효과적인 액티브 네트워크에서의 보안서비스를 위한 ANASP시스템

한인성*, 김진묵*, 유황빈*
*광운대학교 컴퓨터과학과
e-mail:(ishan,jmkim,ryou)@netlab.kw.ac.kr

ANASP System for Effective Active Network Security

In-sung Han*, Jin-muk Kim*, Hwang-Bin Ryou*
*Dept of Computer Science, Kwang-woon University
e-mail:(ishan,jmkim,ryou)@netlab.kw.ac.kr

요 약

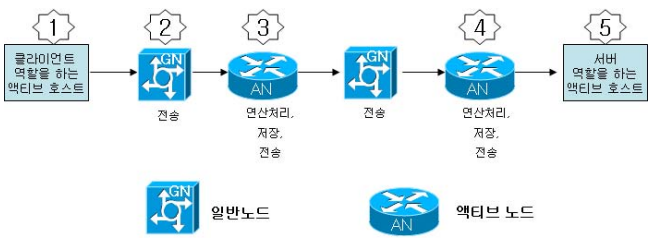
액티브 네트워크란 네트워크에 프로그램 가능한 라우터나 스위치를 배치하여, 전송되는 패킷들을 서비스 특성이나 사용자 요구에 따라 적합하게 연산, 처리작업을 수행하고 수정할 수 있는 네트워크를 말한다. 그러나 이러한 액티브 네트워크의 단점은 기존의 패시브 네트워크가 패킷 포워딩 기능만을 제공하는 것에 비해 더욱 복잡한 네트워크 상태로 인해 보다 많은 보안상의 위협과 공격이 훨씬 쉽고 다양하다. 이에 따라 보안 및 안전의 문제가 중요한 관심사가 되었다.

본 논문에서는 악의적인 목적으로 액티브 노드의 취약성을 이용하여 어플리케이션 코드를 액티브 노드에 설치하게 되어 전체적인 네트워크를 위협할 수 있는 액티브 네트워크의 단점을 보완하고자, 설치하려는 어플리케이션 코드에 대한 인증 및 무결성 과 접근권한 기법을 이용한 어플리케이션 코드의 관리 와 전송제어를 하는 ANASP시스템을 설계 및 구현하고자 한다.

1. 서론

미국 방위 고등 연구 계획국(DARPA)에서 제안된 액티브 네트워크는 단순히 패킷을 전송하는 방식인 기존의 패시브 네트워크에 프로그램 가능한 라우터나 스위치를 배치하여, 전송되는 패킷들을 서비스 특성이나 사용자 요구에 따라 적합하게 연산, 처리할 수 있는 차세대 네트워크 구조에 대한 새로운 접근 방법이다[3].

[그림 1]은 액티브 네트워크의 기본 동작 과정을 그림으로 나타낸 것이다.



[그림 1] 액티브 네트워크의 기본 동작

동작과정은 다음과 같다[2].

① 클라이언트 역할을 하는 액티브 호스트는 데이터와 어플리케이션 코드를 포함하고 있는 액티브 패킷을 일반 노드(스위치나 라우터) 또는 액티브 노드(액티브 스위치 혹은 액티브 라우터)로 구성된 액티브 네트워크에 전송한다.

② 일반노드가 액티브 패킷을 수신한 경우에는 기존의 패시브 네트워크에서와 마찬가지로 다음 노드로 패킷을 전송한다.

③ 액티브 노드가 액티브 패킷을 수신한 경우에는 수신한 패킷의 액티브 패킷여부를 판단하고, 패킷의 데이터를 처리할 코드를 검색한다. 이때, 액티브 패킷에 어플리케이션 코드가 포함되어 있다면, 코드를 액티브 노드에 설치하고 패킷 내부의 데이터를 연산한 후 다음 노드로 전송한다.

④ 액티브 패킷 데이터를 처리할 수 있는 적합한 코

드가 포함되어 있지 않거나 액티브 노드에 설치되어 있지 않았다면 기존의 네트워크와 마찬가지로 다음 노드로 전송한다.

⑤ 최종적으로 서버 역할을 하는 액티브 호스트는 수신한 액티브 패킷의 데이터를 목적에 맞게 처리한다.

위와 같이 액티브 네트워크 기술은 상대적으로 패시브 네트워크가 갖고 있던 자원의 비효율성, 수동성, 신기술과 새로운 서비스 개발 및 네트워크 관리 등의 어려움 등을 개선할 수 있는 차세대 네트워크 구조의 대안이다[3][4].

그러나, 액티브 네트워크는 전송중인 액티브 패킷의 어플리케이션 코드를 액티브 노드에서 실행할 수 있으며, 네트워크로 전송된 코드의 실행 결과에 따라 액티브 노드의 상태를 변경할 수 있어, 패킷의 전송 기능만을 수행하는 패시브 네트워크에 비해 더욱 복잡한 네트워크 상태를 갖게 된다. 이로 인해 보다 많은 보안상의 위협과 공격이 훨씬 쉽고 다양한 방법이 가능하다[1][5][6].

보안에 있어 가장 먼저 해결해야 할 문제 중에 하나는 노드에 대한 인증의 필요성과 설치하려는 액티브 코드의 위해성 여부를 판단하는 것이다.

본 논문에서는 악의적인 목적으로 액티브 노드의 취약성을 이용하여 어플리케이션 코드를 액티브 노드에 설치하게 되어 전체적인 네트워크를 위협할 수 있는 액티브 네트워크의 단점을 보완하고자, 설치하려는 어플리케이션 코드에 대한 인증 및 무결성 과 접근권한 기법을 이용한 어플리케이션 코드의 관리와 전송제어를 하는 ANASP시스템을 설계 및 구현하고자 한다.

본 논문의 구성은 다음과 같다. 먼저, 2장에서는 액티브 네트워크의 개요와 구조, 기술방식에 대해 설명하고, 3장에서는 본 논문에서 제안하고자 하는 ANASP시스템을 이용한 액티브 네트워크 보호 방법에 대해 설명하며, 4장에서는 ANASP시스템의 구성과 어플리케이션 코드를 설치하려는 액티브 노드들의 에이전트 구성에 대해 설명한다. 5장에서는 본 연구에 대한 결과 및 향후 계획을 서술하였다.

2. 네트워크 개요 및 구조 기술방식

액티브 네트워크는 수신한 액티브 패킷을 액티브 노드에서 최적화된 패킷 데이터의 연산을 수행하고 이를 다음 노드로 전송함으로써 기존의 네트워크에 비해 좀 더 효율적이고 능동적인 네트워크를 구성하고자 하는 아이디어이다[7].

액티브 네트워크 구조 정의 방식[3]은 크게 3가지 방식이 있다. 이는 액티브 노드상에서 데이터를 처리하기 위해 액티브 코드를 어떻게 처리하는가에 의해 구분된다.

■ 분리 방식: 액티브 코드들이 스위치나 라우터가 제조될 때 이미 설치되어 있는 방식이다. 동작방법은 설치되어 있는 액티브 코드가 데이터를 수신해 처리한 후, 다음 노드로 전송하는 방식으로 노드가 원하는 새로운 액티브 코드를 추가시키기가 불가능하다.

■ 통합/캡슐 방식: 스위치나 라우터는 액티브 코드를 저장하고 있지 않고, 각 노드는 코드와 데이터를 액티브 패킷 형식으로 전달한다. 단점은 코드의 양이 클 경우, 네트워크 상에서 트래픽 문제, 패킷 분실시 재 전송 문제 등으로 인한 효율성이 저하될 수 있다.

■ 혼합 방식: 패킷 전달 과정에서 발생하는 지연이나 분실에 따른 비효율성을 제거하기 위하여 위의 두 가지 방식을 혼합하여 이용하는 방식이다.

3. 연구 목적 및 보안 시스템 제안

현재 액티브 네트워크는 클라이언트 역할을 하는 액티브 호스트가 어플리케이션 코드를 액티브 패킷으로 캡슐화(데이터와 프로그램을 담은 패킷 기술)하여 액티브 노드로 전송하거나 공통적으로 사용하는 코드를 액티브 노드에 미리 설치해 두는 혼합 방식에 대한 개발이 활발하게 연구되고 있다. 캡슐화된 액티브 패킷을 수신한 액티브 노드는 액티브 패킷으로부터 코드를 분리하고, 액티브 노드의 실행환경에 맞춰 설치한다. 코드를 설치한 액티브 노드는 클라이언트 역할을 하는 액티브 호스트에서 전송한 데이터그램 패킷의 페이로드 영역에서 데이터를 추출하여 사전에 설치된 액티브 코드가 이를 처리한다.

액티브 노드 환경에서 액티브 코드를 전송하려는 액티브 호스트에 대한 인증과 액티브 코드 자체의 안전성 및 무결성의 검증은 반드시 필요한 기본적인 보안요소이다. 서버 역할을 하는 액티브 호스트의 코드가 악의적인 목적을 갖거나 프로그램상의 문제가 있는 코드를 안전성 검증을 무시하고 액티브 노

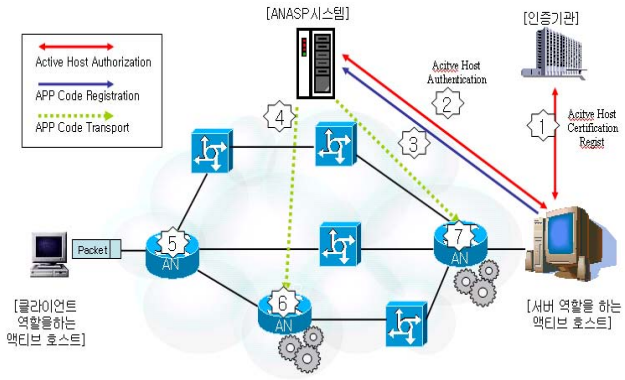
드로 전송하여 설치될 경우, 예기치 않은 실행 오류나 액티브 노드의 성능저하 뿐만 아니라 전체 네트워크의 성능저하를 일으킬 수 있다. 또한, 코드의 무결성 검증이 이루어지지 않을 경우 악의적인 목적을 갖는 호스트로 인해 단일 액티브 노드뿐만 아니라 최악의 경우 액티브 노드의 무차별적인 공격으로 네트워크 전체를 마비시킬 수 있는 잠재적인 위협요소로 확대될 수 있다. 현재, 액티브 노드 보호를 위해 많은 연구가 계속 진행되고 있지만, 근본적인 액티브 노드의 안전성을 보장하지 못하고 있는 상황에서 액티브 네트워크에 대한 취약성을 보완하기 위해 반드시 새로운 보안체계가 필요하다[7].

본 논문에서는 액티브 코드의 설치를 요청하는 서버 역할의 액티브 호스트를 인증하고 접근권한을 통해 안전성 검증을 거친 어플리케이션 코드의 관리 및 제어를 통해 인증된 관리 도메인내의 액티브 노드로 터널링기법으로 전송하여, 설치하는 과정 중에 발생 할 수 있는 위험에 대처하며 어플리케이션 코드의 빠른 배치를 함으로써 네트워크 성능을 보완하기 위해 ANASP시스템을 제안하고자 한다.

4. ANASP시스템 개요

본 논문에서 제안하는 ANASP(Active Network Application Sending Provider)시스템은 인증기관으로부터 발급받은 인증서를 이용해 어플리케이션 코드의 설치를 필요로 하는 서버 역할 액티브 호스트를 인증하고, 서버 역할 액티브 호스트는 ANASP 시스템으로 어플리케이션 코드등록 서비스를 요청한다. 관리도메인내의 액티브 노드로 설치하려는 코드는 ANASP 시스템으로 전송되어 코드의 위험성을 판단하는 검증 절차를 거쳐 ANASP 시스템에 저장된다. 서버 역할 액티브 호스트는 ACL을 통해 접근 권한을 확인하고 코드의 설치 권한이 있다면, 관리 도메인 네트워크내의 액티브 노드에 코드를 설치할지 여부를 결정을 확인한다. 어플리케이션 코드 설치를 필요로 하는 액티브 노드의 선택을 완료함으로써 ANASP시스템은 코드를 ANEP 프로토콜로 캡슐화 및 인증 메커니즘을 추가해 UDP 패킷을 이용해 액티브 노드로 전송하여 설치한다. ANASP시스템을 이용하는 액티브 네트워크 구성요소는 클라이언트 역할 액티브 호스트, 서버 역할 액티브 호스트, 액티브 노드, ANASP 시스템, 일반노드, 인증 발급 시스템 등으로 구성하는 것으로 가정하며 어플리케이션 코드를 운반하는 액티브 패킷은 Active Network Encapsulation Protocol(ANEP)의 구조를 따르고 본 논문에서 코드를 이용해 순수한 데이터를 처리하도록 데이터를 전송하는 패킷을 데이터 그램 패킷이라 부른다. 또한 액티브 패킷을 전송하고 수신하는 포트는 UDP 포트를 사용했다.

[그림 3]은 ANASP 시스템을 이용한 전체 액티브 네트워크 구조를 나타낸다.

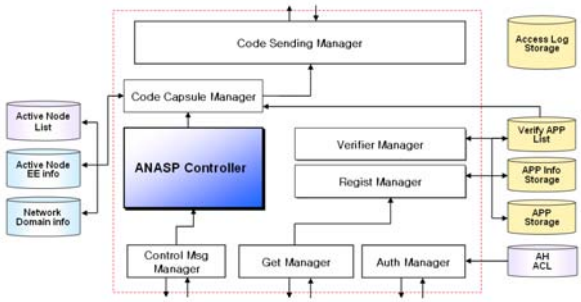


[그림 2]ANASP 시스템을 이용한 액티브네트워크 구조

4.1 ANASP 시스템 구조

ANASP시스템의 구성은 크게 서버 역할 액티브 호스트의 인증과정 후 권한 설정이 이루어지는 관리자, 어플리케이션 코드를 수신 및 수신된 어플리케이션 코드와 코드의 정보를 분리해 어플리케이션 번호를 부여하고 각각 데이터를 저장하는 관리자, 네트워크 정보와 관리 도메인에 존재하는 액티브 노드의 정보와 코드의 캡슐화 및 인증 정보를 추가하는 관리자, 액티브 노드로 어플리케이션 코드를 전송하는 관리자, 어플리케이션 코드를 서버 역할 액티브 호스트의 요청으로 코드의 제어 및 각각의 관리자를 관리하는 ANASP 컨트롤러로 구성해 볼 수 있다. 데이터 저장은 코드를 저장할 수 있는 APP Storage, 서버 역할 액티브 호스트의 코드제어 요구 메시지나 어플리케이션 검증 결과 또는 시스템 내부에서 발생한 이벤트를 저장하는 저장 장치, 서버 역할 액티브 호스트의 접근권한을 검사하는 ACL, 액티브 노드들의 정보가 있는 액티브 노드의 정보저장 장치, 코드가 설치될 노드의 EE 정보가 있는 액티브 노드 EE 저장 장치 및 관리 도메인의 노드 구조 를 갖는 저장 장치로 구성관리 된다.

[그림 3]는 ANASP시스템의 구성도를 나타내고 있다.

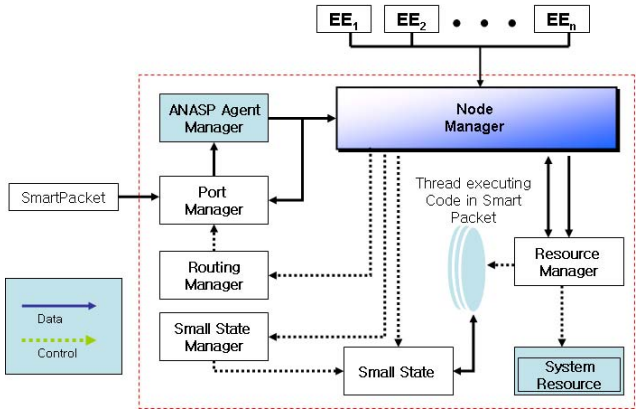


[그림 3] ANASP 시스템 구조

본 논문에서 제안하는 ANASP시스템의 내부 구조를 이루는 핵심 모듈들을 살펴보면, 서버 역할 액티브 호스트를 인증하기 위한 Auth Manager, 코드 등록을 위한 Get Manager, 서버 역할 액티브 호스트의 코드처리 요청을 수신하는 Control Msg Manager가 있다. 또한 서버 역할 액티브 호스트에서 설치를 요청하는 어플리케이션 코드를 확인해 Verified APP Storage로부터 코드를 찾아 액티브 노드 정보를 참조해 코드의 캡슐화 ANEP 패킷을 구성하는 Code Capsule Manager 및 터널링을 통해 전송하는 Code Send Manager, Runaway Exception이나 Memory Hogging을 방지하기 위해 액티브 노드의 자원에 대한 사용 제한이 가능 하도록 코드의 안전성을 판단하여 등록 여부를 결정하는 Verify Manager로 구성되어 있다.

4.2 액티브 노드의 구성

액티브 노드[7]는 ANASP시스템과의 터널링 통신을 위해 ANASP Agent Manager의 추가가 필요하다. ANASP Agent는 ANASP시스템과의 정보교환 및 액티브 호스트의 코드 수정, 갱신, 삭제 등의 요청을 제어하는 Manager이다.



[그림 4] 액티브 노드 시스템 구성

5. 결론

기존의 패시브 네트워크가 가지는 새로운 요구에 대한 능동적인 수용 및 확장성 등에 대한 문제점을 해결하고자 DARPA에서 액티브 네트워크를 제안하였다. 하지만, 액티브 네트워크도 많은 보안상의 문제점들을 내포하고 있다. 그 중에서 액티브 노드에 설치되어 수행되는 액티브 코드들에 대한 안정성, 무결성 검증 및 액티브 노드 자체에 대한 인증성 문제 등을 해결하고자 본 논문에서는 ANASP 시스템을 제안하고자 한다.

이에 ANASP 시스템에 대한 전체적인 구성 및 세부적인 함수적 모듈들에 대해 설계하였고, 향후 이에 대한 구현 및 실험을 수행하고자 한다. 물론, 제안한 시스템이 액티브 네트워크에서 발생 가능한 모든 보안상의 문제점들을 해결할 수는 없을 것이다. 하지만, 액티브 노드에 대한 인증 문제와 액티브 패킷에 대한 무결성 및 안전성 검증을 선행적으로 처리한다면 추후 보다 폭 넓고 많은 보안문제들을 해결할 수 있을 것이라고 예상한다.

참고문헌

[1] 이중수, 이승헌, 이영희, “Active Network 구조 : 문제점 및 접근 방법”, 정보통신응용연구회 SIGCOMM REVIEW 2000.12

[2] D. Wetherall and U. Legedza and J. Guttag,"Introducing new internet services: Why and how",IEEE Network Magazine, 1998.

[3] D. Tennenhouse and D. Wetherall, "Towards an Active Network Architecture," Computer Communication Review 26(2), April 1996.

[4] D. Tennenhouse et al, "A Survey of Active Network Research," IEEE Communications Magazine, January 1997.

[5] R. H. Campbell, et al., "Seraphim: Dynamic Interoperable Security Architecture for Active Networks", IEEE OPENARCH 2000, Tel-Aviv, Israel, Mar 2000

[6] D. Decasper and Planttner, B., "DAN: Distributed Code Caching for Active Networks", INFOCOM'99, New York 1999

[7] A. B. Kulkarni, G. J. Minden, R. Hill, " Implementation of a Prototype Active Network", IEEE OPENARCH '98, 1998.