developing High-Grade Secure System

Hee-Jun Yoo[1U] Young-Mi Kim[1] Jin-Young Choi[1] Dong-Soo Seo[2] Byung-Gyu No[3]
Formal Methods Lab. Dept. of CSE, Korea University[1]
Dept. of Conputer Science, SungShin Women's Univ.[2]
Korea Information Security Agency[3]

요 약

현대 사회는 인터넷 기술의 비약적인 발전으로 인하여 실생활에서 이루어지던 거의 모든 작업들이 인터넷상에서 이루어지는 전자사회(E-society)가 형성되고있다. 이런 과정에서 발생한 중요한 문제중의 하나가 불특정 다수가 자유로이 통신을 하기 위해 개발된 인터넷상에서 보안을 해결하는 것이다. 이 문제를 해결하기 위하여 많은 보안 관련 시스템들이 개발되고 있는 실정이고, 세계 각국의 표준 기구에서는 이러한 시스템에 대한 등급을 평가하고 있다. 각 등급을 살펴보면, 시스템 개발 초기부터 정형기법을 이용하여 개발되어진 시스템들이 고등급을 획득하고 있다. 국내에서도 한국정보보호센터(KISA)에서 보안 시스템에 대한 등급을 평가하고 있다. 본 논문에서는 높은 보안 등급의 IPSec 관련 시스템을 개발하기 위해서 개발단계에서 어떠한 정형기법들이 적용될 수 있는지를 살펴보겠다.

1. 서론

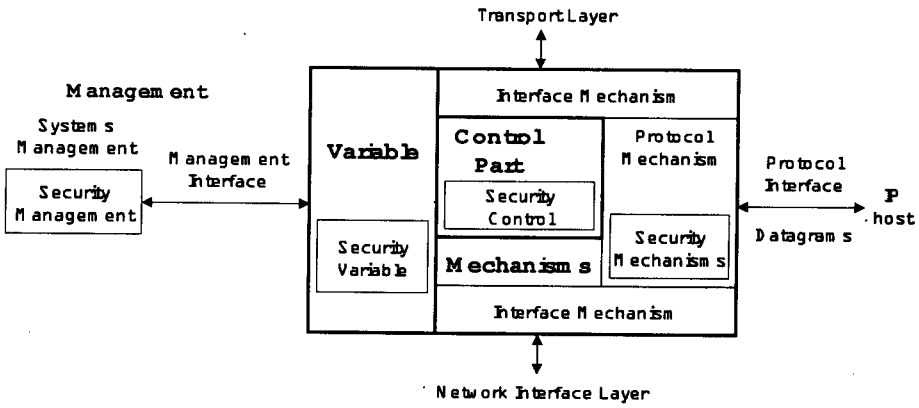
컴퓨터의 보급과 인터넷 기술의 발전으로 인하여 실제 사회 생활의 배경이 인터넷상으로 옮겨지고 있다. 이런 과정에서 불특정 다수의 사용자가 자유롭게 사용할 수 있는 인터넷상에서 신뢰할 수 있는 대상하고만 통신을 하며, 자신의 개인 정보의 유출을 최대한 막을 수 있는 여러 가지 기법들이 개발되고 있으며, 이런 기법들을 실제 인터넷상에서 적용을 하기 위해서 많은 시스템들이 개발되고 있다. 하지만, 어떤 시스템이 신뢰할 수 있는 지에 대한 연구가 진행이 되면서 세계 각국의 표준 기구에서는 이러한 시스템에 대한 등급을 평가하고 있다. 각 등급을 살펴보면, 시스템 개발 초기부터 정형기법을 이용하여 개발되어진 시스템들이 고등급을 획득하고 있다. 미국의 보안 등급인 TCSEC(Trusted Computer System Evaluation Criteria)을 관장하고 있는 기관인 NIST (National Institute of Standards and Technology)에 따르면 등급을 7등급으로 나누면서 정형기법을 사용하여 정형 도구를 사용해서 검증된 시스템에 대해서만 최고등급인 A1 등급을 주고 있으며, 이 등급에서 사용될 수 있는 정형 도구에 대해서도 리스트를 만들어서 검증된 도구만을 사용하도록 하였다. 국내에서도 한국정보보호센터에서 보안 시스템에 대한 등급을 평가하고 있으며, 정형기법을 적용한 시스템에 대해서만 최고등급인 K7 등급을 주고 있다[7]. 하지만, 국내에서는 이 분야에 대한 연구가 전무한 관계로 어떠한 방법론과 도구를 사용하는 것이 더 효율적인지에 대한 자료가 없기에 국제 표준으로 제정되어있는 정형명세언어인 Z[8]와 MSC[11]를 사용해서 IPSEC에 대해 정형 명세를 한 경험을 기술함으로써 등급 평가에 도움이 되고자한다. 논문의 구성은 2장에서 사용된 개념인 IPSEC을 설명한 후에 3장에서 IPSEC에 대한 정형 명세를 기술한 후에 4장에서 결론을 맺겠다.

2. IPSEC

IPv4와 IPv6에서 보안서비스를 제공하기 위하여 AH(Authentication Header)와 ESP(Encapsulating Security Payload)를 제공한다. IPSEC 메카니즘인 AH와 ESP는 정보보호 서비스로 인증, 무결성, 그리고 비밀성 서비스를 제공한다. 이러한 보호 메카니즘의 구현은 IPv6에서는 필수로 IPv4에서는 옵션으로 되었다[1, 2]

IP 보호 구조는 IPv6에서 절대 필요한 부분으로 정의되었다. 그러므로 IPv6를 구현하여 제품을 제공하는 벤드들은 AH와 ESP 기능을 제공하여야만 한다. 하지만 AH와 ESP가 지원된다고 해서 사용자들이 이 서비스를 사용해야만 한다는 것은 아니며 이 서비스가 필요하다면 이용할 수 있어야 한다는 것을 의미한다.

1) 본 연구는 2000년 한국정보보호센터의 지원을 받은 것입니다.



[그림 1] IPSEC의 개념적 모델

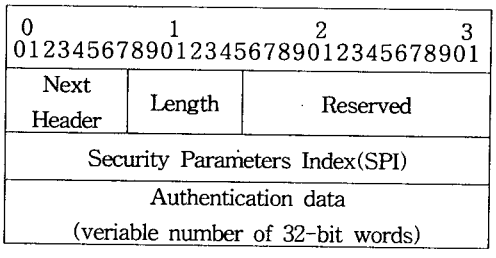
Karila의 "Open Systems Security - an Architectural Framework"[3]에서 나타낸 형식 모델(formal model)의 개념을 사용하면 보호 변수(security variable), 메카니즘(mechanism), 제어(control), 그리고 관리(management)로 구성할 수 있다. 이 개념적 모델은 [그림 1]과 같다.

이런 IPSEC의 구성을 위해서는 AH(Authentication Header), ESP(Encapsulating Security Payload)와 SA (Security Association)등이 필요하다.

IP AH는 IP 패킷의 데이터 무결성 및 인증을 제공한다. 이러한 인증 헤더의 구성은 [그림 2]와 같다[5].

ESP는 IP 패킷의 비밀성과 무결성을 제공한다[6]. 사용자의 요구에 따라 트랜스포트 계층 세그먼트를 암호화하거나 전체 IP 패킷에 대하여 암호화할 수 이다. TCP, UDP, ICMP 등과 같은 트랜스포트 계층 세그먼트를 암호화할 경우 이를 트랜스포트 모드 ESP라하며 전체 IP 패킷에 대하여 암호화할 경우 이를 터널-모드 ESP라 한다.

AH와 ESP는 전송자와 수신자간에 키, 인증 알고리즘, 암호 알고리즘, 그리고 이러한 알고리즘에 필요한 부가적인 파라메트 집합들에 대한 합의가 필요하다. 여기서 키, 인증 알고리즘 등 이들 각각을 보호 속성이라 하며 이러한 보호 속성들의 집합을 보호연관이라 한다[4].



[그림 2] 인증헤더

3. IPSEC에 대한 정형명세

이 절에서는 IPSEC에서 송수신 측에서 이루어지는 패킷과 전달되는 패킷에 대해서 양측에서 이루어지는 동작을 정형명세 언어인 Z와 MSC를 사용하여 명세하였다.

IPSEC은 암호화되어 인증된 패킷을 교환함으로써 비밀성과 인증을 해결한 통신을 하고자 하는 것으로 일반적으로 보호연관(SA)을 살펴보면, 인증 알고리즘으로는 MD5, 암호 알고리즘에는 DES를 사용하였다. 이러한 알고리즘에 대해서는 각각의 기능을 Z로 명세한 경험이 있다[12]. 여기서는 패킷의 형태는 Z를 이용하여 명세하고, 패킷의 전송은 MSC를 사용해서 명세를 하였다.

패킷의 형태를 살펴보면, 일반적인 패킷에 인증 헤더와 암호화 헤더가 첨가되어 있다. 명세된 패킷은 다음과 같다.

```
IP_Packet
Header
Hop-by-Hop
AuthHeader
ESP-Header
Encrypted-data
```

Header, AuthHeader와 같이 각각 명세된 부분은 스키마(Schma) 형식으로 각각의 다시 명세가 되어져 있다. 여기서 AuthHeader 라고 정의된 스키마를 살펴보겠다.

```
AuthHeader
Next Header, Length : EightBit
Reserved : SixteenBit
SecurityParametersIndex : ThirtytwoBit
AuthenticationData : Var
```

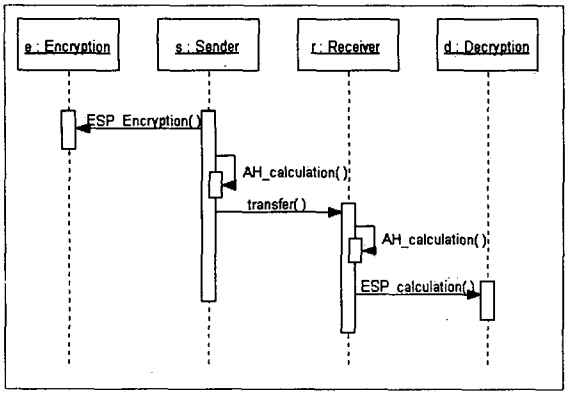
AuthHeader 스키마는 5개의 변수를 가지고 있으며, 변수명 뒤에 변수가 가지는 타입을 정의해 두었다. 예로 Length로 표

기된 변수는 32비트 단어로 된 인증헤더 필드의 길이를 의미하며, 8비트를 차지하고 있다. 이 부분은 스키마와 [그림 2]를 비교해서 살펴보면 구조가 동일하게 구성되었음을 알 수 있다.

이러한 스키마들로 패킷의 구조를 잡고 이런 패킷에 대해서 사용될 인증 알고리즘과 암호 알고리즘은 이전 논문[12]에서 작성된 부분을 사용하였다.

이제는 이런 패킷을 가지고 통신이 이루어지는 부분을 명세하기 위해서 MSC라는 정형기법을 사용하였다. MSC는 시스템의 구성요소들 사이의 상호작용을 기술하고 명세를 위한 그래픽 표현과 텍스트 표현을 동시에 지원하는 언어로서, 주로 통신시스템의 명세에 많이 사용되어진다.

이 부분에서 이루어지는 동작을 간략히 살펴보면, 송신측에서 일반적인 IP 패킷에서 전송하려는 자료를 DES를 사용하여 암호화한 후에 keyed MD5를 이용하여 인증된 값을 추가하여 수신측으로 패킷을 전송한면, 수신측에서는 도착한 패킷에 대해서 같은 알고리즘을 가지고 인증값을 계산하여 일치하면 DES를 이용하여 해독하여 자료를 전달받는 식으로 동작한다. 이 부분에 대한 MSC의 명세는 [그림 3]을 참고하기 바란다.



[그림 3] MSC로 작성된 패킷 전송

크게 송신과 수신, 암호와 복호되는 부분으로 나누었고, 암호화하는 ESP와 인증에 관여되는 AH을 계산하는 부분은 함수로 처리하였다.

여기서 함수 처리된 부분은 Z로 명세하였다. 여기서 발생될 수 있는 문제점은 Z와 MSC를 이용해서 명세되어 각 지원도구를 이용해서 검사된 결과를 통합하여 검사할 수 있는 방법에 대한 연구가 진행되어야할 필요성을 느꼈다.

4. 결론

앞에서 언급한 것과 같이 많은 수의 보안 시스템이 개발되고 있는 최근의 상황에서 국내외의 보안 등급에서 고등급을 획득하는 것은 산업적인 측면에서 매우 중요하다. 세계 각국의 표준기관에서는 여러 가지 정형기법을 적용해 본 결과를 가지고 고등급을 위해서 사용될 수 있는 도구의 리스트를 만들고, 각 도구를 사용할 때 어떠한 문서를 만들어서 제출하여야하는지에 대한 가이드라인을 만들어서 보안 시스템 벤더들에게 배포하고 있다. 국내에서도 한국정보보호센터에서 침입차단 시스템에 대한 등급을 평가하면서, 정형기법을 적용한 제품에 대해서 고등급을 주는 것도 이러한 맥락과 같은 것이다. 하지만, 이 분야에 대한 연구가 전무한 상태이기에 현재 등급평가를 의뢰하는 벤더들도 고등급을 고려하지 않고, 중간 등급으로 평가를 의뢰하고 있는 실정이다.

본 논문의 시도는 시스템의 개발에 적용 가능한 정형기법을 찾아서 사용함으로써, 등급에서 고등급을 획득하고자 하는 것이다. 여기서는 두 정형명세언어를 이용하여 IPSEC에 관련된 시스템을 개발하고자하는 경우에 명세를 진행해 나가면서 필요한 부분에 좋은 효과를 얻을 수 있는 기법을 선택할 수 있도록 간단한 부분에 대해서 두 가지 정형기법을 사용한 경험을 기술하였다. 여기서 발생할 수 있는 문제가 각 기법을 가지고 정확성이 검증되었다고는 하지만, 통합하였을 때에 발생할 수 있는 문제와 국제 표준으로 인정된 정형명세언어이지만, 검사를 위해서 사용된 도구에 대한 검증을 어떻게 할 것인가에 대한 문제가 발생할 수 있다. 따라서, 검증된 도구의 리스트를 만들어서 사용된 기법을 검사하는 것이 필요하다. 논문에서 작성된 Z 명세는 캐나다의 ORA 사에서 개발한 Z/EVES를 사용해서 검사하였으며, MSC는 UML에서 지원하는 VisualUML을 사용하였다.

5. 참고문헌

[1] William Stallings, IPv6 : The New Internet Protocol, http://www.comsoc.org/pubs/surveys/stallings/stallings-orig.html

[2] T. Aalto, "IPv6 Authentication Header and Encapsulated Security Payload", Seminar Presentation, Helsinki University of Technology, May 1996

[3] A. Karila. Open Systems Security - an Architectural Framework, Dissertation, Helsinki University of Technology, Espoo, 1991

[4] R. Atkinson, Security Architecture for Internet Protocol, RFC 1825, NRL, Aug 1995

[5] R. Atkinson, IP Authentication Header, RFC 1826, NRL, Aug 1995

[6] R. Atkinson, IP Encapsulating Security Payload, RFC 1827, NRL, Aug 1995

[7] 국내.외 정보 보호 시스템 평가 가이드, 한국 정보 보호센터, 1998.11.

[8] Antoni Diller, Z An Introduction to Formal Methods, John Wiley & Sons, 1992.

[9] John Nicholls, Z Notation Ver 1.2, ISO Panel JTC1/SC22/WG19, SEP 1995.

[10] Mark Saaltink. The Z/EVES User's Guide. TR-97-5493-06, ORA Canada. Sep. 1997.

[11] ITU-T, Message Sequence Chart(MSC). ITU-T, Geneva, 1994

[12] 유희준 강은영 최진영 이성권 김우곤, 보안 기능을 위한 정형화 설계 방법 연구, 정보과학회 추계학술대회, 1999