제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

액티브 네트워크 환경에서의 이동코드 보안서비스 제공에 관한 연구

한 인 성*, 김 진 묵*, 유 황 빈*
* 광운대학 컴퓨터과학과

요 약

인터넷 사용자들의 수가 빠르게 증가함에 따라, 사용자들이 요구하는 서비스의 종료도 다양해 졌다. 그러나 이러한 사용자들의 다양한 서비스의 요구를 수용하기위해 기존의 패시브 네트워크는 오랜 기간의 표준화가 이루어져야만 사용자의 요구를 수용할 수 있었다. 이러한 서비스 제공의 지연에 대한 문제점을 해결하기 위해 DARPA를 중심으로 라우터나 스위치가 프로그램 실행 능력을 갖고 있어 사용자 중심으로 네트워크를 구성할 수 있는 차세대 네트워크인 액티브 네트워크 구조가 제안되었다.

하지만, 액티브 네트워크 구조는 네트워크 노드에서 이동코드를 사용해, 사용자가 요구하는 서비스를 해결할 수 있는 반면, 기존의 패시브 네트워크보다 훨씬 더 복잡할 뿐만 아니라 보안상의 위협과 공격이 훨씬 쉽고 다양해지는 문제점을 갖게 되었다. 이를 해결하고자 많은 연구기관 및 과학자들이 노력을 기울여 왔다.

이에 본 논문에서는 액티브 네트워크 환경에서 사용자들의 편의성과 융통성을 제공하기 위해 사용되고 있는 이동코드에 대해 보안 서비스 제공을 위한 방안을 연구하였고, 이에 대한 제안으로 ANASP시스템을 소개하고자 한다.

Study of Mobile Code Security Service in Active Network Environment

Han In Sung*, Kim Jin Muk, Ryou Hwang Bin

ABSTRACT

As the number of internet users grows rapidly, the services which users required becomes various. However, for fulfilling these various user requirements, the existing passive network should be standardized for a long time. To resolve the delay on providing services, active network as a new technology was suggested. Its router or switch with DARPA as center has the program running ability, so user oriented network can be composed.

However, active network's architecture can resolve the user required service using mobile code on the network node, but it is more complex, easy-to-attack, various than the passive network. Many researchers have tried to resolve this problem.

So, this paper studied the mobile code security service in active network environment to provide user's convenience and accommodation, and introduced ANASP system as an alternative.

1. 서 론

인터넷이 전 세계적으로 보편화되면서 전자메일, 파일 전송, 원격 접속 등의 기본적인 서비스만을 제공하던 컴퓨터 네트워크는 전자 상거래, 전자 결제, 주문형 비디오(VOD:Video On Demand), 화상 회의 등의 복합적인 서비스를 제공하는 네트워크로 그 영역이 확장되고 있다. 이는 네트워크를 이용하는 사용자들의 요구가 더욱 다양해지고 복잡해짐에 따라 향상된 새로운 네트워크 기술과 서비스의 개발로 이어진 결과지만, 새로운 기술개발과 서비스의 보급은 여전히 네트워크 기반 구조의 표준화라는 테두리를 벗어나지 못하고 있다. 현실적으로 하부 기반 구조를 이루고 있는 네트워크 기술들과 프로토콜들이 표준화 단계를 거치고 실제 네트워크에 채택되어 응용되기까지는 많은 시간과 비용을 필요로 한다. 표준화는 다양한 개체들의 통신을 일관성 있게 지원하고 네트워크를 확장하기 위해서는 반드시 필요한 과정이지만, 표준으로 지정되지 못한 기술들과 표준화가 진행 중인 기술들은 사용할 수 없다는 것에 문제점이 있다. 따라서 사용자의 다양한 요구나 동적인 서비스의 지원은 표준을 근간으로 하고 있는 기존의 정적인 네트워크 구조에서는 거의 불가능하다[1].

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 적절한 연산, 처리를 할 수 있는 차세대 네트워크 구조에 대한 새로운 접근 방법이다. 중간 노드들이 패킷 내용에 대해 연산을 수행하고 수정할 수 있다는 점에서 이러한 네트워크를 'active'라 부른다. 이와 같은 절차들은 사용자마다 혹은 서비스 응용마다 각각의 특성화된 동작들을 수행할 수 있다. 동적인 네트워크 환경, 즉 중간 노드들에게 연산 기능을 부여하고 사용자가 프로그램 가능하도록 함으로써, 네트워크 내에 새로운 서비스를 보다 신속하고 경제적으로 도입해 자원들을 보다 적절하고 효율적으로 활용할 수 있게 한다[5]. 이처럼, 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[2][5].

그러나, 액티브 네트워크는 전송중인 액티브 패킷의 이동코드를 액티브 노드에서 실행할 수 있으며, 네트워크로 전송된 이동코드의 실행결과에 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[6].

본 논문에서는 악의적인 목적으로 액티브 노드의 취약성을 이용해 악의적인 이동코드가 설치되거나 전송중인 이동코드의 위·변조를 통해 네트워크 전체를 위협할 수 있는 보안상의 취약점을 해결하기 위한 ANASP시스템을 설계 및 구현하였다.

본 논문의 구성은 다음과 같다. 먼저, 2장에서는 액티브 네트워크의 개요와 보안구조에 대해 설명한다. 3장에서는 본 논문에서 제안한 액티브 네트워크에서 이동코드의 보안을 위해 제안한 ANASP시스템의 개요와 구조에 대해 살펴보고, ANASP시스템을 이용한 효과적인 액티브 네트워크 보호방법에 대해 설명한다. 4장에서는 본 논문에 대한 결과에 대해 설명하였다.

2. 액티브 네트워크의 개요

2.1 액티브 네트워크의 개요

액티브 네트워크는 네트워크의 노드들이 자신을

통과하는 패킷에 포함된 내용을 변경, 혹은 그 패킷의 정보를 이용하여 특정한 목적의 프로그램 실행이 가능한 네트워크이다. 전통적인 네트워크에서는 송·수신자간에 데이터를 전송하기 위해서, 각 노드들은 단순히 패킷의 헤더 정보를 검사하고 이웃 노드로 전송하는 처리만을 하였다. 이와는 달리 액티브 네트워크에서는 액티브 노드 사용자 중심의 특성화된 네트워크를 구성하게 된다. 액티브 노드(프로그램 가능한 라우터 혹은 프로그램 가능한 스위치) 사용자는 네트워크에 존재하는 여러 노드들 중 자신이 원하는 액티브 노드의 기능을 선택적으로 기능을 변경함으로서 자신만의 네트워크를 구성하게 된다. 이러한 액티브 네트워크에서는 기존의 노드들과도 상호 운영된다[4].

액티브 네트워크의 구성방식을 크게 세 가지 방식으로 구분해 볼 수 있는데, 액티브 네트워크에서 이동코드의 실행 방식에 따라 분리(discrete)방식과 캡슐(capsule)방식 그리고 혼합(integrity)방식으로 구분할 수 있다[7]. 분리(discrete)방식은 이동코드들이 이미 액티브 노드에 상주되어있는 경우다. 액티브 노드 사용자는 전송할 액티브 패킷에 기록된 이동코드 식별번호와 처리할 사용자 데이터를 포함시켜 액티브 네트워크로 전송한다. 패킷을 수신한 액티브 노드는 이동코드 식별자를 통해 식별번호를 확인하고 식별번호와 일치하는 이동코드를 액티브 노드에 적재한다. 이렇게 적재된 프로그램을 이용해 액티브 패킷의 사용자 데이터를 목적에 맞게 수행한다. 이러한 수행으로 변형된 데이터를 포함한 패킷은 이웃 노드로 포워딩 된다. 이러한 방식은 이미 이식되어 있는 이동코드에 대해서만 적용 가능하고, 오직 네트워크 관리자만이 이동코드를 추가 시킬 수 있어 일반 액티브 호스트들이 원하는 새로운 이동코드를 추가시키는 것이 불가능하다. 이 방식을 적용시킨 예로써 Active IP와 SwitchWare에 대한 연구가 있다.

이와는 다르게 캡슐(capsule)방식은 액티브 노드에 프로그램을 저장하지 않고, 각 액티브 노드 사용자가 이동코드와 사용자 데이터를 포함한 액티브 패킷을 네트워크로 전송한다. 액티브 패킷을 수신한 액티브 노드는 액티브 패킷으로부터 이동코드와 데이터를 분리해 이동코드를 액티브 노드의 실행환경(Execute Environment)에 로딩하고, 이를 이용해 사용자 데이터를 신속히 수행한 다음, 수행으로 변형된 데이터를 포함한 액티브 패킷을 액티브 노드의 스케줄에 따라 이웃 노드로 포워딩 된다. 이러한 방식은 전달해야 하는 이동코드의 양이 큰 경우 네트워크상에서 트래픽 문제, 패킷 분실의 경우 재전송 문제로 인한 효율성이 저하될 수 있다. MIT에서 수행중인 ANTS 프로젝트와 펜실베니아 대학의 PLANet이 이러한 방식을 적용하였다.

한편으로는 액티브 패킷 전달 과정에서 발생하는 지연이나 분실에 따른 비효율성을 제거하기 위하여 위의 두 가지 방식을 이용할 수 있다. 액티브 노드들이 공통적으로 사용하는 이동코드들은 미리 액티브 노드에 로딩해 놓고, 각 액티브 노드 사용자의 특정 이동코드는 액티브 패킷에 실어 전송하는 방법이다[3].

2.2 액티브 네트워크 보안구조

액티브 네트워크의 보안에 있어 이동코드 전송자의 인증과 무결성의 검증은 반드시 필요한 기본적인 보안요소이다. 전송하는 이동코드가 악의적인 목적을 갖거나 수행상의 문제발생의 소지가 있는 경우, 액티브 노드에서 이동코드가 실행되면 예기치 않은 실행 오류로 액티브 노드의 성능 저하뿐만 아니라 액티브 네트워크 전체로 악영향을 미칠 수도 있다. 또한, 이동코드의 인증이 이루어지지 않을 경우 악의적인 목적을 갖는 공격자로 인해 이동코드가 위·변조되어 네트워크에 악영향을 미치게 되는 잠재적인 위협요소로 발전할 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[8].

3. ANASP시스템 제안

3.1 ANASP시스템의 개요

ANASP(Active Network Application Sending Provider)시스템은 액티브 네트워크 환경에서의 기본 보안 구조인 액티브 노드의 인증과 액티브 노드에 설치되는 이동코드를 안전하게 전송문제를 해결하기위해 구현된 시스템이다. ANASP시스템은 액티브 노드의 인증 문제를 위해 우선적으로 신뢰할 수 있는 인증기관으로부터 인증서를 발급받는다. 인증기관으로부터 인증된 ANASP시스템은 관리 도메인에 설치되는 액티브 노드들에게 각각 액티브 노드의 공개키와 개인키 쌍을 발급함으로써 액티브 노드를 관리하는 ANASP시스템과 액티브 노드간의 상호 인증이 가능하다. 관리 도메인 내에 액티브 노드가 추가되는 경우, ANASP시스템 관리자는 액티브 노드의 아이피와 액티브 노드에 대한 리소스 정보 그리고 실행환경 정보를 ANASP시스템에 기록한다. ANASP시스템은 등록된 액티브 노드의 공개키 와 개인키 쌍을 생성하고, 액티브 노드로 ANASP시스템의 공개키와 액티브 노드의 공개키와 개인키 쌍을 전송한다.

본 논문에서 제안하는 ANASP시스템은 이동코드를 액티브 노드에 미리 설치한 후 설치된 이동코드를 이용하려는 이동코드 사용자의 데이터만을 처리하는 분리 방식의 구조를 이용해 보다 효율적인 보안을 위해 구현된 시스템이다. 기존의 분리방식에서의 문제점은 네트워크 관리자만이 이동코드를 설치할 수 있다는 단점이 있었지만, ANASP시스템의 적용으로 이동코드의 설치를 필요로 하는 이동코드 사용자들의 인증과 설치요구로 액티브 노드의 활용성을 높일 수 있다. 또한 액티브 노드의 관리를 통해 ANASP시스템에 등록되어있는 액티브 노드로 암호화 및 인증을 통해 이동코드를 전송하므로 이동코드의 위·변조의 위험성을 막을 수 있다.

ANASP시스템에서 관리되고 있는 액티브노드와 상호간에 신뢰관계가 성립되면, ANASP시스템은 각각의 액티브 노드들로 암호화된 이동코드에 인증코드 붙여 전송한다. 전송하는 패킷의 암호화 및 인증은 악의적인 사용자의 패킷도청으로부터 보호되고 무결성이 보장된 이동코드를 액티브 노드로 전송이 가능하도록 설계되었다.

3.2 ANASP시스템의 설계

ANASP시스템을 구성하는 모듈 관리자는 크게 ANASP Controller, AN Key Manager, Regist Manager, Data Generate Manager, Data Sending Manager로 구성할 수 있다. 그림 1은 ANASP 시스템의 구조를 나타내고 있다.

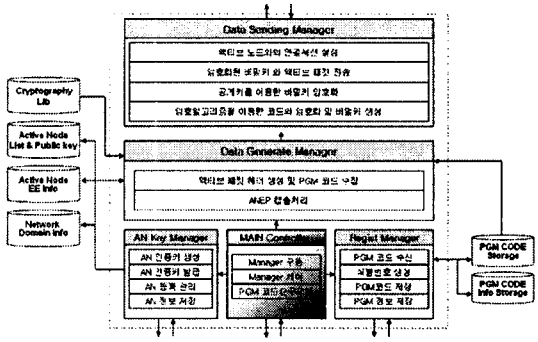

그림 1. ANASP시스템 구성

ANASP시스템은 액티브 노드들을 등록하고 AN Key Manager로 공개키와 개인키 쌍을 생성해 액티브 노드로 전송한다. 이동코드 제공자들은 이동코드를 ANASP시스템으로 전송하면 Regist Manager가 이동코드를 수신해 저장 및 관리를 담당하게 된다. 저장된 이동코드는 프로그램 설치 요구자의 요청으로 Data Generate

Manager를 통해 이동코드를 액티브 패킷으로 캡슐화 하고 이동코드가 캡슐화된 액티브 패킷은 Data Sending Manager로 보내진다. Data Sending Manager는 액티브 노드와의 Session을 설정하고 액티브 패킷암호화 해 액티브 노드로 안전하게 전송을 담당한다.

ANASP시스템을 구성하는 모듈 중 액티브노드로 액티브 패킷의 암호화된 통신을 관리하는 Data Sending Manager는 세션 공개키와 개인키 쌍을 이용해 세션연결을 관리하므로 전송되는 액티브 패킷의 암호화 및 인증을 처리할 수 있는 ANASP시스템의 핵심 모듈이다. 그림 2는 ANASP시스템의 Data Sending Manager의 동작과정을 보여주고 있다.

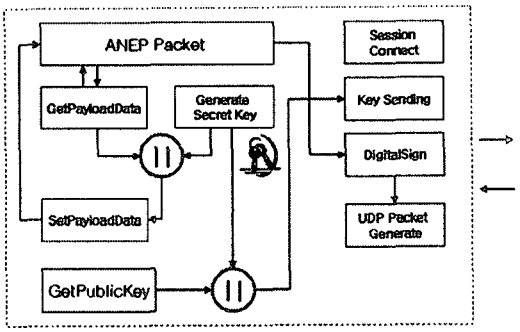

그림 2.Data Sending Manager 동작과정

암호화 및 전자 서명에 앞서 Data Sending Manager는 액티브 노드는 안전한 전송을 위해 상호간의 신뢰관계를 설정한다. 이러한 관계는 Session연결을 함으로써 ANASP 시스템과 액티브 노드간의 안전한 연결설정을 이룰 수 있다.

3.3 ANASP시스템의 설계

액티브 노드의 ANASP 에이전트 관리자는 ANASP시스템과의 액티브 노드간의 암호화된 통신을 위한 기능을 수행 한다. ANASP 에이전트 관리자를 이용해 ANASP시스템은 액티브 노드의 상태 확인 및 액티브 노드의 정보를 확인할 수 있다. 또한 ANASP시스템으로 부터 전송되는 암호화된 이동코드를 수신하기 위해 키 교환기능을 수행하며 키 교환의 완료 후 암호화된 이동코드 패킷을 저장하며 개인키를 이용해 액티브 패킷을 복호화 하는 중요한 기능을 한다. 앞서 설명한 Data Sending Manager에서 진행한 Session 설정을 위한 과정을 에이전트 관리자에서 관리하고, 수신된 액티브 패킷으로부터 ANEP 헤더정보를 확인한다. ANEP 페이로드로부터 암호화된 이동코드를 추출해 Data Sending Manager에서 보내온 비밀 키를 이용해 이동코드를 복호화 한다. 이동코드는 액티브 노드의 NodeManager로 보내어져 정상적으로 액티브 노드에서 실행될 수 있다.

4. 결 론

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] Bob Lindell, draft-nodeos-security-00.txt, Hop-by-hop Message Authentication and Integrity"

[2] Danny Raz and Yuval Shavitt, "An Active Network Approach to Efficient Network M anagement", IWAN'99, 1999.

[3] D.S. Alexander, et al., "The SwitchWare A ctive Network Architecture", IEEE Networ k Specail Issue on Active and Controllable Networks, vol. 12 no.3, 1998.

[4] D. Tennenhouse and D. Wetherall, "Towar ds an Active Network Architecture," Comp uter Communication Review 26(2), April 1 996.

[5] D. Tennenhouse et al, "A Survey of Activ e Network Research," IEEE Communicatio ns Magazine, January 1997.

[6] Konstantinos Psounis, "Active Networks: A pplications, Security, Safety and Architectu res",IEEE Communications Surveys, First Quarter 1999.

[7] AN Node OS Workinh Group, "Architectur al Framework for Active Networks", Jul. 1 999.

[8] 박정민, 채기준, "Active Network의 보안 기술 발전전망" 정보통신응용연구회 SIGCOM M REVIEW 2000.12

[9] 이중수, 이승헌, 이명희, "Arctive Network 구조: 문제점 및 접근 방법", Sigcomm Revi ew 1(1), Dec. 2000.

한 인 성

2001년 배재대학교 컴퓨터 공학 (공학사)

2001년 ~ 현 재 광운대학교 컴퓨터과학과 석사과정

김 진 묵

1998년 배재대학교 컴퓨터공학 (공학사)

2000년 배재대학교 컴퓨터공학 (공학석사)

2000년 ~ 현재 광운대학교 컴퓨터과학과 박사과정

유 황 빈

1975년 인하대학교 전자공학과 (공학사)

1977년 연세대학교 전자공학과 (공학석사)

1989년 경희대학교 정보통신과 (공학박사)

1981년 ~ 현재 광운대학교 컴퓨터과학과 교수