BcN에서의 침입감내를 위한 네트워크 디자인 연구

(Research on Network Design for Intrusion Tolerance of BcN)

박 현 도 † 김 수 † 이 희 조 †† 임 채 태 ††† 원 유 재 ††††

(Hyundo Park) (Soo Kim) (Heejo Lee) (Chaetae Im) (Yoojae Won)

요 약 광대역통합망(Broadband Convergence Network, BcN)은 전화, 인터넷, 방송 네트워크 등 개별적으로 운용되어오던 네트워크들을 하나의 통합망으로 구축, 구동, 관리하는 차세대 네트워크이다. 개별적으로 운용되어오던 네트워크들이 하나로 통합되면서 서비스 별로 산재해 있던 네트워크의 위협요소는 하나의 통합망에서 더욱더 위력적인 요소로 다가올 것이다. 본 논문에서는 BcN 서비스들이 악성 공격에 대해 지속적인 서비스 운영을 보장하기 위한 네트워크 디자인 방법을 제안한다. 본 연구는 서비스 시간과 공간 중요도를 바탕으로 BcN 필수 서비스 구성요소를 도출하고, 구성요소의 형태에 따라 서버 형태, 게이트웨이 형태, 복합 형태의 세 가지 타입으로 구분한다. BcN 환경에서 발생 가능한 공격 시나리오들을 통해 BcN 필수 서비스의 침입감내 기술 적용 방안을 모색한다. 이를 통하여 하드웨어 중복성과 Policy 서버의 보안 정책 설정을 통한 BcN 침입감내 네트워크 디자인을 제안한다. 본 논문에서는 제안한 프로토타입 네트워크를 BcN에 적용하기 전과 적용한 후 BcN에서 공격이 발생되었을 때의 시나리오를 통하여 BcN의 침입감내를 가능케 함을 보인다.

키워드 : BcN, 광대역통합망, 침입감내, 중복성, Policy 서버

Abstract Broadband Convergence Network (BcN) is the network which unifies telephone network, the Internet and broadcasting networks. Threats to each network can bring serious problems in BcN environment since the whole network can be damaged by various types of attack. The purpose of this study is to suggest the prototype of intrusion-tolerant network design of BcN to guarantee the continuous operation of BcN services against malicious attacks. First, BcN service components, selected by analysis of service time and coverage importance, are classified into three groups by their type: server type, gateway type and hybrid type. Second, the necessity of applying intrusion tolerance on BcN services is deduced by possible attack scenarios on BcN. Finally, we suggest the intrusion-tolerant network design suitable to BcN, using hardware redundancy and secure policies. Also, we present that the suggested network design can increase the intrusion tolerance of BcN.

Key words : BcN, Broadband Convergence Network, Intrusion tolerance, Redundancy, Policy server

1. 서 론

현재의 네트워크는 그림 1과 같이 공중 전화망(Public Switched Telephone Network, PSTN), 인터넷, 방송망 등 각기 개별적인 서비스에 따라 개별적으로 구축, 구동, 관리되고 있다. PSTN망은 음성 전화 서비스를 제공하기 위한 네트워크이며, 인터넷은 데이타를 주고받는 서비스를 제공하기 위한 네트워크이며, 방송망은 TV를 포함한 방송 서비스를 제공하기 위한 네트워크이며, 기타 여러 서비스를 제공하기 위하여 전 세계적으로 각기 개별적인 네트워크들이 운영되고 있다.

이렇게 각기 개별적으로 운영되어오던 네트워크들이 하나의 망으로 통합 운영됨에 따라서 개별적 네트워크들이 각각 개별적으로 내포하고 있던 위협요소들 또한

· 본 연구는 정보통신부 및 정보통신연구진흥원의 IT 신성장동력핵심기술개발사업의 일환으로 수행하였습니다.(2005-S-402, 침입감내기술개발)
본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다(2007-SW-51-DJ-01).

† 비 회 원 : 고려대학교 컴퓨터학과
hyundo95@korea.ac.kr
philipjkim@gmail.com
†† 비 회 원 : 고려대학교 컴퓨터학과 교수
heejo@korea.ac.kr
††† 비 회 원 : 한국정보보호진흥원 기술기획팀 연구원
chtim@kisa.or.kr
†††† 종신회원 : 한국정보보호진흥원 기술기획팀 팀장
yjwon@kisa.or.kr

논문접수 : 2005년 12월 27일
심사완료 : 2007년 5월 30일

통합되는 결과를 초래할 것이며, 더욱더 강력하고 복잡한 위협 요소로 발전하여 우리의 인터넷을 통한 풍요로운 삶을 위협할 것이다. 그림 1의 왼쪽과 같이 개별적으로 운영되어온 네트워크에서는 하나의 네트워크의 서비스 장애가 다른 네트워크의 서비스 장애를 초래하지는 않는다. 2003년 1월 25일에 있었던 인터넷에서의 DNS 서버의 서비스 장애로 인하여 인터넷 서비스가 불능상태까지 갔던 1.25 인터넷 대란은 그 대표적인 예이다. 1.25인터넷 대란이 발생하여 인터넷 불통사태가 일어났더라도 전화와 방송망 등 인터넷과는 개별적으로 운용되고 있던 망에서의 서비스 불능상태를 초래하지는 않았다. 하지만 현재 시범 서비스가 시작되어 수년 내에 구축될 광대역통합망 BcN(Broadband Convergence Network)에서는 그림 1의 오른쪽과 같이 침입에 의한 장애로 인하여 BcN이 제공하는 전화, 인터넷, 방송 등 다양한 서비스가 동시에 불능 상태에 빠질 수 있다. 따라서, 침입에 의한 BcN 전체 서비스 장애를 예방하고 침입에 대한 빠른 대응, 더 나아가 대응의 능동적, 지능화와 자동화를 실현하기 위해서는 알려진 공격은 물론 알려지지 않은, 앞으로 발생 가능한 공격까지 탐지, 대응, 복구, 예방을 가능케 하는 침입감내기술의 적용이 필요하다.

본 연구는 총 3단계를 거쳐 BcN 환경에 적합한 침입감내 네트워크 디자인의 프로토타입을 제안한다. 첫째, BcN의 여러 구성요소들 중에 서비스 불능 상태가 되었을 경우 망 전체의 구동에 영향을 미치는 서비스들을 구별하여 BcN 필수 서비스로서 도출한다. 이 필수 서비스 들은 서비스 시간과 공간 중요도를 바탕으로 도출하며, 서비스 형태에 따라 서버 형태, 게이트웨이 형태, 복합 형태의 세 가지 타입으로 구분한다. 둘째, 기존 침입감내 기법들을 분류, 기 분류된 BcN 필수 서비스들에 효율적으로 적용할 수 있도록 한다. 마지막으로, 하드웨어 중복성과 Policy 서버의 보안 정책 설정을 통한 BcN 침입감내 네트워크 디자인을 제안하고, BcN필수 서비스에 침입감내 기법을 적용하기 전과 적용한 후의 시나리오를 통하여 네트워크 디자인에 의한 BcN의 침입감내가 가능함을 보인다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 침입감내 기법 및 침입감내 기술 연구 동향을 기술한다. 3장에서는 3단계 통합과정에 따른 BcN 필수 서비스를 도출한다. 4장에서는 BcN 환경에서 발생 가능한 공격 시나리오를 작성한다. 5장에서는 BcN 범용 침입감내 네트워크 디자인의 프로토타입을 제안한다. 제안된 네트워크 디자인을 통해 BcN의 침입감내가 가능함을 시나리오를 통하여 보여준다. 마지막으로 6장에서는 본 연구의 결론과 향후 과제들에 대해 기술한다.

2. 침입감내 기법 및 침입감내 기술 연구 동향

본 장에서는 BcN 환경에 적합한 침입감내 네트워크의 설계를 위해, 기존의 일반적인 침입감내 기법 및 국내외 침입감내 기술 연구 동향을 알아본다. 침입감내 기술에 사용되는 침입감내 기법에는 다양한 종류가 있으며, 그 형태에 따라 크게 하드웨어적인 기법과 소프트웨어적인 기법으로 구분된다. 하드웨어적 침입감내 기법은 주로 하드웨어 모듈의 중복성을 이용한 결함 허용 구조를 띠고 있으며 소프트웨어적 침입감내 기법은 소프트웨어 모듈의 중복성이나 에러 체크, 다양한 버전의 프로그래밍을 통한 결함 허용 구조의 침입감내 기법들이다.

표 1은 침입감내 기법들을 분류하고 특징을 나타낸 표이다[1,2]. 표에 나타난 침입감내 기법들은 각각 특징이 있으므로 절대적인 성능, 신뢰도의 우열을 가리거나 구현에 따르는 비용을 비교할 수는 없으나 일반적으로 알려진 상대적인 성능과 신뢰도, 비용에 따라 비교하였다. 비용은 복제 모듈의 개수와 보터의 유무, 기타 모듈 구현의 난이도를 기준으로 비교하였다. 성능은 해당 결함 허용 기술의 결함 허용에 대한 처리 능력(Performance)에 대한 항목이다. 예를 들어 DMR(Double Modular Redundancy)은 두 개의 서버가 제공하는 결과가 다를 경우 결함이 생긴 서버에 대한 즉각적인 복구가 요구되고 복구될 때 까지는 시스템의 정상 작동이 불가능하지만, TMR(Triple Modular Redundancy)은 세 개의 서버 중 한 서버에 결함이 생길 경우 보터에 의해 결함이 발생한 서버에 대한 복구 작업을 요청하고 정상적인 나머지 두 서버에 의해 시스템이 계속적으로 가동된다. 따

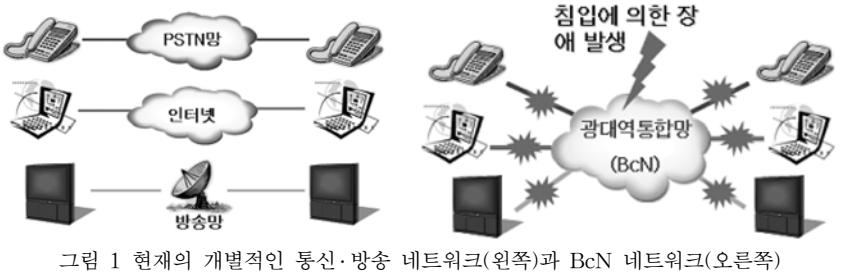

그림 1 현재의 개별적인 통신·방송 네트워크(왼쪽)과 BcN 네트워크(오른쪽)

라서 DMR에 비해서는 TMR의 성능이 더 높기 때문에 DMR은 하, TMR은 중으로 분류하였다. 신뢰도(Tolerance)는 1개의 주 모듈과 n개의 복제된 모듈, 즉 n+1개의 모듈 중 몇 개의 결함까지 신뢰할 수 있는지를 수치로 나타내었다.

BcN은 기존에 개별적으로 운용되어 서비스를 제공하고 있던 개별적인 망들이 하나로 통합되어 운용 관리되는 망으로, 침입감내 기법을 적용하기 위해 하드웨어적 중복성을 보장함으로써 네트워크 개별요소 하나가 서비스를 제공하지 못하는 상황이 되더라도 다른 하나 또는 복수의 중복 요소가 서비스를 지속적으로 제공할 수 있도록 하여 망의 침입감내를 보장할 수 있다. 소프트웨어적 침입감내 기법들은 BcN 망의 구성으로 구현되는 기법들이 아닌 BcN에서 서비스를 제공하지 못하게 되면 통합망 전체의 망 운용에 영향을 주는 요소들에 각각 적용되어 개별 요소의 침입감내를 보장하게 된다.

2.1 침입감내 기법

표 1 내용참조

2.2 국내외 침입감내 기술 연구 동향

최근 국내외에서는 다양한 침입감내기술 관련 연구가 진행되고 있다. 미국 DARPA에서는 침입감내기술 관련 프로젝트로 HACQIT(Hierarchical Adaptive Control of Quality of service for Intrusion Tolerance)[3], SITAR (Scalable Intrusion-Tolerance Architecture)[4], ITUA (Intrusion Tolerance by Unpredictable Adaptation)[5], ITDOS(Intrusion Tolerant Distributed Object Systems) [6] 등의 연구를 완료하였다. 또한 유럽에서는 IST에서 주관한 MAFTIA(Malicious and Accidental Fault Tolerance and Information Assurance)[7]에 대한 연구를 완료하였다. 또한 DSN(Dependable Systems and Networks)에서 발표된 SCIDIVE(A Stateful and Cross Protocol Intrusion Detection Architecture for Voice-over-IP Environments)[8], ADEPTS(Adaptive Intrusion Response using Attack Graphs in an E-Commerce Environment)[9]에 대한 연구 결과가 국외에서 최근 발표되었다. 국내에서는 한국정보보호진흥원(KISA)에서 주관한 DNS, DHCP 침입감내 시스템[10]의 연구와 개발이 완료된 상태이다. 표 2는 이러한 최근 침입감내기술에 대한 비교를 위해 사용된 침입감내 기법과 장, 단점을 정리한 것으로, 기존 연구들은 각각 장점을 가지고 있으나, 기존의 침입감내 기술은 개별로 구동되어온 네트워크 환경에서의 침입감내 기술이다. 그러므로, 여러 서비스가 통합되어 구동되는 BcN이라는 환경을 고려한 침입감내 기술이 아니므로 BcN환경에서 효과적으로 침입감내를 보장할 수 있는 네트워크의 설계가 필요하다.

3. BcN 필수 서비스

본 장에서는 BcN망에서 필수적으로 침입감내 기술이 적용되어야 하는 중요한 서비스들을 도출하여 BcN 필수 서비스로서 구성한다. 개별적으로 운용되어 오던 기존의 네트워크에서는 하나의 망이 서비스를 제공하지 못하더라도 다른 망의 운용과는 크게 문제가 되지 않는다. 1.25대란을 겪으면서 잘 알고 있듯이, 전세계 인터넷의 불통 사태가 있더라도 전화망이나, 혹은 방송 망은 망 구동과 관련하여서는 피해를 입지 않았다. 그러나 여러 서비스를 제공하는 개별 네트워크들이 통합 운용되는 BcN에서는 개별 요소 하나의 서비스 불능이 망 전체의 운용에 영향을 미칠 수 있기 때문에 이러한 요소들을 우리는 BcN 필수 서비스라 한다.

BcN은 3단계 통합 과정을 통하여 개별적으로 산재해

표 1 침입감내기법의 분류

분류 기준	기술명	비용	성능	신뢰도	비고
하드웨어적 기법	DMR	하	하	1	두 서버의 결과가 같을 때만 신뢰 가능
	TMR	중	중	1	셋 중 한 서버의 결함까지 신뢰 가능
	NMR	상	상	(n/2) - 1	n개 중 (n/2) - 1개 결함까지 신뢰 가능
	Standby Sparing	중	하	1	예비 서버에 결함이 발생하기 전에 주 서버가 복구되어야 계속적인 신뢰 가능
	Watchdog 타이머	하	하	1	점검 주기 이후 변동사항이 복구되지 않으므로 읽기 전용 서버에 대해서만 신뢰 가능
	Self-Purging Redundancy	중	중	m(<n)	m : 한 모듈이 대신할 수 있는 다른 모듈의 개수, n : 총 모듈 수
소프트웨어적 기법	체크포인팅 & 롤백	하	하	1	데이타가 체크포인트 이후에 바뀔 경우 복구되지 못함
	Recovery 블록	중	하	1	복구와 관련된 Recovery 블록에 결함이 발생할 경우 신뢰할 수 없음
	N-버전 프로그래밍	상	상	n	n : 같은 기능을 다른 방법으로 구현한 프로그램의 개수
	State Machine Approach	하	중	(n/2) - 1	NMR과 유사한 신뢰도를 가지나 속도가 떨어지므로 빠른 복구를 요함

표 2 국내외 침입감내기술의 비교

프로젝트명	기법	장점	단점
HACQIT	DMR	간단한 구조로 구현이 용이	탐지기능 미약, 시스템 확장성의 한계
SITAR	NMR	기존 서버의 교체 없이 적용 가능, 사용자에게 투명성 보장	DoS 공격에 대한 대응 한계, COTS 서버 외의 구성요소에 대한 보안 필요
ITUA	Hot standby sparing	침입에 대한 신속한 로컬 반응으로 피해 최소화, 집중화의 위험성 방지	관리자에 문제가 생길 경우에 대한 대응 방안 부족
ITDOS	NMR	일정 회수 이상의 연속된 Failure에 대한 서비스 가용성, 기밀성 보장	ITDOS 방화벽 프록시는 내부 호스트로부터의 위협 제거 불가능
MAFTIA	Hot standby sparing	다양한 기술 적용, 자동 환경 설정으로 관리가 용이함	다양한 기법이 사용되어 구현 비용이 높음
DNS, DHCP 침입감내 시스템	Hot standby sparing	L4/L2 스위치를 이용한 부하 분산 및 가용성 보장, DNS, DHCP 서버에 직접 적용 가능	다양한 장비들이 사용되어 구현 비용이 높음
SCIDIVE	Footprinting	VoIP 시스템에 일어날 수 있는 다양한 종류의 침입탐지	탐지에 비해, 대응과 예방 기능이 상대적으로 미약함
ADEPTS	I-GRAPH	I-GRAPH를 이용한 침입대응책 결정, 수행	전자상거래 시스템에 특화되어 타 서비스에 적용할 경우 수정 필요

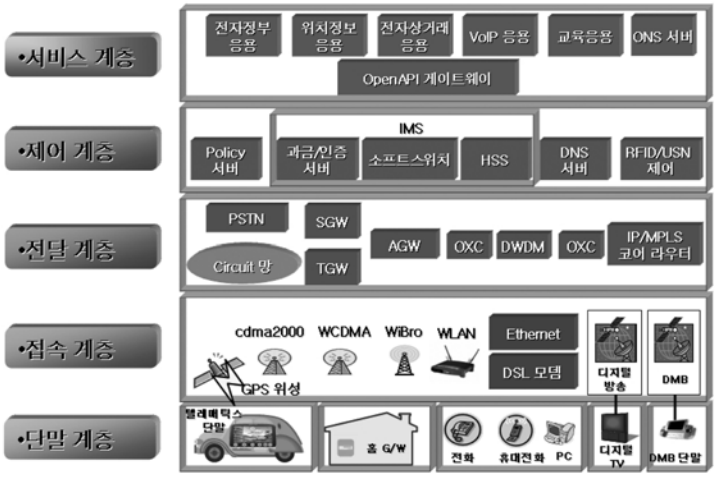

그림 2 BcN 계층별 핵심품목 구성도

있는 네트워크들이 하나의 통합망으로 구축된다. 일차적으로 전화와 인터넷 패킷망의 통합과정을 거친 후에 유선과 무선의 통합과정을 거치고 마지막으로 방송과 통신 네트워크가 융합되면서 개별적으로 운용되어온 개별 네트워크들이 하나의 망으로 통합된다. 그림 2는 3단계 통합과정을 거쳐 구성되는 BcN의 계층별 핵심품목 구성도이다.

본 장에서는 그림 2에서 선정된 필수 서비스들을 형태별로 분류하고, 시간 중요도와 공간 중요도에 따라 구분함으로써 필수 서비스의 중요도에 대하여 분석한다.

3.1 3단계 통합 과정에 따른 BcN 필수 서비스

첫 번째 통합 단계인 음성·데이타 통합 과정에서는 액세스 게이트웨이(AGW)와 트렁크 게이트웨이(TGW), 그리고 이러한 게이트웨이들을 제어하는 소프트스위치에 문제가 발생될 경우 VoIP 서비스는 이루어 질 수 없으며, 그 결과 음성·데이타의 통합 서비스는 제공될 수 없다. SIP 프록시 서버와 SIP 로케이션 서버 역시 VoIP서비스를 제공하기 위한 BcN 필수 서비스이기 때문에 BcN에 위해를 가하기 위한 침입자에 의해 공격대상이 될 확률이 높으며 문제가 발생할 경우 VoIP와 관련된 모든 서비스를 제공하지 못하게 된다. 결국 AGW, TGW, 소프트스위치와 DNS 서버, SIP 프록시/로케이션 서버는 BcN의 음성·데이타 통합 단계에서 필수 서비스로 정의 될 수 있다.

두 번째 통합 단계인 유·무선이 통합되는 BcN환경에서는 단말에서의 다양한 모듈 탑재와 IMS 또는 IMS와 소프트스위치의 연동을 통해 서비스가 제공되게 될 것이다. 유·무선 통합단계에서의 필수 서비스로는 IMS

와 소프트스위치가 될 것이며, 사용자 개인 정보를 포함하고 있는 HSS, 과금/인증 서버, Policy 서버와 전달망 계층의 AGW와 서드파티 애플리케이션 서버에게 망 자원을 제공하는 OpenAPI 게이트웨이, IP 주소 변환을 담당하는 DNS 서버도 유·무선 통합 과정에서의 필수 서비스들이 될 것이다.

세 번째 통합 단계인 통신·방송 융합 단계에서는 유·무선 통합과 마찬가지로 대부분 단말기나 혹은 단지내, 지역 방송국 수준에서 패킷화가 완료되어 IP 백본망과 연결되거나 AGW를 통해 패킷화가 이루어지며, IMS 기반의 이종망간 통합 서비스가 보장되기 때문에 이 과정에서 중점적으로 고려되어야 할 필수 서비스는 제어계층의 소프트스위치나 IMS 전달계층의 미디어게이트웨이인 AGW, 개인 정보 DB인 HSS와 QoS를 관리하는 Policy 서버, 과금/인증 서버, RFID/USN 환경에서 네임서버 역할을 담당하는 ONS 서버라 할 수 있다.

BcN은 음성/데이타 통합, 유/무선 통합, 방송/통신 융합의3단계 통합과정을 통하여 기존의 개별 네트워크를 점차적으로 통합하여 운용할 수 있는 망으로 발전시킨다. BcN에서 망의 자원과 망의 운용에 관련된 구성 요소들에 대한 분석을 통하여 도출된 BcN 필수 서비스와 각각의 필수 서비스들이 BcN에서 제공하는 기능들을 표 3에 정리하였다.

3.2 BcN필수 서비스의 형태별 분류

선정된 필수 서비스들을 분류하는 기준은 여러 가지가 있을 수 있으나, 침입감내기술의 적용을 위한 분류로는 필수 서비스의 종류에 따른 분류가 가장 적당하다. 그 이유는 필수 서비스를 분류함에 있어서 어떠한 서비스를 제공하는지, 그 형태에 따라 분류하는 것이 향후 BcN범용 침입감내 네트워크를 설계함에 있어서 형태별 범용 네트워크를 설계할 때에 중요한 근거가 되기 때문이다.

BcN 필수 서비스는 데이타베이스를 보유하고 데이타를 추가, 삭제, 갱신하는 작업을 수행하는 필수 서비스는 서버 형태의 필수 서비스로 정의할 수 있다. 또한, 데이타베이스를 보유하고 있지는 않지만 데이타의 흐름을 제어, 관리하는 필수 서비스들은 게이트웨이 형태의 필수 서비스로 정의할 수 있다. 게이트웨이의 특성과 서버의 특성을 모두 가지고 있는 복합 형태의 필수 서비스들은 복합 형태의 침입감내 기술을 적용함으로써 복합형 필수 서비스의 침입감내를 극대화 시킬 수 있다. 표 4는 BcN 필수 서비스를 형태별로 분류한 표이다.

표 3 BcN 3단계 통합에서의 필수 서비스

BcN 필수 서비스	제공기능
소프트스위치	o 게이트웨이(AGW, TGW, SGW) 제어 o 호 접속 서비스 및 라우팅 제공
IMS	o 소프트스위치의 기능, 사용자 가입, 인증/과금 정보 관리
Policy 서버	o 소프트스위치/IMS와 연동하여 망 자원 사용 현황 파악 및 할당, 보안 정책 설정
HSS	o 가입자 프로파일 DB o 서비스 가입 관련 정보 관리
과금/인증 서버	o 가입자 인증, 권한 검증, 과금 수행
OpenAPI 게이트웨이	o OpenAPI 응용서버와의 인증 담당
ONS 서버	o RFID 정보로 모든 물품을 식별할 수 있는 코드(ePC)를 기반, 실제 물품 정보가 있는 서버 주소 제공
DNS 서버	o 인터넷 도메인 이름을 IP 주소로 변환
AGW	o 다양한 형태의 이 기종 망과 IP 망을 연결
TGW	o AGW와 같은 기능 o 가입자 연결 및 관리 기능이 없고 캐리어 급의 대형 패킷 스위칭과 같은 기존 탠덤 교환기를 대체하는 역할을 담당
SGW	o IP 망과 PSTN 망의 전송 계층 변환
SIP 프록시 서버	o SIP 로케이션 서버와의 연동을 통한 연결 기능 o 연결 후 통화 메시지에 대한 중계 기능
SIP 로케이션 서버	o 발신자와 수신자의 연결을 위한 SIP 프록시 서버의 위치 정보 요구에 대한 정보 제공

표 4 BcN 필수 서비스의 형태별 분류

분류		해당 BcN 필수 서비스	특징
서버 형태	읽기전용	DNS, ONS, SIP 로케이션/프록시 서버	데이타 보유, 읽기전용 형태의 정보 제공 담당
	읽기/쓰기	Policy 서버, HSS, 과금/인증 서버	데이타 보유, 읽기/쓰기 형태의 정보 처리 담당
게이트웨이 형태		AGW, TGW, SGW	데이타 보유하지 않음, 이 기종 망간의 데이타 변환·처리
복합 형태		소프트스위치, IMS, OpenAPI 게이트웨이	데이타 보유, 읽기/쓰기를 통한 정보 처리, 데이타 변환

3.3 BcN 필수 서비스의 중요도 분석

앞에서는 BcN의 수많은 구성 요소들 중에서 서비스 장애가 발생할 경우 통합망 구동에 영향을 줄 수 있는 중요 구성요소로서 필수 서비스를 선정하였다. 즉, 다른 서비스들에 비해 공간중요도와 시간 중요도가 높은 구성요소들이 필수 서비스로 선정되었다. 공간 중요도란 해당 서비스에 장애가 발생하였을 경우 장애 범위의 정도를 기준으로 한 중요도이며, 시간 중요도는 해당 서비스의 지속적인 서비스 제공 가능시간을 기준으로 한 중요도이다. 시간/공간 중요도를 기준으로 필수 서비스를 선정하였으며, 또한 필수 서비스들 내에서도 이 두 가지 중요도 기준에 의해 형태별로 구분될 수 있다. 시간 중요도와 공간 중요도를 기준으로 필수 서비스를 다시 구분하면, 게이트웨이 형태의 필수 서비스는 시간 중요도가 공간 중요도에 비해 상대적으로 높으며, Policy서버를 제외한 HSS, SIP서버, DNS서버 등, 서버형태의 필수 서비스들이 시간 중요도 보다는 공간 중요도가 상대적으로 높다. 그리고 복합 형태의 서비스 들은 시간 중요도와 공간 중요도가 함께 높은 서비스 들이다. 그림 3은 선정된 BcN 필수 서비스를 공간 중요도와 시간 중요도에 따라 분류한 것이다.

그림 3 BcN 필수 서비스의 시간중요도와 공간중요도에 따른 분류

우리는 BcN 3단계 통합과정을 통해 BcN 필수 서비스를 도출하고, 도출된 필수 서비스들을 서비스의 형태별로 분류하였으며, 필수 서비스들의 중요도를 시간 중요도와 공간 중요도로 나눠 구분하였다. BcN 침입감내 기법의 적용은 우선적으로 필수 서비스에 적용하여 망의 운용과 관련된 침입감내를 보장해야 하며, 시간 중요도와 공간 중요도가 상대적으로 높은 서비스들을 우선적으로 보호해야 한다. AGW, TGW, SGW와 같은 게이트웨이가 서비스를 제공하지 못하게 되는 경우보다 DNS서버를 사용하지 못하게 되는 경우 사용자들이 입는 피해의 규모는 더 커질 수 있기 때문이다.

4. BcN 환경에서 발생 가능한 공격 시나리오

BcN 환경에서 발생 가능한 공격들의 유형은 실로 기술하는 것이 불가능 할 정도로 샐 수 없이 많다. 본 장에서는 BcN 환경에서 발생 가능한 대표적인 공격 시나리오를 작성한다. 이를 통하여 발생 가능한 공격을 예측하고, 공격이 발생되었을 때 BcN에서의 피해 상황을 알아봄으로서 BcN 침입감내 기술의 적용 방안을 모색한다.

BcN은 유·무선, 그리고 수많은 개별 네트워크가 통합되는 망이다. 그림 4는 유선, 무선, 그리고 기업 네트워크로 구성된 BcN 전체 환경 중 일부에서 인터넷 웜이나 봇을 통한 DDoS공격에 의해 필수 서비스가 올바른 서비스를 제공하지 못할 경우 네트워크에 어떠한 문제가 발생되는지에 대하여 보여준다. 그리고 인터넷 웜이나 봇에 의해 네트워크가 감염되어 DDoS공격을 하는 네트워크 단말들을 유선 구간의 단말들로 표현했지만, 앞으로 네트워크 서비스가 가능한 모든 단말들이 BcN 환경에 통합되기 때문에 기존의 네트워크와 단말 및 잠재적으로 BcN에 추가될 가능성이 있는 다양한 네트워크와 단말들에 대해 인터넷 웜이나 봇 등, 악성코드에 감염되어 BcN을 위협하는 요소가 될 것이다. 또한 개별적인 네트워크가 BcN으로의 발전되는 것과 함께 단말 기술의 발전에 힘입어 단말들의 엄청난 성능 발달은 현재에도 충분히 경험하고 있으며, 이러한 발전은 현재 우리가 상상하는 그 이상의 피해결과를 초래하는 요인으로 작용할 것이다. 그림에서는 유선, 무선, 그리고 기업 네트워크에 대하여 가정하였지만, 그림 4의 모습은 BcN 전반에 걸쳐 발생되는 모습의 일부분이다.

그림 4의 (a)는 BcN필수 서비스 중 DNS가 DDoS공격에 의해 올바른 서비스를 제공하지 못할 경우 무선 구간과 기업네트워크의 서버나 호스트들은 도메인 네임을 이용한 인터넷 서비스를 제공받을 수 없게 된다. 1.25 인터넷 대란에서 경험했던 인터넷 불통사태가 전화, 방송 등의 네트워크로 확대됨은 물론이며, 전세계의 모든 네트워크들이 불통사태로 걷잡을 수 없이 확대될 것은 자명하다. 또한 그림 4의 (b)는 HSS가 DDoS공격에 의해 올바른 서비스를 제공하지 못할 경우 다른 네트워크 단말 사용자들이 사용자 인증/과금 등의 서비스를 제공받지 못하므로, 인터넷을 사용할 수 없게 되는 결과를 초래하는 것을 그림으로 보여준 것이다. 이 경우 역시 (a)와 마찬가지로 BcN 환경에서는 인터넷뿐만이 아닌 전화, 방송 등 다양한 네트워크 서비스를 중단시키는 결과를 초래할 것이다.

BcN에서의 필수 서비스에 대한 공격 시나리오를 통하여 필수 서비스가 서비스 불능 상태가 될 때에 BcN 망의 운용과 관련하여 피해가 기존의 개별적으로 운용되어오던 네트워크보다 훨씬 크다는 것을 알았다. 그러므로, BcN망을 안전하게 운용하여 BcN에서 서비스를 제공받는 모든 사용자가 서비스를 지속적으로 제공받기

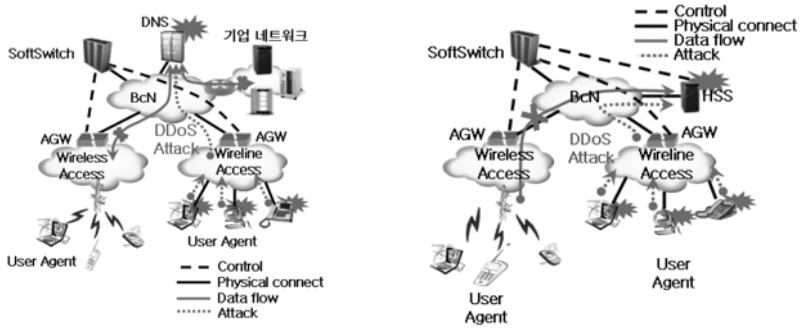

그림 4 BcN필수 서비스 중 DNS와 HSS에 대한 공격 시나리오

위해서는 BcN에 침입감내 기법을 필수적으로 적용해야만 한다.

5. BcN 범용 침입감내 네트워크 디자인 프로토타입

앞 장에서 BcN 필수 서비스는 크게 서버 형태, 게이트웨이 형태, 복합 형태로 구분하였다. 본 장에서는 서버 형태와 게이트웨이 형태의 BcN 필수 서비스 구성요소에 대해 각기 다른 하드웨어 중복 네트워크를 설계하고, 중복성을 바탕으로 구성된 필수 서비스 구성요소 군 각각에 대해 Policy 서버를 배치하여 보안 정책 설정 및 관리, 감시를 가능하게 한다. 이를 통해 침입에 대한 예방 및 대응이 가능함과 동시에, 침입이 일어난 경우에도 일정 시간 이상 서비스를 지속할 수 있어야 한다. 또한 개별 서비스적으로 침입감내 네트워크를 설계할 경우에는 그만큼 많은 비용을 지불 할 수 밖에 없다. 그러므로 어떠한 망에서도 적용 가능한 범용 침입감내 네트워크 디자인 프로토타입을 제안한다.

향후 망의 통합에 따른 다양한 공격에 대처하기 위해

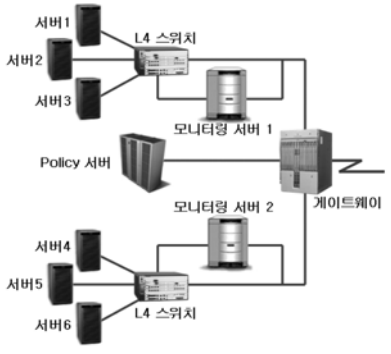

그림 5 서버형태의 BcN 필수 서비스의 침입감내 네트워크 디자인

서는 트래픽의 L4스위치를 통한 부하분산과 모니터링 서버에 의한 DDoS공격이나 웜의 전파를 탐지하여 L4 스위치에 정책을 하달하는 침입감내 시스템이 도입되어야 한다. 하지만 단순 서버의 침입감내 시스템 도입을 통해서는 통합된 망의 침입감내에 적절하다고 할 수 없다. 그 이유는 공격은 특정 서버에 대한 공격도 있겠지만, 대상이 수많은 서버가 될 수도 있다. 그러할 경우 모든 서버의 모니터링 서버는 이상 징후를 탐지하기 위하여 각기 개별적으로 리소스를 할당해야 한다. 이를 보완하기 위하여 한쪽의 서버가 이상이 발생하였을 경우 네트워크의 다른 서버의 모니터링 서버에게 현재상황을 보고하고 다른 네트워크의 서버는 이상 징후 현상을 전달받아 특별히 모니터링 하지 않고도 현재 공격에 대한 대비를 수행할 수 있도록 하는 시스템이 그림 5이다. 그림 5의 구조는 서버1, 서버2, 서버3은 TMR구조를 가진 서버 군이며, L4스위치에 의해 공격 트래픽을 컨트롤 할 수 있도록 되어있다. 그러나 L4스위치를 이용하여 단순 트래픽 분산 기술만 적용된 상황에서는 만약 서버 1이 공격 받는다면, 서버 2와 서버 3이 공격에 의해 쉽게 서비스 불능 상태가 되기 때문에 공격에 대해 모니터링 서버를 이용하여 트래픽 차단 등의 정책을 L4스위치에 하달할 수 있도록 해야 한다. 또한 고속 네트워크 환경하에서는 전세계 서버 모두가 공격 당하는 대에 걸리는 시간은 지극히 짧다. Slammer웜의 경우 전세계의 취약한 서버의 90퍼센트가 감염되는데 단지 10분이 걸렸던 사례를 통해 단순 트래픽 부산 기술만으로는 대응이 역부족이라는 것을 익히 알고 있다.

또한 모니터링 서버 1에서 모니터링 한 결과는 Policy 서버로 전달되고 Policy서버는 전달받은 결과를 모니터링 서버 2에 정책 하달함으로써 다른 부분에 구성되어 있는 서버는 침입에 의해 손상 받기 전에 예방이 가능하게 된다. Policy 서버는 서비스 인증, 네트워크 장비 사용 내역 추적, 파일 제어를 담당하는 정책 기반 네트

워크의 보안 구성요소이다. Policy 서버에서 사용되는 정책 관련 소프트웨어는 방화벽이나 침입탐지시스템(IDS) 등의 하드웨어와 연동하며, 방화벽 필터링 및 감사 대상 범위를 네트워크 경계선 내, 외부에 위치한 PC를 포함한 네트워크 전반으로 확대시킨다. 이와 함께, 원격 접속 시스템, 모바일 노트북, VPN 게이트웨이, 공유 서버, DMZ 서브넷, 웹서버, 현장의 데스크탑 및 브로드밴드 연결 등 다양한 형태의 장비들에 대한 정책 기반 보안 서비스를 제공한다. 따라서, Policy 서버는 여러 가지 서비스들이 융합되어 다양한 장비들이 한 네트워크에 연결되어 있는 BcN 환경에서 많은 보안상의 이점을 제공한다.

Policy 서버에서 적용이 가능한 정책은 크게 네 가지로 분류할 수 있다. 첫째, Group Role 기반 접근 제어 보안 정책은 사용자 그룹 레벨에 따라 보안 권한을 차등 부여함으로써 파일/디렉토리, 프로세스, 네트워크 포트에 대한 강제적 접근 제어를 가능하게 한다. 이 정책은 데이타를 보유하고 있는 서버 형태의 필수 서비스에 적용되어 사용자의 접근 권한을 다양하게 설정함으로써 데이타의 기밀성과 무결성을 보장할 수 있다. 둘째, 비정상 접근 또는 서비스 요청 거부 정책은 불필요 포트 차단 및 ping 요청 거부 등의 방법을 통해 비 정상적인 접근과 서비스 요청을 거부하는 정책이다. 이 정책은 서버 형태와 게이트웨이 형태 모두에 적용될 수 있으나, 게이트웨이 형태의 필수 서비스에 적용할 경우 서버를 향한 악의적인 공격을 미리 차단하여 서버의 부하를 줄여줄 수 있기 때문에 게이트웨이 형태의 필수 서비스들에 우선적으로 적용하는 것이 바람직하다. 셋째, 접속 장치 보호 정책은 방화벽 카드와 같은 하드웨어를 사용하여 각종 접속 장치를 공격으로부터 보호한다. 이 정책은 BcN에 존재하는 다양한 게이트웨이 형태의 필수 서비스와 소프트스위치, IMS와 같은 복합 형태 필수 서비스들에 적용되어 해당 장치를 보호하는 효과를 얻을 수 있다. 넷째, 비 인증 접속 차단 정책은 Policy 서버에 배치된 중앙 집중형 정책들이 라우터나 트래픽 흐름과 상관없이 서비스 사용자나 호스트로 할당되며, 서버의 구성요소인 방화벽 카드를 이용하여 인증된 Policy 서버에서 내려진 명령에만 순응하도록 제어한다. 이 정책은 서버 형태나 복합 형태의 필수 서비스들에 적용되어 해당 서비스들이 인증된 명령에만 동작하게 하기 때문에 DDoS와 같은 공격을 예방할 수 있다. 네 가지 정책 이외에도 다양한 새로운 정책이 Policy 서버에 추가될 수 있으며, 이 때 Policy 서버는 빠른 정책의 업데이트를 통해 BcN의 침입감내를 보장하고 네트워크 상태를 최적으로 유지해야 한다. 표 5는 Policy서버에 각 정책이 반영되었을 때의 효과에 대해 정리한 것이다.

그림 6은 서버 형태와 게이트웨이 형태의 BcN 필수 서비스들이 서로 연결되어 있는 네트워크에서 적용 가능한 침입감내 네트워크 디자인을 도식화한 것이다. 그림 6 중 게이트웨이 형태의 필수 서비스에 대한 침입감내 기술을 적용한 부분은 게이트웨이 형태의 필수 서비스의 침입감내를 보장하기 위하여 중복기술과 L4스위치와 모니터링 서버를 이용한 트래픽 분산과 차단 등의 정책 실현을 통하여 개별 게이트웨이 형태의 필수 서비스를 보호할 수 있다. 또한 Policy서버 3을 통하여 다른 곳에 있는 게이트웨이 형태의 필수 서비스에 적용된 모니터링 서버에 정책을 하달함으로써 침입에 대한 예방이 가능하도록 한다. Policy 서버는 앞에서 설명한 다양한 보안 관련 정책을 해당 네트워크에 적용하여 보안 수준을 향상시키고, 사용자와 사업자간에 QoS/SLA 준수 여부를 감시하고 망 자원의 사용 현황을 파악하여 적합한 QoS를 보장하는 망 자원을 할당하는 기능을 제공한다. 서버형태의 필수 서비스와 게이트웨이 형태의 필수 서비스들은 각각 중복성을 가지고 침입감내를 보장하며, 적용된 각각의 침입감내 네트워크에 포함되어 있는 각각의 Policy서버들의 전체적인 유기적 공조를 통해 BcN 망 전체적인 보안 정책 강화 및 각 구성 요소가 포함된 지역 네트워크의 보안 정책을 강화한다. 이를

표 5 Policy 서버의 정책과 효과

정책 적용 해당 서비스	보안 정책	적용에 대한 효과
DNS, ONS, SIP 로케이션 / 프록시 서버, Policy 서버, HSS, 과금 / 인증 서버	Group Role 기반 접근 제어 보안 정책	RBAC (Role-Based Access Control)에 의한 정확하고 쉬운 정책 설정과 사용자 주체, 프로세스 주체, 또는 사용자-프로세스 주체로 개별 자원에 대한 세밀한 보안 정책 설정 가능
AGW, TGW, SGW	비 정상 접근 또는 서비스 요청 거부 정책	패킷 필터링 및 감사 기능의 자동화, 스니핑과 스푸핑 차단
AGW, TGW, SGW, 소프트스위치, IMS, OpenAPI 게이트웨이	접속 장치 보호 정책	방화벽 경계선 내, 외부에 위치한 VPN 종단점, 브로드밴드 액세스 게이트웨이와 같은 인터넷 접속 장치를 안전하게 보호
Policy 서버, HSS, 과금 / 인증 서버, 소프트스위치, IMS, OpenAPI 게이트웨이	비 인증 접속 차단 정책	웹과 전자상거래(e-commerce)용 서버, DMZ 서브넷, 서비스 사용자 데이타베이스 등을 인터넷을 통한 각종 해킹 공격으로부터 보호

통해 발생 가능한 다양한 공격 및 침입 행위를 차단할 수 있고, 차단되지 않은 침입에 의해 서비스 구성요소에 장애가 발생할 경우에도 TMR이나 DMR과 같은 기법이 적용된 네트워크 디자인을 바탕으로 일정 시간 이상 서비스를 지속적으로 운영할 수 있다.

4장에서 소개된 경우와 같은BcN에서 발생 가능한 공격 시나리오에 대해 그림 6과 같은 범용 침입감내 네트워크 디자인을 적용할 경우 예상되는 결과는 다음과 같다. DNS서버는 형태 분류상 서버 형태에 해당한다. DNS 서버에 TMR을 적용, L4스위치에 연결하면 하나의 서버는 주 서버로서의 역할을 수행하고, 나머지 두 서버들은 백업으로 데이타를 동기화하며 대기 상태에 있게 된다. 공격자가 활성 상태에 있는 DNS 서버를 공격하여 정상적으로 작동하지 않을 경우에 L4스위치는 공격으로 정상 작동이 불가능한 서버를 대기 상태로 전환하고 대기 상태에 있던 백업 서버 중 하나를 활성 상태로 전환하여 도메인 네임 서비스를 제공하는 데에 침입감내를 보장하게 된다. 풀메쉬(Full-mesh) 토폴로지로 연결된 두 개의 게이트웨이 역시 한 대가 침입에 의해 작동하지 않아도 백업 게이트웨이가 지속적인 서비스를 제공하므로 게이트웨이 형태의 BcN 서비스 구성요소인 TGW, SGW, AGW 등에 적용할 경우 일정 수준 이상의 침입감내가 가능해진다.

향후 BcN은 개별적으로 운용 되어오던 개별 네트워크들이 통합되는 통합망이다. 현재 침입감내 기술들은 개별 네트워크에 특화되어 개별 네트워크의 침입감내를 보장하도록 설계된 네트워크 디자인들이 대부분이다. 그러나 이렇게 개별적으로 특화된 네트워크들이 수많은 서비스가 통합되는 BcN에 적용된다면, 수많은 서비스에 개별적으로 침입감내 기술을 적용하기 위하여 수많은 비용이 들 수 밖에 없다. 또한, 통합망에서 침입감내 기술들이 개별적으로 개발 적용된다면, 인터넷 웜과 같이 네트워크의 서버들을 감염시키는 공격을 예방하기에는 부족함이 많다. 그러므로, 공격에 대한 사전 예방을 위해서는 네트워크들의 침입 공조 대응 기술이 필요하며, 이를 통해 일부 네트워크가 침입을 당할 때 침입 상황을 다른 네트워크에 보고하여 사전 예방을 수행할 수 있게 된다.

본 연구에서 제안한 BcN범용 침입감내 네트워크는 이러한 조건을 모두 만족하는 침입감내 기술이다. 서버 형태의 필수 서비스는 개별적인 침입감내를 위해 복제기술이 적용되어 자체적으로 침입감내를 수행함과 동시에 네트워크 단말 계층의 Policy서버는 다른 서버들과의 유기적인 공조 침입 대응이 가능하도록 한다. 그리고, 전달망 계층의 게이트웨이 형태의 필수 서비스에는 지능형 L4스위치와 복제 기술을 통하여 자체적으로 침입에 대한 대응을 수행하며, BcN 전달망 계층의 Policy서버는 다른 게이트웨이 형태의 필수 서비스와 유기적인 공조 침입감내 서비스를 제공할 수 있도록 한다. 그리고 서버 형태의 필수 서비스들에 적용된 Policy서버와 게이트웨이 형태의 필수 서비스에 적용된 Policy서버들간의 유기적인 공조를 통하여 전체 BcN의 침입감내 서비스를 제

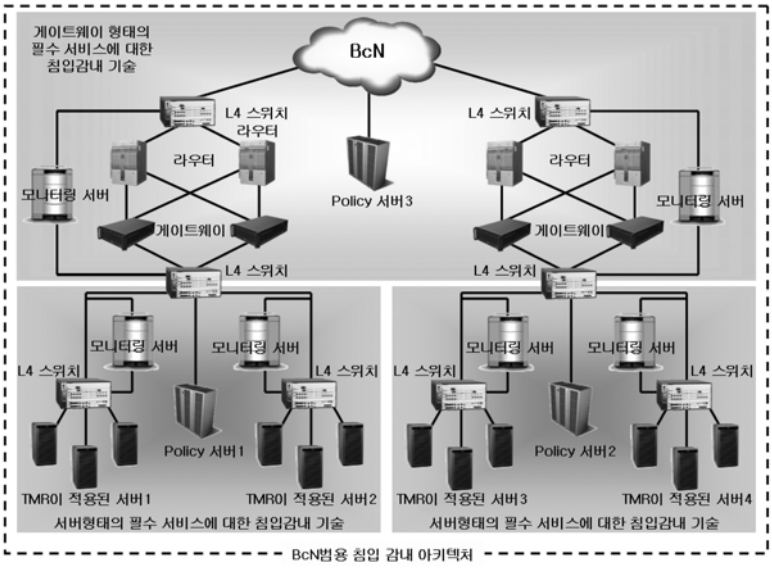

그림 6 서버형태의 필수 서비스와 게이트웨이 형태의 필수 서비스의 침입감내 기술 적용, 범용 침입감내 네트워크 구조도

공할 수 있다. 기존 침입감내 연구 동향 중 NMR 기법을 기반으로 한 SITAR, ITDOS는 BcN 침입감내 네트워크와 하드웨어적인 중복성을 이용했다는 점은 유사하지만, 내부 호스트로부터의 공격이나 DDoS와 같은 공격에 취약하다는 단점이 존재하였다. 하지만, 본 논문에서 제안된 침입감내 네트워크 디자인은 Policy 서버가 보안 정책을 관할, 다양한 내, 외부로부터의 공격 및 침입 행위에 대해 원천적으로 차단하는 장점을 가지고 있다.

6. 결 론

본 연구는 BcN 구성요소들 중에서 침입에 의하여 정상적인 서비스를 제공하지 못할 경우 통합망 전체에 영향을 줄 수 있는 필수 서비스를 선정, 서버 형태, 게이트웨이 형태, 복합 형태로 구분하였으며, 이들을 보호하여 BcN의 침입감내를 보장하기 위해 필수 서비스들에 대한 침입감내 네트워크 디자인의 프로토타입을 제안하였다. 그리고 필수 서비스에 침입감내 기법을 적용하지 않았을 때의 BcN에서의 공격 시나리오를 통하여 피해의 심각성을 알았으며, 제안한 침입감내 네트워크 디자인의 프로토타입을 제안한 후의 시나리오를 통하여 BcN의 침입감내를 보장 할 수 있음을 보였다.

BcN은 여러 산재해 있는 네트워크를 통합하여 하나의 통합망으로 운영되는 네트워크이다. 결국 산재해 있는 네트워크가 통합되는 것은 산재해 있는 서비스들의 취약점 또한 통합되며, 산재해 있는 잠재된 피해 상황들이 통합되는 결과로 직결된다. 여러 산재해 있는 서비스들에 각기 다른 침입감내기술을 적용한다면, 새로운 서비스를 제공하기 위한 구성요소가 추가될 때마다 기술의 추가개발이 불가피하며, 추가비용이 지속적으로 발생할 수밖에 없다. 그러므로 효율적인 침입감내기술 개발은 범용 침입감내기술 개발을 목표로 해야 한다. 본 논문에서는 이미 선정된 필수 서비스 및 새로운 필수 서비스들에 대해 적용 가능한 범용 네트워크 디자인의 설계를 위해 세 종류로 분류된 필수 서비스의 형태에 적합한 L4스위치와 서버 및 게이트웨이의 중복성, Policy 서버를 통한 보안 정책 설정을 이용한 침입감내 네트워크 디자인을 제안하였다.

BcN은 현재 개발 중에 있는 네트워크 환경으로 그 구성요소 및 네트워크 전체 네트워크는 가변성을 가지고 있으며, 본 논문에서 제안한 네트워크 디자인을 직접 적용, 그 성능을 정량화, 평가할 수는 없으나 수많은 BcN 서비스 구성요소의 중요도 부여, 형태 구분을 통해 중요도가 높은 구성 요소에 대해 적합한 형태의 네트워크를 설계함으로써 향후 BcN의 보안 및 침입감내 능력을 향상시켜 BcN에서의 생존성을 보장할 수 있다.

참 고 문 헌

[1] EventHelix, "Fault Handling and Fault Tolerance," http://www.eventhelix.com/RealtimeMantra/FaultHandling/.

[2] Wikipedia, "Fault Tolerant system," http://en.wikipedia.org/wiki/ Fault_tolerant_system.

[3] James Reynolds, James Just, Ed Lawson, Larry Clough, Ryan Maglich, "The Design and Implementation of an Intrusion Tolerant System," Proc. IEEE DSN, 2002.

[4] Feiyi Wang, Fengmin Gong, Chandramouli Sargor, Katerina Goseva-Popstojanova, Kishor Trivedi, Frank Jou, "SITAR: A Scalable Intrusion-Tolerant Architecture for Distributed Services," Proc. IEEE SMC, 2001.

[5] Tod Courtney, James Lyons, HariGovind V. Ramasamy, William H. Sanders, and Mouna Seri, Michael Atighetchi, Paul Rubel, Christopher Jones, Franklin Webber, Partha Pal, and Ronald Watro, "Providing Intrusion Tolerance With ITUA," Proc. IEEE DSN, 2002.

[6] David Sames, Brian Matt, Brian Niebuhr, Gregg Tally, Brent Whitmore, David Bakken, "Developing a Heterogeneous Intrusion Tolerant CORBA System," Proc. IEEE DSN, 2002.

[7] A. Adelsbach, D. Alessandri, C. Cachin, S. Creese, M. Dacier, Y. Deswarte, K. Kursawe, J. C. Laprie, B., Pitzmann, D. Powell, B. Randell, J. Riordan, R. Stroud, P. Verssimo, M. Waidner, I. Welch, A. Wespi, "MAFTIA Conceptual Model and Architecture," LAAS-CNRS Report No. 01426, 2001.

[8] Yu-Sung Wu, Saurabh Bagchi, Sachin Garg, Navjot Singh, "SCIDIVE: A Stateful and Cross Protocol Intrusion Detection Architecture for Voice-over-IP Environments," Proc. IEEE DSN, 2004.

[9] Bingrui Foo, Yu-Sung Wu, Yu-Chun Mao, Saurabh Bagchi, Eugene Spafford, "ADEPTS: Adaptive Intrusion Response using Attack Graphs in an E-Commerce Environment," Proc. IEEE DSN, 2005.

[10] 이강신, 임채태, 이태진, 김형종, 이동훈, "SITIS: Scalable Intrusion Tolerance Middleware for Internet Service Survivability," Proc. IEEE PCM, 2004.

박 현 도

2004년 고려대학교 수학과, 컴퓨터학과(학사). 2007년 고려대학교 컴퓨터학과(석사). 2007년~현재 고려대학교 컴퓨터학과(박사과정). 관심분야는 네트워크 이상 탐지 및 방어

김 수

2005년 고려대학교 컴퓨터학과 학사. 2005년~현재 고려대학교 컴퓨터학과 석사과정. 관심분야는 Network topology, Wireless networks

이 희 조

1989년~2000년 포항공대 컴퓨터공학과 학사/석사/박사. 2000년~2001년 미국 Purdue University 박사후연구원. 2001년~2003년 안철수연구소 최고기술책임자(CTO). 2004년~현재 고려대학교 정보통신대학 컴퓨터·통신공학부 부교수. 관심분야는 네트워크 보안, 인터넷웜/DDoS 공격 대응기술, 고가용성 시스템 설계

임 채 태

2000년 충남대학교 컴퓨터과학과(학사) 2003년 포항공과대학교 컴퓨터공학과(석사). 2003년~현재 한국정보보호진흥원 선임연구원. 관심분야는 BcN 보안, VoIP 보안, 이동통신, 네트워크

원 유 재

1985년 충남대학교 계산통계학과(학사) 1987년 충남대학교 계산통계학과(석사) 1998년 충남대학교 전산학과(박사). 1987년~2001년 한국전자통신연구원 책임연구원/팀장. 2001년~2004년 안랩유비웨어/안철수연구소 CTO. 2004년~현재 한국정보보호진흥원 팀장. 관심분야는 정보보호, 멀티미디어통신, 이동통신