초고속국가망 인터넷의 보안 취약성 개선 방안

신주현*, 백선경*, 윤미진*, 김성석*, 김판구**
* 조선대학교 전자계산학과
** 조선대학교 컴퓨터공학과
e-mail:jhshinkr@unitel.co.kr

Advanced security system structure for network security in Korea Information Infrastructure

Ju-Hyun Shin*, Sun-Kyung Back*, Mi-Jin Yoon*
Sung-Suk Kim*, Pan-Koo Kim**
*Dept of Computer Science, Chosun University
**Dept of Computer Engineering, Chosun University

요 약

초고속국가망은 지식정보사회에 대비하여 국가가 공공기관을 중심으로 데이터서비스와 인터넷서비스를 제공하고 있는 비영리 정보통신 망이다. 이에 따라 공공기관이 다양한 형태의 정보를 자유롭게 이용할 수 있는 기반을 제공해야 한다. 따라서 최근 침해유형이 웜·트로이목마 등의 악성프로그램에 의한 DDoS 공격이나 대량의 패킷생성으로 네트워크 과부하를 일으키는 등의 네트워크 공격이 많아지면서 인터넷 사용자에 대한 보안의 필요성이 강조된다. 본 논문에서는 초고속국가망 인터넷 서비스에 대한 네트워크의 주요 구성요소를 진단해 보고 최근 침해 유형에 대한 보안의 취약성을 분석한 후 이를 해결할 수 있는 방안으로 네트워크 구조와 보안시스템의 효율적 개선안을 제시한다.

1. 서론

초고속국가망은 정부가 세계 최고의 정보통신대국을 만든다는 전략으로 국가, 지방자치단체, 학교 및 연구기관 등 공공기관을 중심으로 고속의 통신서비스를 제공하는 국가적인 통신망이다. 이러한 초고속국가망은 공공기관이 다양한 형태의 정보를 자유롭게 이용할 수 있는 기반을 제공함으로서 업무의 효율성이 향상되며, 공공이관이 정보통신 시설을 선도적으로 이용하게 되어 민간부문에 대한 수요를 창출할 수 있다. 초고속국가망에서 인터넷 사용량은 점차 증가하고 있고 최근 정보화에 역행하는 공격유형이 네트워크를 마비시키는 형태로 변화되고 있는 추세여서 네트워크 보안강화를 위한 많은 연구가 이루어져야 한다.

본 논문에서는 초고속국가망 가용성을 최대로 하기위해 사업자 네트워크 구조와 보안시스템 기능을 분석한 다음 최근 침해 유형에 대한 보안의 취약성을 분석한 후 이를 해결할 수 있는 방안으로 네트워크 구조와 보안시스템의 효율적 개선안을 제시한다. 제2장에서는 초고속국가망 인터넷 서비스의 네트워크 구조와 보안 시스템의 기능을 분석하고, 제3장에서는 최근침해유형에 대한 네트워크 보안의 문제점을 진단하고, 제4장에서는 초고속국가망 인터넷 보안 취약성에 대한 개선방안을 제시한다. 제5장에서는 결론으로서 초고속정보통신망의 가용성을 높일 수 있는 향후 방안으로 국가적 차원의 제도화된 정보보호 방침과 가입자 정보를 보호하기 위한 사용자의 보안의식수준의 필요성을 제시한다.

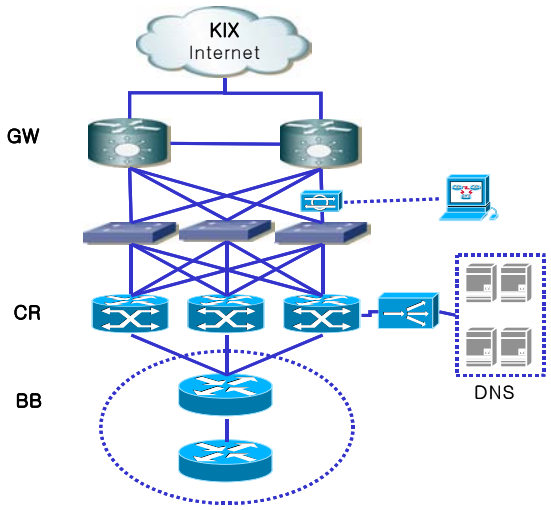
2. 초고속국가망 네트워크 보안 구조 분석

인터넷 서비스는 네트워크를 이루고 있는 주요 구성요소와 네트워크를 운영하는 정책에 의해 관리

되며 제공되어진다. 네트워크 주요 구성요소는 네트워크 구조, 네트워크 장비, 보안시스템 그리고 대응체계 등이 있다. 이들 구성요소중 하나라도 문제가 생긴다면 네트워크는 그 기능을 제대로 발휘할 수 없으며 작게는 특정 서비스만 정지 되지만 더 나아가 네트워크 마비까지 발생할 수 있다. 따라서 초고속국가망 보안현황을 진단해 보기 위해서는 핵심적 역할을 하는 네트워크 현황을 파악하고 보안시스템에 대한 기능 분석이 우선시 되어야 한다. [그림 1]은 사업자 네트워크를 계위별로 구분하고 각 계층의 네트워크 구성요소와 보안시스템에 대한 구조를 나타내고 있다. [그림 1]의 사업자 네트워크는 전체를 나타내는 것이 아니며, 일부 주요 기능만을 축약하여 나타내었다.

2.1 네트워크 구조 분석

계위별 네트워크 구성은 중요 라우터 4개가 연결된 4계위구조를 취하고 있으며, 이들 라우터는 스위치를 통해 인접 라우터 모두로 연결이 되어 있다. 이는 네트워크의 가용성을 위한 측면으로 어느 단에 문제가 발생하여도 서비스가 이루어지게 하려는 사업자적 네트워크 안정화 방안이다. 같은 관점으로 DNS 앞단에 L4를 설치하여 각 DNS로 집중될 수 있는 트래픽을 효율적으로 분산시키고 있다. 이렇게 가용성을 위한 네트워크는 어느 정도 잘 구성되어 있다는 것을 알 수 있으나, 보안측면으로는 IDS가 탐지하는 구간이 게이트웨이 라우터와 기가 스위치 하나에서 미러링을 통해 트래픽 캡쳐후 유해트래픽을 탐지하고 있다. 트래픽이 흐르는 길은 많은데도 하나의 길목만 막는 것은 아직 보안이 완전하게 해결되지 못함을 보여준다.



[그림 1] 사업자의 계위별 네트워크 구조

이와 같이 사업자 네트워크 구조가 가용성이 뒷받침되는 네트워크를 어느 정도 보장하고 있는 상황에서 그 위에 요구되어 지는 것은 신뢰적 네트워크 구성을 위한 보안성이다. 초고속국가망 인터넷을 보호하기 위해 사용 중인 보안시스템은 침입탐지 시스템(IDS)과 침입차단시스템(FW), L7 스위치, 라우터로 구성된다.

2.2 보안 시스템 기능 분석

네트워크상에서 일어나는 유해한 행위들은 네트워크 전용 보안시스템을 통해 탐지 및 차단할 수 있다. 이러한 보안시스템들은 어느 위치에 놓이느냐에 따라 각 역할과 비중이 달라지며, 그 위치에서 최적의 보안설정을 통해 각 보안시스템은 유해 공격에 대응할 수 있게 된다.

1) 침입 탐지 시스템(IDS)

초고속국가망에서 IDS는 트래픽이 흐르는 기가 스위치나 기가 라우터등의 게이트웨이에 위치하여 허가받지 않은 접근이나 해킹 시도를 감지하여 네트워크 관리자에게 통보해 주고, 필요한 대응을 취하게 해주는 보안 시스템이다. 새로운 유해 패턴에 대해서는 모니터링을 통해 이상 징후임을 감지하고 관리자에게 통보한다.

2) 침입 차단 시스템

초고속국가망에서 운영중인 침입차단시스템으로는 방화벽(FW)과 라우터가 있다. 침입차단이라는 측면에서는 두 장비의 기능은 거의 비슷하나, FW은 게이트웨이와 코어 라우터 사이에 위치하여 주로 인증되지 않은 침입에 대한 보호기능을 통한 차단을 수행한다. 반면에 라우터는 사업자 네트워크 종단 부분에 위치하여 라우팅 기능을 주로 수행하고 문제가 발생한 경우에 대해 ACL(Access Control List)를 통해 차단 기능이 구현되고 있다.

3. 초고속국가망 인터넷의 보안 취약성 분석

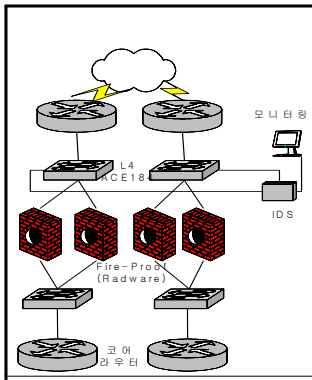
제2장에서 초고속국가망 인터넷 서비스를 위한 보안 시스템 및 네트워크 구조에 대한 분석을 통해 인터넷 웜과 같은 새로운 침해유형에 대한 네트워크 구조의 취약성과 보안시스템상의 유해트래픽 탐지 및 차단 방법의 취약성을 분석하고자한다

3.1 초고속국가망 사업자 네트워크 구조의 취약성

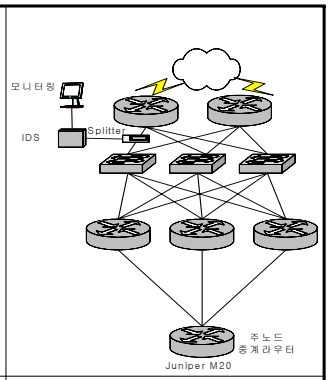
초고속국가망상의 취약성을 조사한 결과 서버팜의 집중화 현상으로 네트워크에 대한 감염 및 확산의 우려가 있고, 다중화 구조로 유해트래픽 탐지가 힘든 네트워크 구조를 취하고 있어서 네트워크 공격에 대한 취약성을 드러내고 있다. 다음에서 유해트래픽 탐지가 힘든 두가지 구조에 대한 취약성을 분석해 보고자 한다.

1) 다수 라우팅 경로상에서 유해트래픽 탐지

초고속국가망에서 사업자 네트워크의 다수 라우팅 구조는 백본 이중화 구조와 Full Mesh 구조를 취하고 있다.



[그림 2] 이중화 구조



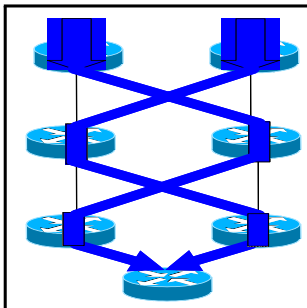
[그림 3] Full Mesh 구조

[그림 2]의 경우 1계층에서 2개의 라우터가 게이트웨이로 이용되며, 2계층에서 백본 스위치 2대, 3계층에서 백본라우터 2대가 있다. 또 4계층에 중계라우터가 2대 있고 마지막으로 가입자 수용 라우터 1대로 연결되는 네트워크 구조이다. 이때 외부에서 유입된 트래픽이 게이트웨이 라우터를 거쳐 가입자 수용라우터로 이어지기까지 경로는 2^4x1 이 된다. [그림 3]의 경우도 각 계층에서 다음 계층으로 연결되는 네트워크 장비를 모두 연결하는 구조다. 이처럼 라우팅 경로의 수가 많아질 수 록 네트워크 장비의 장애에 대한 네트워크 가용성을 보장하지만 구조에 맞는 보안시스템이 구축되었을 때 충분한 가용성을 보장할 수 있다.

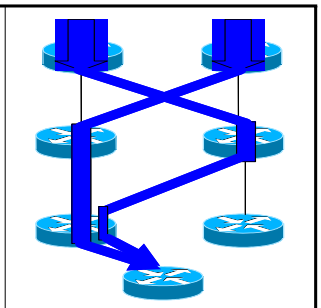
2) 비대칭 네트워크 상에서 유해트래픽 탐지

[그림 4] [그림 5]와 같이 전달되는 트래픽이 네트워크 상태에 따라 다수 경로로 전달될 수 있는 네트워크를 비대칭 네트워크라고 한다.

예를 들어 A층 라우터에서 B층 라우터로 정보가 전달되는 경우 트래픽이 전달되는 경우의 수는 A1라우터에서 B1라우터로 전달되는 경우와 A1라우터에서 B2라우터로 전달되는 경우로 나누어진다. A1라우터와 B1라우터 사이, A1라우터와 B2라우터 사이에 침입탐지시스템이 설치되어 있다고 하면 하나의 공격이 시도되어 A1라우터를 통해 B층으로 전달될 때 문제가 된다. 만일 트래픽이 분산되어 B1라우터로만 지나가거나 B2라우터 한곳으로만 가지 않고 B1라우터와 B2라우터 모두를 통해 나누어 전달된다면 침입탐지시스템은 침입을 탐지할 수 없게 된다.



[그림 4] 비대칭 성질의 트래픽1



[그림 5] 비대칭 성질의 트래픽2

3.2 네트워크 보안시스템의 취약성

1) 침입탐지 시스템(IDS)의 취약성

초고속국가망에서 IDS가 갖는 취약성은 첫 번째, 유해트래픽 정보를 가지는 DB에 의해 패턴 매칭을 통해 탐지를 하기 때문에 발견되지 않은 새로운 침입기법에 대응이 어렵다. 두 번째, IDS가 유해트래픽으로 판정하기 까지 경과된 시간 안에 이미 공격은 진행되어 예방차원의 보안이 안된다. 세 번째, 정상적인 트래픽으로 위장 가능한 DDoS공격에 대한 경우 차단이 안 되는 취약성을 갖고 있다.

2) 침입차단 시스템(FW)의 취약성

FW의 취약성으로 첫 번째, 정책 DB에서 설정해 놓은 접근 허용 규칙에 따라 유해트래픽을 차단하므로, FW을 우회하여 공격의 경우 유해트래픽 차단이 불가능하다. 두 번째, 자체 성능의 부족으로 인한 다운 현상이 발생할 수 있고, 세 번째로 정상적인 트래픽으로 위장한 DDoS공격에 무방비한 취약성을 지닌다.

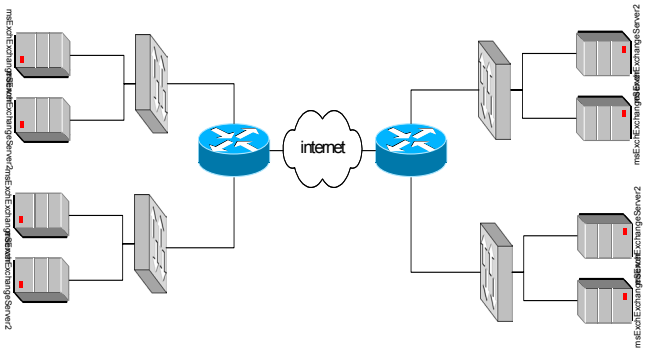
4. 초고속국가망 인터넷의 보안 취약성 개선 방안

4.1 인터넷서비스 네트워크 구조의 개선

서버의 부하를 분산시키기 위해서 서버 앞단에 로드밸런싱 장비를 설치·운영하는 것이 좋다. 그러나 L4 스위치가 다운되거나 L4 스위치로 패킷을 라

우팅하는 라우터에 장애가 발생한 경우 해당 서비스는 중지될 수 있다. 즉, 만일 서버가 서비스를 제공할 수 없는 경우를 고려하여 서버는 분산된 위치에 설치되어야 한다. 이는 해당 서버로 집중되는 트래픽을 분산시키는 효과도 얻을 수 있다.

[그림 6] 는 유해트래픽에 영향을 덜 받을 수 있는 주요 서버의 위치를 바꾸어 네트워크 구조를 변화시켰으며 각각의 서버 앞단에 보안시스템을 설치한 구조다.



[그림 6] 분산지역 서버팜 구조

4.2 보안시스템의 다중화 구성으로 유해트래픽 탐지 효율 향상

백본이 이중화되어 있다거나 Full Mesh 형태로 구성되어 있는 경우 보안시스템이 설치되어야하는 구간이 증가하게 되므로 유해트래픽을 효율적으로 탐지하고 차단하기 위해서는 보안시스템을 다중화하여 설치하면 해결할 수 있다. 즉, 다수의 경로를 모두 감시 할 수 있는 보안시스템을 설치하는 것이다. 우선 백본을 이중화로 구성한 경우 트래픽이 지나는 경로가 2곳밖에 없기 때문에 보안시스템 역시 설치대수가 많지 않고 운영하기가 편하다. 반면 Full Mesh로 구성한 경우는 보안시스템 설치 대수가 많고 운영하기가 힘들다.

[그림 2]의 경우 백본이 이중화되어 있는 경우 게이트웨이와 백본스위치 연결구간 또는 백본 스위치와 백본 라우터 연결구간에 보안시스템을 설치할 수 있다. 예를 들면, 게이트웨이 라우터1과 게이트웨이 라우터2로부터 백본 스위치1로 전달되는 경우수가 2가지이고, 백본스위치1로부터 백본라우터1과 백본라우터2로 전달되는 경우수가 2가지이다. 경로가 한정되어있기 때문에 유해트래픽을 탐지 또는 차단하기 위해서 백본스위치1으로부터 백본라우터로 전달되는 2가지 경로에 보안시스템을 설치하여야 하며 백본스위치2로부터 백본라우터로 전달되는 경우까지 포함하여 그 수는 총 4대가 된다. 이때 고려해야 할 점은 백본스위치 하나로부터 두 경로를 통해 트래픽이 분산되어 전송될 가능성을 고려하여야 한다.

5. 결론 및 향후 연구 과제

본 논문에서는 초고속국가망 인터넷 보안 취약성 개선을 위한 사업자 네트워크의 구조와 보안시스템의 효율적 방안에 대해 연구했다. 가용성 향상을 위한 방법으로는 네트워크 구조의 개선과 보안시스템의 기능이 보강되어야 함을 알 수 있었다.

향후 연구로는 초고속국가망 가입자는 계속 증가하고, 네트워크 공격 형태는 더욱 지능적으로 발전해 가고 있기 때문에 인터넷망의 효율적인 관리를 위한 트래픽 분석 시스템과 변화되는 인터넷서비스 기술인 VPN, MPLS 기반의 보안기술에 관한 연구를 수행할 계획이다.

참고문헌

[1] "초고속국가망의 가입자망 유형별 정보보호 대응방안“,정보화정책, 2003

[2] “초고속국가망 보안 취약점 분석 및 대응 방안 연구“, 전산원, 2000. 12

[3] “초고속국가망 보안대책 수입을 위한 국내외 동향 조사 및 연구”, 한국전산원, 1998

[4] “인터넷 트래픽 측정 및 분석 기술동향”, 한국전산원, 2002

[5] 황성원, “미국의 정보통신기반보호정책 동향”, 한국정보보호진흥원, 2002

[6] 조진현, “미국의 사이버보안정책 동향”, 한국정보보호진흥원, 2002,11

[7] 이희조, “인터넷 기반구조의 취약성분석과 보안강화방안”, Review, 2003.4

[8] “인터넷 방화벽과 네트워크 보안”, 이한출판사, 2002

[9] J. Howard, "An Analysis of Security Incidents on the Internet," Ph.D. Thesis Carnegie Mellon University, 1998.

[10] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," RFC 2267, January 1998.

[11] David Marchette, “A Statistical Method for Profiling Network Traffic,” in Proceedings of the Workshop on Intrusion Detection and Network Monitoring, Santa Clara, California, USA, Apri

[12] L. Garber. “Denial of Service attacks rip the Internet”. IEEE Computer , Apr. 2000.