보안 강화를 위한 액티브 패킷 모델 설계

이남석[0] 양일권 박영수 이상호
충북대학교 전자계산학과
cooper@cnlab.chungbuk.ac.kr

Design Active Packet Model For Security

Nam-suk Lee[0] Eal-kuen Yang, Young-su Park, Sang-ho Lee
Dept. of Computer Science, Chung-buk National Univ.

요 약

기존의 네트워크에서는 새로운 프로토콜을 개발하고 전개한다는 것은 많은 표준화 절차를 요구하고, 관련 응용에서 모든 요구를 네트워크가 수용할 수 없기 때문에 제한적이다. 액티브 네트워크는 네트워크에 프로그래밍이 가능하다는 것으로 새로운 네트워크의 패러다임으로 등장하였다.

액티브 네트워크는 복잡한 구조를 갖고 있고, 보안상으로도 많은 문제점을 갖고 있다. 이 논문에서는 액티브 네트워크의 보안 모델을 소개하고, 보안과 관련된 새로운 옵션을 추가한 패킷모델, 액티브 네트워크의 구조인 실행환경과 노드 운영체제에서의 패킷 처리 과정을 알아본다.

1. 서 론

액티브 네트워크(Active Network) 기술은 좀 더 진보된, 융통성 있는 새로운 네트워크 패러다임이다.
액티브 네트워크는 노드에 프로그램 가능한 인터페이스를 제공하고, 노드들이 패킷 연산을 수행하고 수정할 수 있다는 점에서 이러한 네트워크를 액티브라 한다. 액티브 네트워크는 새로운 서비스를 구성하거나 개량하는 것을 제공하고, 새로운 네트워크 서비스를 개발하고 배치하는데 드는 시간을 줄일 수 있다. 또한 긴 표준화 작업을 거치지 않고도 새로운 서비스를 빠르게 배치할 수 있게 하며 변화하는 요구 사항들에 대해 네트워크가 민첩하게 받아들일 수 있도록 하는데 사용된다. 네트워크 노드에는 사용자 프로그램을 주입할 수 있는 응용 기반 구조를 제공한다.

액티브 네트워크의 구성 요소에서, 기존의 네트워크의 패킷에 해당하는 캡슐이 있는데 사용자의 데이터와 프로그램 혹은 그에 상응하는 내용을 담고 있다. 액티브 패킷 혹은 스마트 패킷이라 부른다.
액티브 노드는 액티브 패킷을 생성할 수 있는 액티브 클라이언트 혹은 액티브 서버를 일컫는다.
액티브 네트워크는 소프트웨어 구조로서 실행 환경(Execution Environments)과 노드 운영체제(NodeOS)로 구성된다. 실행 환경은 프로그램과 데이터를 포함하고 있는 액티브 패킷을 처리하고, 노드 운영체제는 패킷 스케줄링, 자원 관리, 패킷 분류 등과 같은 서비스를 제공하며, 노드 운영체제 상에서 운영되는 실행 환경에 대해 여러 서비스를 제공한다.[1][2]

액티브 네트워크는 지금까지의 네트워크보다 훨씬 더 복잡할 뿐만 아니라 보안상의 많은 문제점을 가지고 있다. 이 논문에서는 액티브 네트워크에서의 보안을 위한 구조를 소개한다.
액티브 네트워크에서 액티브 패킷과 액티브 노드들을 어떻게 보호할 것인가가 중요한 문제가 된다. 액티브 네트워크의 응용과 서비스와 라우터들은 상호 인증에 의한 신뢰를 기반으로 이루어 질 수 있고, 암호화와 전자서명(digital signature)은 프로그램 코드와 데이터를 포함하는 액티브 네트워크 패킷들의 비밀성과 무결성을 보장할 수 있다. 보안 정책들은 코드와 데이터가 제한된 경로를 사용하고 라우터 자원에게 제한된 접근을 하도록 한다.[1]

이 논문에서는 액티브 네트워크의 보안 모델을 소개하고 패킷 구조 설계와 그 패킷의 프로세스에 대해 알아본 후 결론을 맺는다. 여기서는 액티브 네트워크의 여러 프로젝트들과 관련하여, 어떤 특정한 모델을 가정하여 기술하지는 않는다.

2. 액티브 네트워크의 보안 모델

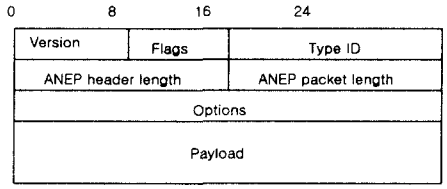
액티브 네트워크의 보안 구조는 인증(authentication), 권한부여(authorization), 무결성(integrity) 등 보안의 기본적인 문제에 대한 해결책을 제시하고 신뢰할 수 있는 모델을 제공해야 한다.[1]
인증은 액티브 패킷에 응답할 수 있는 통신 주체(principal)를 부여하는 것이다. 실제로 통신 주체는 가능한 대상자의 신원을 정확하게 확인하기 위하여 전자서명된 패킷을 가질 수 있다. 신원이 인증되었을 때 신원 및 부가 정보를 나타내는 인증 정보를 가진 인증서를 받는다. 인증서는 변경이나 위조를 방지하기 위하여 암호학적으로 보호된다.[1][2]
권한 부여는 액티브 패킷이 네트워크의 자원 상에서 동작할 수 있도록 하는 것이다. 즉 보안 구조가 인증된 통신주체의 요청에 대하여 어떤 보안 관련 엑세스를 부여할 것인

지를 결정하는 과정이다. 가장 보편적인 권한부여 모델은 접근제어 리스트(ACL : Access Control Lists)모델이며 이것은 네트워크 자원에 대해 통신주체 및 역할의 접근 권한을 기술하고 부여한다.[1][3]
액티브 패킷들이 신뢰할 수 없는 네트워크를 통해서 전달되거나 잘못된 노드에서 실행될 때 액티브 패킷들이 위조되거나 변경되는 것을 방지할 수 있어야 한다. 따라서 양 종단뿐만 아니라 중간에 놓인 모든 노드들 사이의 신뢰 관계를 설정할 수 있도록 홉별로 제어(hop-hop control)하는 것이 필요하다.[1][4]

실행환경 인터페이스는 thread pools(computation), memory pools(memory), channels(communication), files(persistent storage)와 domains 과 같은 액티브 노드 운영 체제의 자원을 추상화한다. 도메인은 자원을 관리하고, 메시지가 전송되는 채널의 집합을 할당하는데 기본적인 추상화 부분이다. 채널은 노드의 안팎에서 패킷의 통신을 위한 기본적인 추상화 부분이다.[2][5]

도메인은 서브도메인을 생성한다. 통신 주체는 도메인의 생성시간에 만들어지고, 그 후의 도메인 동작들을 제어한다. 노드는 하나 또는 그 이상의 도메인을 실행환경(EE)에 할당된걸 갖고 동작을 시작한다. 실행환경(EE)은 패킷속의 액티브 코드가 실행환경(EE)의 도메인의 일부에서 동작할지를 결정한다.[6]

액티브 패킷이 도착하면, in-channel에 노드에 의해 할당이 되고 처리된다. 액티브 패킷 처리가 실행환경(EE)에서 발생하면 액티브 코드는 실행환경(EE)서비스와 자원을 엑세스하면서 실행하고 액티브 패킷에서 처리 결과는 out-channel로 전송된다. 그 전송된 패킷은 패킷들에 포워딩되고, 수정, 삽입될 수 있다. 패킷에 대한 처리는 노드나 실행환경(EE)에서 그 결과가 계속적으로 변하게 된다.[7]



<그림 1. ANEP Definition>

Source Identifier	1
Destination Identifier	2
Integrity Checksum	3
N/N Authentication	4

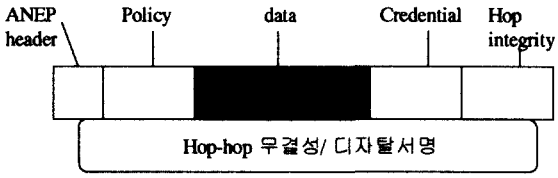
<Option Type>

액티브 패킷은 인터넷상에서 ANEP(Active Network Encapsulation Protocol)를 사용하여 전송될 수 있다. ANEP는 Type ID 필드를 포함한 header 포맷을 제공하고, 패킷이 전달되는 EE를 제공한다. ANEP header는 type-length-value필드를 정의한 옵션을 제공하고, 그 옵션은 근원지, 도착지, 무결성, 종단간의 인증을 포함한 ANEP 프로토콜에서 정의한다.[2][7]

3. 패킷 보안 모델

3.1 패킷 구조

패킷 구조는 인증서 리스트, 정적이고 가변적인 패킷 payload를 분리, 부인하지 않는 암호화된 인증을 지원해야 한다. 패킷 구조는 다음과 같다.[7]



<그림 2. Packet Format>

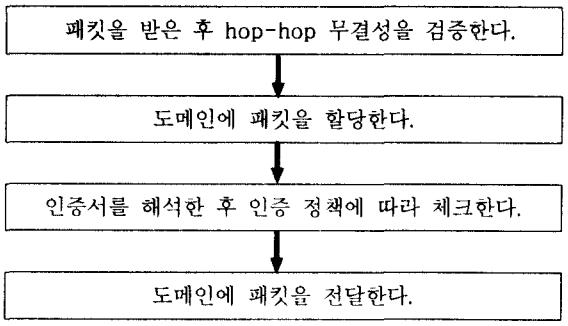
Option Type Value	Name
1	Hop Integrity
2	Credentials
3	Varying NodeOS data
4	Static Payload
5	Varying Payload
6	Policy

<표1. 새로 정의된 옵션>

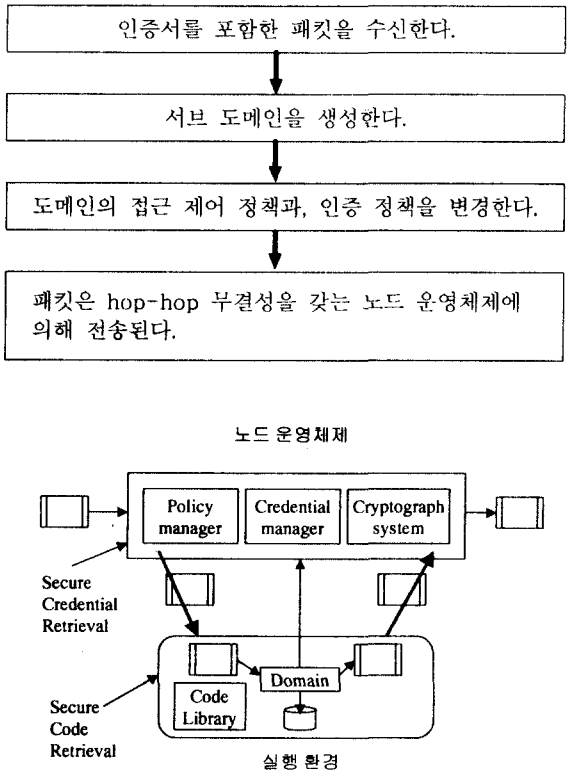
3.2 패킷의 이벤트 처리

다음은 보안능력을 갖고 있는 패킷과 도메인의 이벤트 처리 과정이다.

3.2.1 노드 운영체제에서의 처리 과정



3.2.2 실행 환경에서의 처리 과정



<그림 3. Packet 처리>

4. 결론

액티브 네트워크와 같은 융통성 있는 환경에서의 노드들과 패킷들을 보호하는 것은 쉬운 일이 아니다. 이 논문에서는 액티브 네트워크 환경의 이해와 보안 모델 구조, 그리고 패킷을 정의하였다. 그리고, 제시된 패킷 모델을 기반으로 실행 환경과 노드 운영체제 사이의 패킷 처리 과정을 통해, 인증 과정을 알아보았다.
패킷에 보안과 관련된 여러 새로운 옵션들을 정의함으로서, 패킷 인증을 통해 액티브 노드를 보호 할 수 있다.

이 논문을 포함한 기존의 연구 결과에서 액티브 네트워크에 대한 다양한 보안 모델들은 네트워크에서의 시험이 부족하다. 따라서 적절한 안전성 및 보안 요구사항을 만족시키기 위해 여러 네트워크 환경에서 실험되어야 한다.

5. 참고 문헌

[1] 박정민, 채기준, "Active Network의 보안 기술 발전 전망" 정보통신응용연구회 SIGCOMM REVIEW 2000.12
[2] 이중수, 이승헌, 이영희, "Active Network 구조 : 문제점 및 접근 방법", 정보통신응용연구회 SIGCOMM REVIEW 2000.12
[3] AN Node OS Working Group, "NodeOS interface specification" January 2000
[4] Bob Lindell, draft-nodeos-security-00.txt, "Active Networks Protocol Specification for Hop-by-hop Message Authentication and Integrity"
[5] Zhaoyu Liu, Roy H. Campbell, and M. Dennis Mickunas, "Securing the node of an active network" in Active Middleware Services September 2000
[6] AN Security Working Group, "Security architecture for active nets" July 1998
[7] S. Murphy, E.Lewis, "Strong Security for Active networks", IEEE OPENARCH 2001