제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

안전한 시스템 상에서의 신뢰채널 구현에 관한 연구

유준석*, 임재덕*, 김정녀*
*한국전자통신연구원 정보보호연구본부
e-mail : jsyu92@etri.re.kr

A Study on the Implementation of Trusted Channel on Trusted Systems

Joon-Suk Yu*, Jae-Deok Lim*, Jeong-Nyeo Kim*
*Information Security Research Division, ETRI

요 약

신뢰채널은 시스템 사이에 신뢰성이 보장되는 통신 경로를 제공하며, 이는 통신 트래픽에 대한 기밀성 및 인증, 부인방지 등의 다양한 보안 서비스를 포함한다. 본 논문에서는 강제적 접근제어가 구현된 커널, 즉 보안 운영체제 사이에서의 신뢰채널 구현에 대해 설명한다. 설명하는 신뢰채널은 트래픽에 대해서 불법적인 노출과 변조를 방지할 수 있도록 기밀성 서비스와 인증 서비스 중 메시지 인증을 제공하며, IP 계층의 커널수준에서 구현되어 사용자에게 투명하게 동작한다.

1. 서론

현재의 유닉스나 리눅스와 같은 다중 사용자 환경에는 여러 가지 보안 위협 요소와 취약점들이 존재한다. 그 중에서 시스템 관리자, 즉 루트 사용자에게 모든 권한이 집중되어 있으므로 발생할 수 있는 문제나 트로이 목마와 같은 것들은 대부분 시스템 자체의 취약점으로 인한 것이며, 강제적 접근제어(Mandatory Access Control)나 역할기반 접근제어(Role-Based Access Control)와 같은 접근제어 메커니즘을 통하여 어느 정도 보완이 가능하다.

[1]에서는 기존 운영체제에 이러한 접근제어 메커니즘을 커널 수준에서 접목시킴으로써 기존의 운영체제의 보안성을 향상시킨 보안 운영체제를 개발하였다. 하지만 이러한 접근은 시스템 자체의 공격에 대한 보안성은 제공하지만 시스템 사이에서 통신되는 트래픽에 대한 보안성은 제공하지 않는다.

오늘날 대부분의 시스템들이 인터넷과 같은 개방형 네트워크에 연결되어 사용되고 있는 것이 현실이며, 따라서 통신되는 내용이 외부에 불법적으로 노출되거나 변조될 위험을 항상 지니고 있다. 따라서 네트워크를 통해 처리되는 정보의 가치가 커지고 있는 현실에서 네트워크 보안은 필수적인 요소로 자리 잡아가고 있다. 즉, 시스템 자체에 대한 보안만으로는 다양한 공격들로부터 정보를 안전하게 보호할 수 없으며, 시스템 보안과 더불어 네트워크 측면에서의 보안 수단도 강구되어야 한다.

신뢰채널은 시스템들 사이에서 신뢰성이 보장되는 통신경로의 제공을 의미하고 이는 통신 트래픽에 대한 기밀성 및 인증, 부인방지 등의 다양한 보안 서비스를 포함한다[2].

본 논문에서는 강제적 접근제어가 적용된 시스템 사이에서의 신뢰채널 구현에 대해서 설명한다. 설명하는 신뢰채널은 통신 트래픽에 대해서 불법적인 노출과 변조를 방지할 수 있도록 기밀성 서비스와 인증 서비스 중 메시지 인증을 제공한다. 본 신뢰채널은 IP 계층의 커널수준에서 구현되며, 사용자의 개입 없이 투명하게 동작한다.

본 논문은 다음과 같은 구성을 가진다. 2 장에서는 제공하고자 하는 신뢰채널 서비스의 대략적인 기능에 대해서 설명한다. 3 장에서는 신뢰채널의 설계 및 구현과 관련된 내용을 살펴보도록 하며, 4 장에 결론을 맺는다.

2. 기능개요

신뢰채널은 앞에서 언급한 바와 같이 보안 운영체제가 설치된 시스템 간의 통신 트래픽에 대해 기밀성 및 인증을 보장하기 위해서 사용된다. 이를 위해서 보안 운영체제가 설치된 시스템을 목적지로 가지는 출력 패킷에 대해서 암호화 수행 및 인증정보 추가를 수행하며, 수신된 패킷은 상위 프로토콜로 전달되기 전에 인증정보에 대한 검증과 복호화를 수행하게 된다.

송신측에서 패킷에 대한 신뢰채널의 적용 여부는 목적지의 주소와 사용자의 보안등급(MAC class)에 따라서 결정된다. 즉, 목적지의 주소가 등록된 신뢰시스템 목록에 포함되고 사용자가 보안등급을 가질 경우에만 신뢰채널이 적용되는 것으로 한정하고 있다. 단, 사용자가 보안등급을 가지지 않는 경우에도 ID 나 패스워드 등과 같이 보호되어야 할 정보들은 해당 애플리케이션 차원에서 제공되는 것으로 가정한다.

신뢰채널의 적용이 결정되어 사용될 때 신뢰채널의 인증과 기밀성 보장에 사용되는 키와 알고리즘은 미리 설정되어 있다고 가정한다.

3. 설계 및 구현

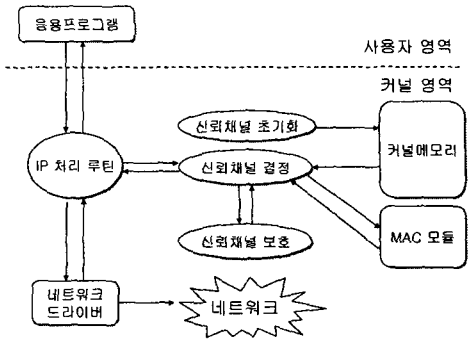
구현하는 신뢰채널은 FreeBSD 4.3 커널에 접근제어 메커니즘을 통합시킴으로써 보안성을 향상시킨 보안 운영체제가 설치된 시스템들 사이에서 통신되는 패킷에 대해서 적용된다. 신뢰채널 구현은 IP 계층에 통합되어 신뢰채널 적용이 결정된 패킷에 대해 암호화 및 인증작업을 처리하도록 구현된다.

패킷의 기밀성 보장을 위해서는 64 비트 블록암호 알고리즘인 blowfish 를 CBC(Cipher Block Chaining) 모드로 사용하며, 패킷 인증을 위해서는 HMAC-MD5 를 사용한다. Blowfish 는 현재 널리 사용되고 있는 DES 나 IDEA 보다 속도면에서 우수한 특성을 지니는 것으로 알려져 있다[3].

3.1 구조 및 구성

신뢰채널의 구현은 기능상 신뢰채널의 적용여부를 결정하는 신뢰채널 결정모듈과 신뢰채널 결정여부에 따라 패킷의 암/복호화 및 신뢰채널 헤더 관련 처리 등을 수행하는 신뢰채널 보호모듈, 그리고 각종 초기화를 수행하는 신뢰채널 초기화모듈로 나눌 수 있다. 이 중에서 신뢰채널 결정모듈과 신뢰채널 보호모듈은 IP 계층에 통합되어 구현되며, 이들은 송신측과 수신측에서 서로 상이한 기능을 수행하게 된다. 즉, 송신측에서 결정모듈은 패킷에 대해 신뢰채널 적용여부를 결정하며, 수신측에서는 수신된 패킷에 신뢰채널이 적용되었는지를 검사한다. 또한 송신측에서의 보호모듈은 신뢰채널 헤더의 생성 및 패킷 암호화 등이 이루어지고 수신측에서는 헤더의 제거 및 복호 등이 수행된다. 이는 이 후 절에서 패킷의 출력과 입력과정을 통해 상세하게 설명한다.

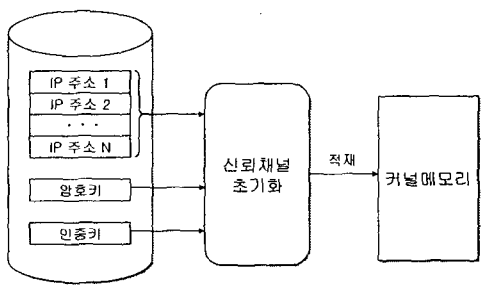
[그림 1]은 신뢰채널 서비스가 구현된 전체적인 구조를 도식화하여 간략하게 보여준다.



[그림 1] 전체구조 및 구성

3.2 설정파일 및 초기화

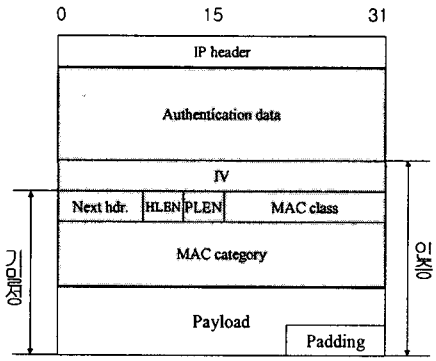
신뢰채널 설정파일은 패킷의 암/복호에 사용될 128 비트의 암호키를 저장하는 키 파일과 패킷의 인증에 사용될 128 비트의 인증키를 저장하는 인증 파일, 그리고 신뢰채널이 적용되어야 할 호스트의 주소 목록을 가지고 있는 호스트 파일로 이루어진다. 세 가지 설정파일은 보안 운영체제가 설치된 시스템들이 공통적으로 사용하게 되며, 각 시스템에서 보안 관리자 역할을 가진 특정 사용자(이하 보안 관리자)가 미리 생성하여 설정한다. 이 때 파일들은 보안 관리자만이 접근할 수 있는 특정 디렉토리에 저장되어 보관되는데, 이는 보안 운영체제의 RBAC 기능을 이용함으로써 가능하다. 설정파일은 시스템 부팅 시에 신뢰채널 초기화모듈에 의해 자동으로 커널 메모리로 로딩되어 사용된다. 따라서 해당 파일들은 보안 관리자만이 생성, 변경, 삭제 등을 수행할 수 있고 권한이 없는 사용자 혹은 공격자의 부당한 접근을 막을 수 있다. 또한 파일의 내용을 커널 메모리에 적재하여 사용하는 것은 시스템 운용 중에 발생하는 디스크 접근에 의한 오버헤드를 줄여줌으로써 시스템의 효율성을 높여주고 일반 메모리 영역보다 어려운 접근으로 인하여 높은 보안성을 제공한다. [그림 2]는 신뢰채널 구현에 사용되는 설정파일을 보여준다.



[그림 2] 신뢰채널 설정파일 및 초기화

3.3 신뢰채널 헤더

신뢰채널의 적용이 결정된 통신 트래픽에 대해서 신뢰채널을 적용하기 위해서 송신측에서는 신뢰채널 헤더를 생성하며, 이 헤더는 IP 패킷의 IP 헤더와 페이로드 사이에 삽입되며, 이러한 형태는 IPsec 에서 트랜스포트 프로토콜의 구성형태와 비슷하다[4, 5]. [그림 3]은 신뢰채널 헤더 및 전체적인 패킷의 형태를 보여준다.



[그림 3] 신뢰채널 헤더 및 패킷 형태

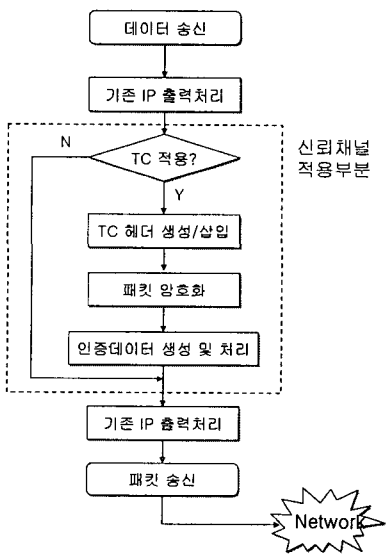
[그림 3]에서 음영으로 표시된 부분이 신뢰채널 헤더를 나타내며, 이는 7 개의 필드로 구성된다. 각 필드에 대한 설명은 다음과 같다.

- Authentication data : 128 비트의 값으로 인증이 수행되는 영역에 대한 해쉬값이다. 수신측에서 패킷의 변조여부를 확인하는 데에 사용된다.
- IV : 패킷의 기밀성 영역을 암호화 할 때 사용되는 64 비트의 값으로써 송신측에서 임의의 값을 생성하여 사용한다. 이는 헤더에 저장되어 수신측에서 패킷을 복호화 할 때 사용한다.
- Next header : 신뢰채널의 처리가 끝나고 처리되어야할 상위 프로토콜을 나타낸다. 이는 기존 IP 헤더에서 다음 프로토콜 필드의 값이며, IP 헤더의 다음 프로토콜 필드는 신뢰채널이 적용되어 신뢰채널 헤더가 IP 헤더 뒤에 존재한다는 의미를 나타내는 프로토콜 매크로로 변경된다.
- HLEN : 기존 IP 패킷에 덧붙여지는 신뢰채널 헤더의 총 길이를 4 바이트 단위로 나타낸다. 최대 60 바이트를 표현하지만 신뢰채널 헤더는 36 바이트의 고정된 크기를 가진다.
- PLEN : 패킷의 암호화를 위해 패킷에 덧붙여지는 패딩의 길이를 나타낸다. Blowfish 의 경우에 8 바이트 단위로 암호화가 이루어지며, 따라서 0 에서 7 의 값을 가진다. 패딩되는 비트는 '0'을 사용한다.
- MAC class : 패킷을 전송하는 사용자의 보안등급 값이다. 이는 원격 호스트로 전송되는 자료의 보안정보 설정에 사용된다.
- MAC category : 패킷을 전송하는 사용자의 보안범주 값이다. 이는 원격 호스트로 전송되는 자료의 보안정보 설정에 사용된다.

3.4 패킷 출력 및 입력

패킷의 출력과 입력과정에 있어서 신뢰채널 결정모듈과 신뢰채널 보호모듈의 역할은 상이하며, 본 절에서는 각 과정에 있어서 패킷의 처리과정에 대해서 설명한다.

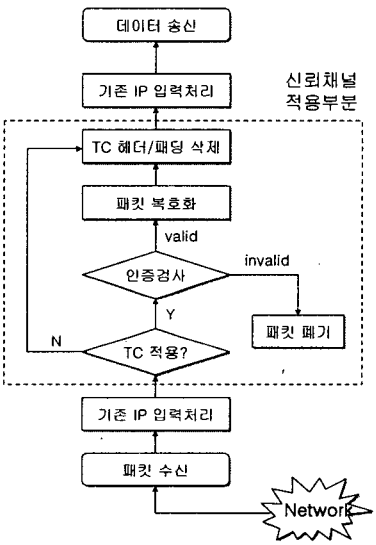
우선 출력과정에서 사용자 프로세스로부터 데이터 송신 요청이 발생하면 해당 요청은 상위 프로토콜 처리를 수행하는 루틴을 거쳐 IP 계층에서 출력을 담당하는 *ip_output()*까지 전달된다. 이 루틴에서는 일정한 IP 처리 절차를 수행하고 패킷을 단편화하여 하위 계층으로 넘기기 전에 TDB 를 호출하여 신뢰채널 적용여부를 판단하게 된다. 이 때 판단은 목적지의 주소와 사용자의 보안등급을 기반으로 이루어진다. 목적지 주소가 커널 메모리에 적재된 주소 목록에 있을 경우에는 사용자의 보안등급을 확인하여 사용자의 보안등급이 존재할 경우에만 신뢰채널의 적용을 결정한다. 이 경우에는 실질적인 신뢰채널 처리를 수행하는 신뢰채널 보호모듈로 제어가 넘어가며, 신뢰채널을 적용할 필요가 없으면 기존의 IP 출력 처리를 수행하게 된다. 신뢰채널 보호모듈에서는 신뢰채널 헤더를 생성하여 패킷에 추가하고 지정된 알고리즘을 통하여 패킷을 암호화 한다. 그리고 암호화된 패킷에 대하여 인증정보를 생성하여 신뢰채널 헤더에 추가한다. 이상 처리가 완료되면 제어는 기존 IP 출력 루틴으로 넘어가고 IP 출력 루틴은 패킷의 단편화를 수행한 후 하위 계층의 출력 루틴으로 패킷을 전달한다. [그림 4]는 패킷의 출력과정을 도식화하여 보여준다



[그림 4] 출력패킷 처리

패킷이 수신되면 하위 프로토콜의 입력 루틴을 거쳐 IP 계층에서 입력을 담당하는 *ip_input()*까지 전달

된다. 패킷을 전달받은 IP 입력 루틴은 패킷의 재조합 및 기타 처리를 수행하고 패킷을 상위 계층으로 넘기기 전에 신뢰채널 결정모듈을 호출하게 된다. 수신측의 신뢰채널 결정모듈에서는 전달된 패킷이 신뢰채널이 적용되어 암호화된 패킷인지를 검사한다. 이는 IP 헤더에서 다음 프로토콜을 나타내는 필드를 확인함으로써 이루어진다. 만약 신뢰채널이 적용된 패킷이라고 결정되면 신뢰채널 보호모듈로 제어가 넘어가게 되는데 TPB 에서는 이미 설정된 인증키와 알고리즘을 통하여 해당 패킷을 인증한다. 인증을 통과한 경우에만 패킷은 복호화되고 신뢰채널 헤더와 패딩값이 제거된 후 상위 프로토콜로 패킷이 전달한다. 만약 신뢰채널이 적용되지 않은 패킷이라고 판단되면 기존 IP 처리와 동일하게 그대로 상위 계층으로 패킷이 전달된다. [그림 5]는 패킷의 입력과정을 도식화하여 보여준다.



[그림 5] 수신패킷 처리

4. 결론 및 향후 연구

다양한 접근제어 메커니즘을 기존 운영체제의 커널 수준에서 통합시킨 보안 운영체제[1]는 기존 운영체제에서 가지고 있던 시스템 자체의 취약성에 대해서 일정 수준의 대안을 제시하고 있으나 스니핑이나 스푸핑과 같은 네트워크 상에서 이루어지는 공격들에 대해서는 무방비로 노출되어 있는 상태이다.

본 논문에서는 보안 운영체제가 설치된 시스템간의 통신에서 기밀성과 메시지 인증을 제공할 수 있는 신뢰채널 구현에 대해 기술하였다. 본 신뢰채널은 사용자 보안등급에 기초하여 트래픽을 암호화 함으로써 중요 자료에 대한 기밀성을 제공할 수 있으며, 부가적으로 모든 트래픽의 암호화로 인해 발생하는 과부하를 줄일 수 있다. 또한 커널수준에서 구현되며, 추가적인 사용자의 개입없이 투명하게 사용될 수 있다는 장점을 지닌다. 하지만 신뢰채널의 사용을 위해 모든 신뢰 시스템에서 동일한 설정파일을 미리 수동적으로 설정해야 한다는 점은 시스템의 관리적인 측면에서 오버헤드로 작용할 수 있을 것이다. 지금까지 설명한 신뢰채널이 프로토타입의 성격을 가지고 있다는 점을 감안한다면 향후 개발에 있어서는 이러한 관리적인 측면에서의 개선이 있어야 할 것이다.

참고문헌

[1] J. G. Ko, J. N. Kim, & K. I. Jeong, "Access Control for Secure FreeBSD Operating System", *Proc. of WISA2001, The Second International Workshop on Information Security Applications*, 2001

[2] "Common Criteria for Information Technology Security Evaluation , Part 2: Security functional requirements, Version 2.1", 1999

[3] B. Schineier, "Description of a New Variable-Length Key, 64-Bit Block Cipher(Blowfish)", Fast Software Encryption, Cambridge Security Workshop Proceedings, Springer-Verlag, 1994

[4] RFC 2401, "Security Architecture for the Internet Protocol", 1998

[5] 이만영 외 공저, " 전자상거래 보안 기술", 생능출판사, 1999

[6] 김병철 외 공역, "TCP/IP 프로토콜", 도서출판 미래컴, 2000