고신뢰 네트워크 구성을 위한 보안 요구사항 및 기술 분석

김도현*, 봉진숙*, 신용태*
*숭실대학교 컴퓨터학과
{dohyunkim, jsbong}@icn.ssu.ac.kr, shin@ssu.ac.kr

Security requirements and technical analysis for highly Trusted Network configuration

Dohyun Kim*, Jinsook Bong*, Yongtae Shin*
*Dept of Computing, Soongsil University

요 약

기존 IP기반의 공용망에서는 폐쇄망의 구조로 사용되고 있다. 이런 구조는 구조상의 문제와 보안상의 문제를 가지고 있다. 본 논문에서는 현재 IP기반의 공용망에서 발생할 수 있는 여러 보안 문제를 해결하기 위해 현제 네트워크 구조의 문제와 보안상의 문제를 제시하고 고신뢰 네트워크 시스템의 필요성을 제안한다. 제안하는 고신뢰 네트워크에 기능 요구사항과 보안 요구사항에 대하여 분석하고 보안 요구사항별 고신뢰 네트워크 핵심기술을 도출한다.

1. 서론

현재 정부 및 공공기관들은 부처별 고유 업무의 안정적 수행을 위해 주로 폐쇄망으로 운영되고 있다.

그러나 최근 개방·공유·소통·협력을 기반으로 대민행정 정보, 정부의 공공정보 등을 활용한 다양한 서비스들의 제공이 증가되고 있다.

이에 정부 및 공공기관을 중심으로 부처별 고유 업무의 안정적 수행을 위한 견고한 네트워크 환경 제공은 물론, 서비스 융합 트렌드에 따른 스마트워크 요구를 수용하고 부처 간에 인프라와 정보를 안전하고 효율적으로 공유하기 위하여 고신뢰 네트워크 구조 및 보안기술의 필요성이 증대되고 있다.

또한 IP 네트워크 기반의 공용망에서는 IP주소의 변조가 용이 할 뿐 아니라 IP주소를 알면 해당 시스템에 쉽게 접근할 수 있어 다양한 보안문제가 발생할 수 있다.

서론에 이어 2장에서는 현재 네트워크 보안 취약점과 이를 보완하기위한 고신뢰 네트워크 시스템에 대해 살펴보고, 3장에서는 고신뢰 네트워크 시스템 요구사항 및 보안 기술 분석을 분석한다. 마지막으로 4장에서는 결론 및 향후과제를 제시한다.

2. 관련연구

2.1 기존네트워크 보안 취약점

기존네트워크 보안 위협의 근본적인 문제는 네트워크의 구조적 완전성에 기인하고 있다. 네트워크 아키텍처, 주소체계, 라우팅 프로토콜 등 네트워크를 구성하는 핵심 기반 기술들은 근본적으로 보안에 취약하다. 그러므로 네트워크는 새로운 보안 위협이 발생할 때마다 시그니처 및 소프트웨어 패치 등을 기존의 탐지, 방어 시스템에 추가하는 방식으로 네트워크 보안 위협을 해결해왔다. 그러나 이러한 방법은 일시적일 뿐 보안 위협에 대한 근본적인 해결방안이 될 수 없다.

이러한 문제로 인해 IP 보안 취약점, BGP 취약점, 네트워크 장비 보안 취약점 등이 발생할 수 있다.

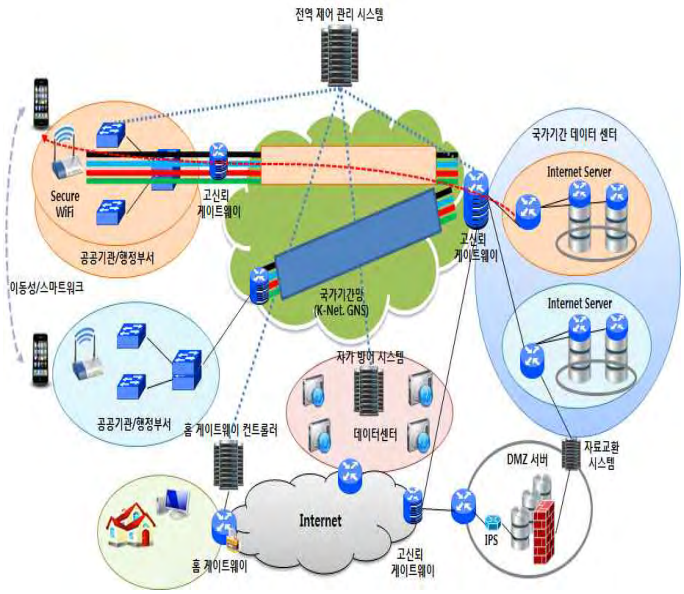
2.2 고신뢰 네트워크 시스템 개요

고신뢰 네트워크란 기밀성, 가용성, 품질, 이동성 등의 관점에서 비신뢰적인 통신망을 통해 단말, 서버 및 네트워크 기기 간에 신뢰적인 통신을 가능하게 하는 네트워크이며,(그림 1)과 같은 고신뢰 네트워크의 구조를 나타낸다.

고신뢰 네트워크는 HW, SW, 데이터 등 각종 정보자원을 국가기간 데이터센터로 통합하고 다양한 통신매체를 통해 접근하는 사용자에게 적절한 서비스를 제공할 수 있다.

또한 폐쇄망으로 운영되었던 국가 및 공공기관의 전용 네트워크를 (그림 1)과 같이 물리적으로 통합하고 안전한 터널 및 터널 스위칭을 사용하여 논리적으로 분할함으로써 안전하고 효율적으로 망을 운영할 수 있다.

"본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음"
(IITP-2015-H8501-15-1008)



(그림 1) 고신뢰 네트워크 구조

또한 폐쇄망으로 운영되었던 국가 및 공공기관의 전용 네트워크를 (그림 1)과 같이 물리적으로 통합하고 안전한 터널 및 터널 스위칭을 사용하여 논리적으로 분할함으로써 안전하고 효율적으로 망을 운영할 수 있다.

고신뢰 네트워크는 다음과 같은 시스템 구성요소를 가진다.

(1) 홈 게이트웨이

외부 인터넷망과 가정 내 다양한 전자기기들 간 정보교류를 중계하는 관문 역할을 하는 장치이다. SDN 기반의 동적인 보안정책을 분배하며 탐지, 예방, 차단, 모니터링 기능을 지원해야 한다.

(2) 고신뢰 게이트웨이

동적 네트워크 은닉 구조 기반의 실시간 연결성 및 비밀성 보장에 필요한 비화 라우팅과 실시간 사이트 인증을 제공할 수 있는 게이트웨이 장치이다. 이 장비는 망은닉(주소은닉), 스크램블드 포워딩, 매니지드 터널링과 같은 기능을 지원해야 한다.

(3) Secure WiFi

무선 환경에서는 비인가 불법 AP설치, 외부 AP를 통한 자료 유출, Ad-hoc을 통한 자료 유출, 외부 사용자의 내부 침입, DDoS 공격 등의 보안위협이 발생하기 쉬우므로 Protected AP, VPN 게이트웨이, WiFi 관리 기능 등을 지원해야 한다.

(4) 전역제어관리 시스템

네트워크 접속을 위한 단말/사용자 인증과 네트워크에 대한 동적 정책설정을 통한 지능적 제어관리 기능을 하는 시스템이다. 본 시스템은 네트워크 와 게이트웨이에 대한 관제 및 네트워크 기기 인증 제어를 수행한다.

이 기능은 보안등급, QoS, 서비스를 인지하여 네트워크 구성 및 서비스제어를 위해 동적이고 전역적인 다중인증 기술을 지원해야 한다.

(5) 자가방어 시스템

트래픽을 증가시키는 다양한 DDoS 공격이나 정형화 되지 않은 APT 공격에 대해 능동적으로 빠르게 대응할 수 있는 SDN 기반 지능형 보안 시스템이다.

이를 위해 SDN 기반 NFV 컨트롤러와 VTN 별 보안 서비스 체이닝 자원 관리가 가능한 오케스트레이션 기술, 보안/트래픽 강도에 따라 필요한 자원만을 사용하여 공격에 대비하는 동적 서비스 체이닝 알고리즘 활용기술이 필요하다.

3. 고신뢰 네트워크 시스템 요구사항 및 보안 기술 분석

고신뢰 네트워크 시스템은 비신뢰적인 통신망을 통해 단말, 서버 및 네트워크 기기 간에 기밀성, 무결성, 가용성을 보장하기 위하여 다음과 같은 기능 및 요구사항들을 만족하도록 설계되어야 한다.

<표 1> 기능 요구사항

기능	요구사항
접근제어 기반의 Seamless한 데이터 공유 기능	- 사용자 인증과 서비스 인증 및 네트워크 제어를 한 번의 다중 인증
통신 미디어에 독립적인 통신 기능	- 통신 미디어에 관계없이 안전한 데이터 통신 지원
다단계 관리 감독 기능	- 다단계 관리 감독 기능 지원 요구
망 통합 기능	- 종단 간 안전한 터널 및 터널 스위칭 기반의 논리적 망 분리가 적용된 업무망으로의 통합 요구
확장성	- 증가되는 데이터 및 서비스를 수용하기 위해 네트워크 시스템의 확장성 요구
Backward compatibility 기능	- Backward compatibility를 갖는 네트워크를 구성
데이터 및 정보 표준화 기능	- 데이터 관리의 편의성을 위해 데이터 및 정보 표준화 기능 요구

추가적인 기능 요구사항으로 접근제어 기반의 Seamless한 데이터 공유 기능은 네트워크 구성 및 서비스를 동적, 전역적으로 제어하는 기술이 필요하고, 빠른 이동중에도 데이터를 주고 받는데 이상이 없도록 빠른 알고리즘 활용기술이 필요하다. 또한 Backward compatibility 기능은 상용기술과 장비를 활용하여 기존장비에 신규 기능을 추가하는 기술이 필요하다.

<표 2> 보안 요구사항

보안기능	요구사항
무결성	- 전송된 데이터가 송신 중 변경되지 않음을 보장
APT 및 DDoS 완화 기능	- APT, DDoS 공격에 능동적 대응
보호-탐지-대응의 심층 방어 기능	- 기존보안 시스템들이 서로 협력하여 보호-탐지-대응으로 이루어지는 심층적인 방어 요구
주소 은닉 기능	- 서버의 IP 주소가 노출되지 않도록 서버 및 네트워크 장비의 주소 은닉 요구
동적 다중경로 데이터 전송 기능	- 데이터가 추적되는 것을 방지하기 위해 동적 다중경로 데이터 전송 요구
다중 인증 기능	- 종합적, 지능적인 보안 관리를 위해 다중인증 사용
다단계 암호화 및 접근제어 기능	- 높은 접근 권한을 가진 사용자만이 접근할 수 있도록 다단계 암호화 및 접근제어 기술 요구

추가적인 보안 요구사항으로 APT 및 DDoS 완화 기능은 SDN기반의 지능형 보안 시스템 필요하며, 보호-탐지-대응의 심층 방어기능은 공격 발생 이후의 전 과정에 대한 보호가 필요하다. 다중 인증 기능은 보안 등급, QoS, 서비스를 인지하여 동적, 전역적으로 제어할 수 있도록 하는 제어 기술이 필요하다. 또한 다단계 암호화 및 접근제어 기능은 중요한 정보일수록 높은 암호화 수준으로 암호화하는 것이 필요하다.

앞서 도출된 고신뢰 네트워크의 보안 요구사항을 중심으로 현재 IP 네트워크에서 사용 중인 보안 기술의 한계점과 고신뢰 네트워크의 핵심기술을 도출된 결과는 <표 3>과 같다.

<표 3> 보안 요구사항별 고신뢰 네트워크 핵심 기술 도출

요구사항	기존 보안 기술의 한계	고신뢰 네트워크 핵심 기술
무결성	VPN 기술은 이동성 및 확장성에 한계가 존재	Safe VPN, Managed Tunneling
APT 및 DDoS 완화 기능	고도화되는 APT 및 DDoS공격에 대한 선제적 대응 한계	지능형 네트워크, Advanced Anti DDoS, 망은닉(HAIPE, TOR)
주소 은닉 기능	VPN이나 NAT는 장비의 주소가 외부로 노출	망은닉(HAIPE, TOR)
다중 인증 기능	종래의 NAC는 서비스에 대한 접근 통제 불가능	IAM
보호-탐지-대응의 심층 방어 (Defense-indepth) 기능	종단의 보안을 주목적으로 하는 UTM만으로는 전역적 보안 제공 불가능	UTM + 전역적 제어 관리 시스템, 지능형네트워크
다단계 암호화 및 접근제어 기능	VPN, NAC 기술만으로는 사용자 및 서비스 특성에 따른 단계적 암호화 및 권한별 접근제어 불가능	IAM, Managed Tunneling
동적 다중경로 데이터 전송 기능	데이터 경로의 추적을 방지하기 위한 보안 기술의 부재	스크램블드 포워딩

4. 결론 및 향후과제

본 논문에서는 현재 IP기반의 공용망에서 발생할 수 있는 보안 문제점에 대해서 제시하였다.

현재 네트워크 환경의 문제점으로 인해 최근 대두되고 있는 고신뢰 네트워크 기술에 대하여 기능 요구사항과 보안 요구사항을 분석하여 핵심 기술을 도출하였다.

추가적으로 고신뢰 네트워크 기술은 기능과 보안 측면에서 여러 요구사항이 필요하기 때문에 고신뢰 네트워크 시스템이 안정적으로 도입되기 위해서 기능과 보안 측면에 초점을 맞춘 연구가 필요하다.

참고문헌

[1] 장정숙, 김은주, 전용희, “고신뢰 네트워크 운영을 위한 정보 보안 모델링“, 한국정보기술 학회논문지, 2014.10.

[2] 박혜숙, 이순석, 현종웅, “KEIT PD ISSUE REPORT: 세이프네트워크 기술”, 한국산업기술평가관리원, 2013.04.

[3] 예병호, 박종대, “고신뢰 네트워킹 기술”, “ETRI”, 2015.

[4] 이우식, 오현석, 김남기, 최윤호, “다양한 대용량 공격 트래픽을 효과적으로 차단하기 위한 보안 서비스 체이닝 기술”, 한국통신학회 학술대회논문집, 2014.01.

[5] 김석훈, 김귀정, “클라우드 기반 스마트 사무환경 구축을 위한 지능형 세이프 네트워크 기술”, 디지털융복합연구, 2014.12.

[6] 서신석, 홍성철, 홍원기, “BGP 보안 위협 요소와 대처 방안”, 한국통신학회 학술대회논문집, 2008.11.