http://dx.doi.org/10.3745/KIPSTC.2011.18C.5.317

ONSU-MF(One Network Security Unit-Multi Function)기법과 OSD-MD(One Security Device-Multi Defense)기법 기반의 보안정책 구현

서 우 석[†] · 이 규 안[††] · 전 문 석[†††]

요 약

본 논문은 다양한 보안방어 정책과 기기들이 산재해 있으나, 이를 표준화하여, 각 방어정책의 특성과 방어기법을 새롭게 정의함으로써 기존 네트워크 인프라 구현을 포함한 새로운 보안정책 도입 및 추가 구현 시 관리자 또는 사용자가 손쉽게 정책을 추가하고 바로 적용 가능하도록 각 보안 분야별 정책과 기기를 명세 보고서화 하는데 의의가 있다. 따라서 하나의 네트워크 보안기기를 기반으로 부여 가능한 정책들을 분류하는 ONSU-MF(One Network Security Unit-Multi Function)기법과 하나의 보안기기로 다양한 보안방안을 구현하는 OSD-MD(One Security Device-Multi Defense)기법으로 구분하고 이를 통합한 표준화 구현기법을 통해 향후 네트워크 보안 인프라 개선 메커니즘을 제안코자 한다.

키워드 : ONSU-MF, OSD-MD, 보안정책 적용 알고리즘, 네트워크 보안, 정책 표준화, 방어흐름

Implementation of Security Policies of ONSU-MF(One Network Security Unit-Multi Function) and OSD-MD(One Security Device-Multi Defense)

Seo Woo Seok[†] · Lee Gyn An[††] · Jun Moon Seog[†††]

ABSTRACT

This study is meaningful in that it standardizes various security and defense policies and devices, newly defines characteristics of defense policies and defense techniques, and specify and report various kinds of security polities and devices in order for administrators or users to add and apply the policies when introducing new security policies including the implementation of existing network infra and applying additionally. Therefore, this study aims to divide the policies into ONSU-MF(One Network Security Unit-Multi Function) that classifies one network security device-based policies and OSD-MD(One Security Device-Multi Defense), which implements various security methods by using one security device, and suggest network security infra improvement mechanism through the standardization implementation technique integrating the two methods.

Keywords : ONSU-MF, OSD-MD, Security Policy Apply Technique, Network Security, Policy Standards, Defense Flow

1. 서 론

21세기 정보화 발전방향은 침입기법 발전과 더불어 성장해 왔다. 2009년 인터넷 대란을 기점으로 보안 산업의 격변기가 시작되었으며, 다양하고 무수히 많은 보안장비와 솔루션, 정책기반의 프로그램들이 쏟아져 나왔다.

이러한 사회적 현상은 정보보호에 대한 안전 불감증으로 인한 파급효과라고 할 수 있다. 또한, 발전방향은 통합 정보보호 관제 시스템을 개발하는 단계까지 이르렀으나 호환성 관리에 한계가 나타났다. 하지만 기존에 운영하던 보안장비와 솔루션 관제를 통해서 각각의 기기 또는 솔루션과 정책마다 고유한 특성으로 발생하는 장애를 해소하고 종합적인 보안관제라는 획기적인 보안분야의 새로운 장을 열었다.

상호 정보공유가 이질화된 서로 다른 개발사들이 제안, 구축, 구현한 장비와 솔루션을 종합관제 하는 부문에는 그 한계점이 나타나기 시작했다. 정책들이 중첩되는 문제, 정책

† 정 회 원 : 숭실대학교 컴퓨터학과 박사과정
†† 정 회 원 : 서울중앙지방검찰청 첨단범죄수사2부 근무
††† 종신회원 : 숭실대학교 컴퓨터학부 정교수
논문접수 : 2011년 5월 18일
수 정 일 : 1차 2011년 6월 27일, 2차 2011년 7월 28일
심사완료 : 2011년 8월 8일

등급단계 구성 이원화, 직렬정책 적용 시 급격한 통신량의 감소, 병렬정책 적용 시 침입 가능한 정책의 필요불충분 공간 도출 등의 장애가 발생했다.

따라서 보안장비, 솔루션, 정책 등을 표준화하고 각 보안 분야별 제한정책 및 기기 명세를 보고서화 함으로써 하나의 네트워크 보안기기를 기반으로 부여 가능한 정책분류 명세인 One Network Security Unit-Multi Function(이하 ONSU-MF라 한다.) 기법으로 다양한 Platform, Network 방어 정책, 방어를 위한 적정한 서버 선택 등을 통한 방어 영역과 하나의 보안기기로 다양한 보안방안을 구현하는 One Security Device-Multi Defense(이하 OSD-MD라 한다.)기법을 기반으로 하는 다중 보안정책 구현으로 분류하고 두 기법으로 구성 가능한 최적의 보안 표준모델과 결과를 제안함으로써 무분별한 신기술로 인해 발생할 수 있는 장애를 해소하는 방안을 제안하고자 한다.

본 논문의 구성은 2장에서는 최근 보안장비 현황과 침해사례를 제시하고, 3장에서는 다양한 네트워크 인프라 구현을 통한 적용 장비와 정책 분석이 기술되고, 4장에서는 ONSU-MF와 OSD-MD기법 분석과 보안정책 구현 결과를 도출하고 , 5장에서는 향후연구 방향과 결론을 기술했다[1][2].

2. 관련 연구

2.1 최근 보안장비 운영현황

네트워크를 구성하고 있는 보안장비 운영을 위한 솔루션과 장비들이 단계적인 방어 등급 구성에 따른 계획하에 단계적으로 구성되고 도입되는 과정보다는 공중망을 통한 침해사례가 발생하거나 또는 침해로 인한 문제점과 장애가 발생할때마다 VPN(Virtual Private Network), IDS(Intrusion Detection System), IPS(Intrusion Prevention System) 등과 같은 보안기기와 정책구현을 위한 솔루션들이 도입되고 있는 실정이다.

하지만, 이러한 장비와 솔루션들을 종합적으로 관제 가능한 부분은 기존의 장비들을 하나의 특화된 솔루션 범주 내에 묶어서 관리 및 운영하는 ESM(Enterprise Security Management) 정도이다. 또한, 현재 네트워크 보안시장에서는 새로운 차세대 네트워크 보안을 위한 기본적인 방향을 통합 모니터링 영역, 종합 분석 영역, 종합 보안관리 영역, 접근제어 솔루션 영역, 위험관리 영역의 5단계로 구분하고 이를 유기적인 연결 매체로 구성한 방안이 제시되고 있다.

보안부문의 신기술 또한 보안시장에서 지속적으로 개발 및 구축되고 있으며, ONSU-MF와 OSD-MD형태를 표준화 없이 혼용하는 보안기법으로 많은 보안장애와 침해가 나타나고 있다[3][4].

각각의 보안장비와 기기들은 과거 솔루션과 보안기기 상의 보안정책이 별도로 도입되었으며, 이러한 도입과 구축으로 인한 서비스 제공을 위한 대역폭의 저하를 가져오는 등의 문제점을 발생시켰다.

* *미 표준화(Non-Standardization)로 인한 문제점*
  - *동일 정책의 활용으로 서비스 통신 대역폭(Bandwidth) 저하*
  - *보안정책의 중복으로 관리 및 운영을 위한 정책 디자인의 효율성 저하*
  - *신규 보안 솔루션 또는 보안기기 도입시 전체 네트워크 디자인 재 구성*
  - *새로운 공격기법에 대한 대처기능과 기존 보안정책의 가용성 저하*
  - *관리차원의 인수인계 등의 정보공유 상의 상호 의사결정 장애 초래*
  - *솔루션간의 신뢰성(Reliability) 저하*
  - *보안기기간의 의존 및 신뢰(Trustability) 저하*
  - *침해로 인한 2차적인 방어정책 구현상의 복잡성으로 방어지연*

2.2 보안장비 운영에 따른 침해사례

네트워크 보안을 위한 장비와 솔루션 상에 최근 발생하는 침해현황은 지난 2010년 월간 침해사고 통계 요약 상의 2009년 총계 현황 대비 각 구분별 신고건수가 <표 1>과 같

〈표 1〉 보안부문 침해건수와 현황표

구분	2010년[기준 : 건]									
	1	2	3	4	5	6	7	8	9	10
Warm & Virus	932	1,302	1,085	1,315	1,751	1,674	1,609	1,405	1,507	1,621
Hacking	898	1,076	1,053	1,468	1,062	1,160	1,300	1,644	2,183	1,732
- Spam	154	317	222	431	285	169	556	666	889	549
- Phishing	78	106	116	102	95	77	66	50	56	54
- Simplicity Attack	232	230	345	396	404	411	404	423	310	265
- Hacking[etc]	223	233	267	227	132	136	155	323	424	381
- variation	211	190	103	312	146	367	119	182	504	438
Bot	0.6%	0.6%	0.7%	0.9%	0.8%	0.6%	0.5%	0.4%	0.4%	0.4%

은 현황을 보이고 있으며. 이중 네트워크 기반의 침해건수가 가장 일반적이다.

또한, 인터넷 침해사고 동향 자료에 따른 침해사례로는 지난 2010년 DDoS(Distributed Denial of Service attack) 공격을 기반으로 7.7 인터넷대란을 발생시킨 공격트래픽인 Cache-Control 지시자를 포함한 HTTP GET 요청에 따른 장애와 해당 공격 구성을 50:50의 비율로 구성한 사례가 있다[5].

침해를 목적으로 접근하는 빈도수가 가장 높은 취약점 공격 유형은 크게 Warm & Virus, Hacking이 있다. 이러한 침해현상은 인터넷이라는 불특정 다수가 접근하기 손쉬운 통신접근 방법이 존재하고 그 통신정보에 무분별하게 공개되어진 악성코드와 공격 Tool이 가장 큰 주요 원인이다[6][7][8].

3. 네트워크 인프라 구현을 통한 적용 장비와 정책 분석

네트워크 기반의 인프라를 구성하고 지속적인 운영을 위한 구현방안을 단일 네트워크 보안기기를 기반으로 정책들을 분류하는 ONSU-MF기법과 단일 보안기기로 다양한 보안방안을 구현하는 OSD-MD기법의 직렬과 병렬 형태를 각기 구성으로 구분함으로써 4가지의 네트워크 보안 인프라 구현을 위한 방법을 제안한다.

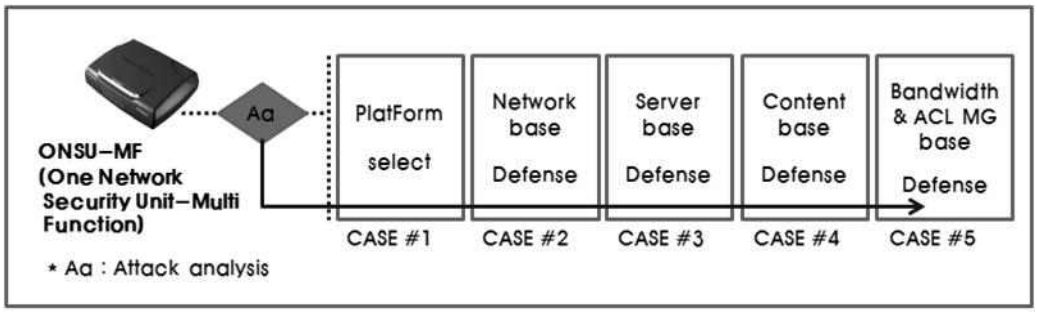
기존 방어를 위한 운영방식과의 차이점은 각 보안기기 또는 솔루션을 유기적으로 혼용하고 접근에 따른 신속하고 빠른 ONSU-MF 기법과 OSD-MD기법에 따라 종합적인 방어대책을 구성하는 것을 제안한다.

3.1 ONSU-MF와 OSD-MD기법분석과 제안

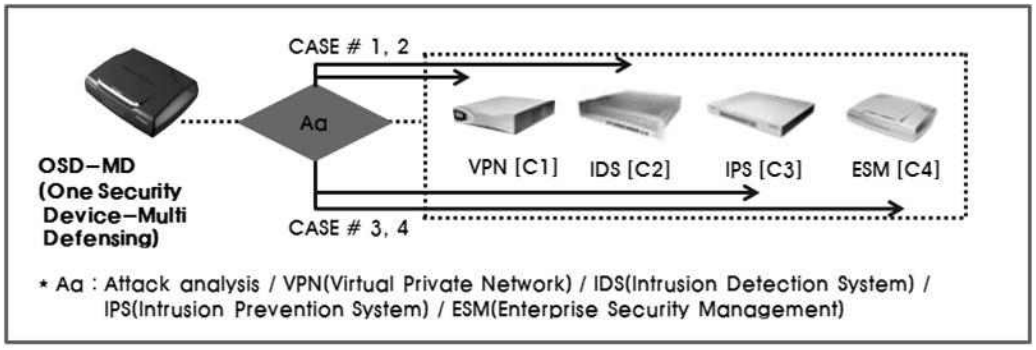
ONSU-MF 경우 단일 네트워크 통합 보안기기를 구축함으로써 (그림 1)과 같이 시스템 내의 장비가 선점하는 하드웨어 PlatForm을 구성하는 소스뿐만 아니라 보안정책 구현을 위한 기반 환경까지 실시간으로 외부에서 접근하는 Packet을 분석하고 동시에 적용 가능한 기법이다. 총 5가지의 환경 설정 변수 값을 CASE #1에서 CASE #5까지 구성한다. 따라서 최초 외부로부터 내부 네트워크 통합 보안기기로 접근 시에 능동적인 최종 대응 시스템 환경을 선택하고 방어한다.

** 환경 설정 변수 값 [공격수준에 따른 적용 변수선택]*

- *PlatForm select*
  ASIC Platform Bypass[yes] Segment 8,
  PC Platform Bypass[no] Segment 6,
  ASIC Platform Inline Applyance,
  Purpose-build platform Segment 8,
  Server Platform Inline Applyance
- *Network base Defense*
  BDoS, TCP - SYN Proxy, Critical based, No
- *Server base Defense*
  SYN Flood defense, SYN Proxy & Critical based, SYN cookie based



(그림 1) ONSU-MF 정의



(그림 2) OSD-MD 정의

- *Content base Defense*
  with AppXcel, BDoS(Signature), Available only on the FW/SSL VPN appliance, Stateful inpsection
- *Bandwidth & ACL MG base Defense*
  Yes, No

OSD-MD는 다소 ONSU-MF기법과 유사한 기능으로 판단할 소지가 있으나, 본 기법은 총 4가지의 환경 구성 보안기기를 구성하고 능동적인 최종 대응 시스템 환경을 선택하는 기법인 ONSU-MF기법과는 다르게 (그림 2)와 같이 장비단위로 침해 경우의 수를 구성한다.

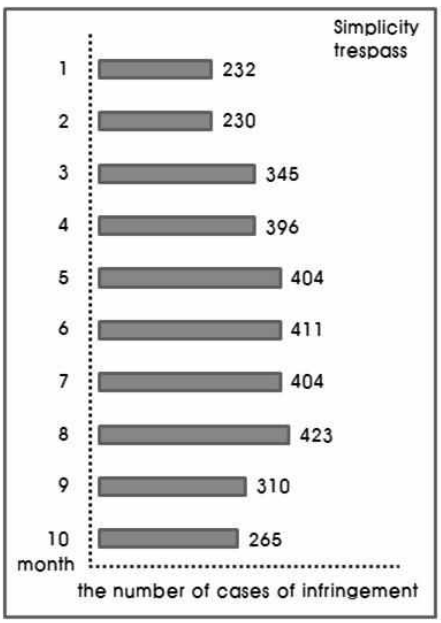
네트워크 보안환경을 유지하기 위한 방안으로 각 기기별 특화된 정책을 1:1에서 1:N까지 적용하는 기법이다.

ONSU-MF와 OSD-MD기법은 상호 보안환경에 필요한 취약점 공격과 실험 등을 통해 최적의 기법과 보안적용 우선순위를 선정함으로써 향후 새로운 보안기기 구축과 도입 및 구현하는 경우와 기존에 운영하던 보안기기를 종합적으로 관리하고자 하는 부문에 표준화 정보를 제공한다.

3.2 ONSU-MF기법과 OSD-MD기법 적용을 위한 침해사고 현황분석

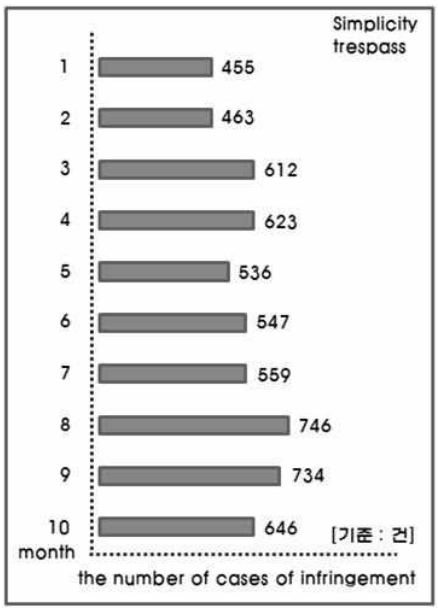
종합 보안운영 방안을 위한 표준화와 실험을 위한 기반구축을 위해 각 기법에 대한 네트워크 적용 시 발생 가능한 인프라 취약점을 분석한다.

(그림 3)은 2010년 월간 침해사고 통계 요약인 인터넷 침해사고 동향 및 분석 월보에 따른 단순 침입시도에 대한 침해건수를 나타낸 것으로 최종 공격에 의한 2차적인 진행형 공격은 아니며, 단순 접근을 통해 Port의 Bypass 기능을 통과하거나 이외의 다단계의 설정환경 하에서 1단계까지의 접근이 가능한 예시이다.



(그림 3) ONSU-MF 침해사례

(그림 4)의 경우 역시 2010년 월간 침해사고 통계요약인 인터넷 침해사고 동향 및 분석 월보 자료를 기준으로 그림 3과 비교할 때, 높은 침해사례 건수를 나타내고 있지만, 단순 침입시도와 이외의 해킹건수를 나타내고 있으며, 현재 보안시장의 다양한 기업과 기관들이 운영하는 보안기법이 침해건수 분석결과를 기준으로 OSD-MD기법과 유사한 정책의 보안기법들이 필요 및 적용되어지고 있다는 것을 나타낸 것이다. 따라서 향후 종합 보안기기 시스템 구성에 있어서 OSD-MD기법에 비중을 두고 연구해야함을 나타내는 현황표이다.



(그림 4) OSD-MD[VPN, IDS, IPS, ESM, SMS, NMS based] 침해사례

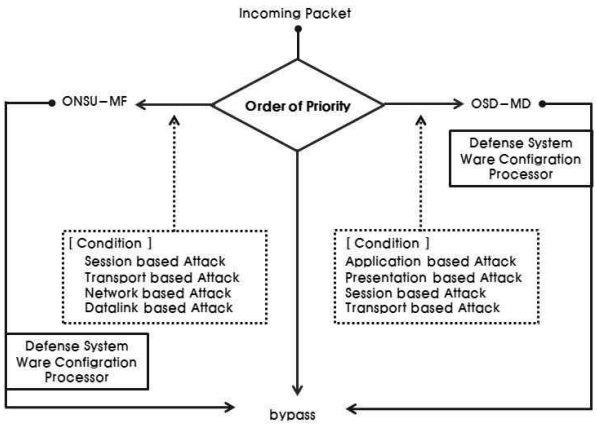
3.3 ONSU-MF와 OSD-MD기법 적용 우선순위 선정

두 가지 방어 기법 중 최초 유입되는 침입에 대한 우선순위를 선정하는 알고리즘을 (그림 5)와 같이 구현함으로써 어느 한 기법만을 구축하고 운영하는 방법에서 실시간 선정 알고리즘을 적용하는 통합 보안방식을 택했다.

선정방법은 OSI 7 계층을 기준으로 ONSU-MF기법은 Session 계층에서 하위 Data link 계층까지의 접근을 방어하는 종합 보안정책을 적용하고 OSD-MD기법은 Transport 계층 상위에서 Application 계층까지의 접근 방법을 차단하고 탐지하는 방법을 적용한다. 또한, TCP/IP 계층의 경우는 Network 계층을 기준으로 분리 적용한다.

** ONSU-MF 구현 알고리즘*
input packet
condition(packet_kind<ONSU-MF class(session, transport, network, datalink_layer_attack), branch ONSU-MF, branch OSD-MD
select1(platform)=ASIC Platform Bypass[yes] Segment 8,

PC Platform Bypass[no] Segment 6, ASIC Platform Inline Applyance, Purpose-build platform Segment 8, Server Platform Inline Applyance
select2(network base defense)=BDoS, TCP - SYN Proxy, Critical based, No
select3(server base defense)=SYN Flood defense, SYN Proxy & Critical based, SYN cookie based
select4(content base defense)=with AppXcel, BDoS(Signature), Available only on the FW/SSL VPN appliance, Stateful inpsection
select5(Bandwidth & ACL MG base defense)=Yes No
merge=select1||select2||select3||select4||select5
active merge
run merge



(그림 5) ONSU-MF와 OSD-MD기법 적용 우선순위 선정 알고리즘

** OSD-MD 구현 알고리즘*
input packet
condition(packet_kind<OSD-MD class(over application_layer_attack), branch OSD-MD, branch ONSU-MF
select1(VPN)=general VPN, SSL VPN, SSL VPN+[Web] Firewall
select2(IDS)=host based, network based, hybird, application based
select3(IPS)=virtual, general, real
select4(ESM)=user & policy manager, weakness & danger risk manager
select5(SMS.and.NMS)=select one module
merge=select1||select2||select3||select4||select5
active merge
run merge

3.4 최적화 종합 MF & MD 기법 분석

초기 네트워크를 통해서 유입되고 공격되어지는 침입형태를 분석하고 침해가능성을 파악함으로써 발생 가능한 방어기법의 한계치를 확인하는 등의 초기대응을 취한다.

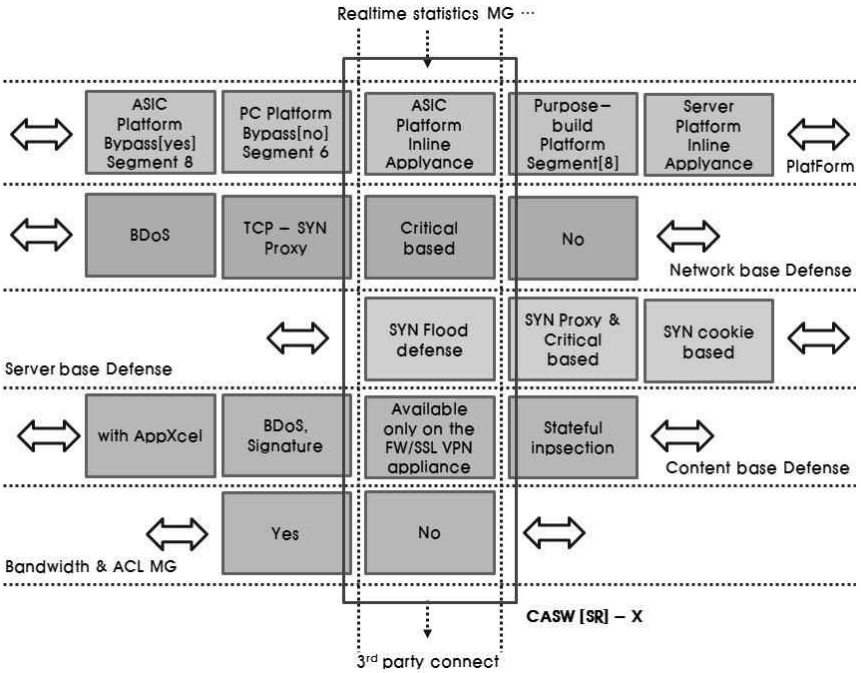
〈표 2〉 Attack 분석 프로세서

Unit	Influx packet capacity	Attack Kind	Excute
Access Packet Assaying	[A] 1 ~ 5G	[1] FlatForm	Operating Defense System Ware Configuration Processor
		[2] Network base	
		[3] Server base	
		[4] Content base	
		[5] Bandwidth & ACL MG	
	[B] 6 ~ 10G	[1] FlatForm	
		[2] Network base	
		[3] Server base	
		[4] Content base	
		[5] Bandwidth & ACL MG	
	[C] 11 ~ 15G	[1] FlatForm	
		[2] Network base	
		[3] Server base	
		[4] Content base	
		[5] Bandwidth & ACL MG	
	[D] 16G and over	[1] FlatForm	
		[2] Network base	
		[3] Server base	
		[4] Content base	
		[5] Bandwidth & ACL MG	

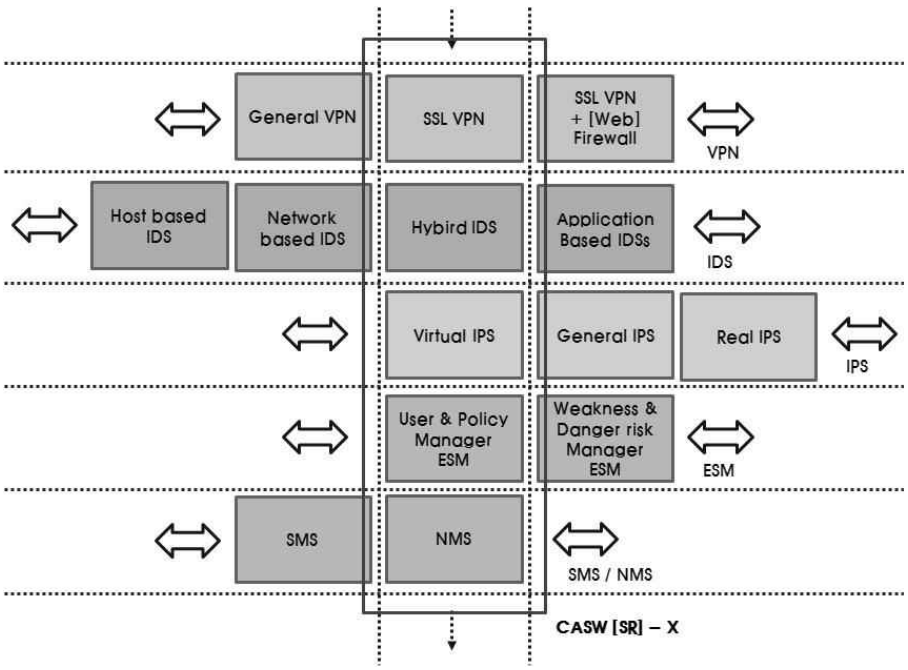
또한 최종 적용하기 위한 방어기법을 선정하는 사전조치 프로세서 운영 단계는 <표 2>와 같으며, 각 공격유형을 종류별로 Platform 기반, 네트워크 기반, 서버 기반, 콘텐츠 기반 등으로 구분하는 프로세서를 구현한다. 유입되는 통신량의 대역폭을 확인하고 대역폭 점유 량에 따라 ONSU-MF기법의 정책에 따른 능동적이고 실시간적인 방어형태를 선정한다.

종합 MF & MD 기법은 3단계의 방어 프로세서를 운영하는데, 1단계는 ONSU-MF기법의 Attack 분석 프로세서를 적용해서 침해 접근을 분류하고 2단계는 (그림 6)과 (그림 7)과 같은 선택적 프로세서 중 1단계의 침해 접근 분류 결과에 따른 ONSU-MF기법의 DSW(Defense System Ware) 환경설정 프로세서 또는 OSD-MD기법의 Defense System Ware 환경설정 프로세서를 선정하는 단계로 나누어진다.

마지막으로 해당 접근정보가 원하는 네트워크 인프라 접근권에 대한 허용단계로 운영된다. 각각의 기법을 개별적으로 적용하는 단계와는 달리 두 가지 큰 부류의 기법을 상호



(그림 6) ONSU-MF기법의 Defense System Ware 환경설정 프로세서



(그림 7) OSD-MD기법의 Defense System Ware 환경설정 프로세서

연계하여 적용함으로써 각 방어기법에서 침해 가능한 정책 또는 보안기기의 문제점을 상호보완 한다.

또한, 각 기법에 존재하는 두 가지 경우의 수인 직렬 또는 병렬구현을 2단계 내부 서브 프로세서로 운영함으로써 침해비율을 최소화 한다.

ONSU-MF기법은 PlatForm 기반의 분류를 포함한 5가지 정책반영 형태를 갖고 있으며, 접근하는 침해분류를 기준으로 (그림 6)과 같이 각 정책들이 최초 공격성 침해 유입과 함께 단계별로 적용 가능한 정책 등을 유기적으로 최상위 단계부터 한 단계씩 적용함으로써 최종 방어 프로세스 구현을 하는 프로세서이다.

따라서 해당 프로세서를 이용한 방어정책 구현 프로세서의 예를 들면, 침해가 발생함과 동시에 Platform 기반의 ASIC Flatform Inline Applyance, 네트워크 방어 기반의 Critical based, 서버 방어 기반의 SYN Flood defense, 콘텐츠 방어 기반의 Available only on the FW/SSL VPN appliance, Bandwidth & ACL MG 활용 유무 등이 단계별로 분석된 침해공격의 성향에 따라 구성 및 융합되고 최종 방어 솔루션을 구현한다.

OSD-MD기법 또한 (그림 7)과 같이 각 보안기기 들이 유동적으로 선정되는 지능적인 프로세서이며, 활용되어지는 예로는 최초 불법적인 접근이 감지됨과 동시에 SSL VPN, Hybird IDS, Virtual IPS, User & Policy Manager ESM, NMS가 일시적, 단계적으로 분석된 공격의 성향에 따라 구성되고 혼용되어 최종 방어 기기를 구현한다.

최적화 종합 MF & MD기법을 분석하고 적용한 이후의 최종 보고서는 (그림 8)과 같은 형태로 다양한 공격 패턴을 인지하고 적용되어진 정책과 솔루션 정보를 Case 별로 지속적으로 정보화하고 축적함으로써 향후 동일한 패턴의 공격성향을 가진 불법적인 접근 정보가 인지되는 시점에 과거 해당 방어정책과 솔루션이 정의되어진 표준화 보고서를 관리자에게 통보하고 축적되어진 데이터베이스로부터 해당 방어정보를 축출 및 방어기법에 재적용하기 위한 논리적인 최적화된 표준 보안기법에 대한 지속적인 연구방향을 제시하고 있다.

4. ONSU-MF와 OSD-MD기법 분석과 보안정책 구현 실험결과

많은 기관과 기업들이 두 가지 형태의 방어 기법 표준화를 통한 구현보다는 (그림 9)와 같이 한시적인 방어를 위한 방안을 선택한다.

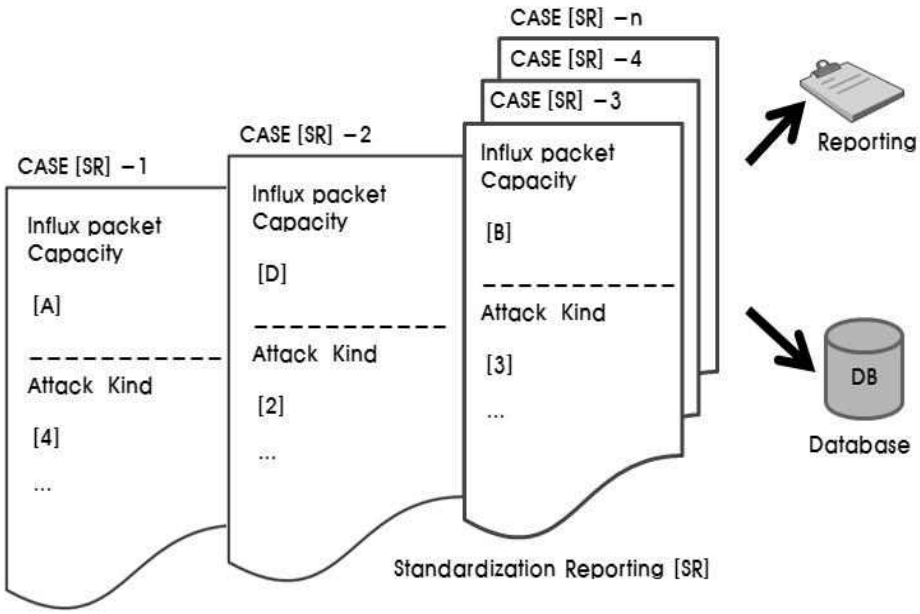
종합적인 방어 기획에서부터 과거와 현재까지의 수많은 공격패턴에 대한 정보를 기반으로 데이터베이스 구축 후 활용하는 등의 지속적인 보안정보 유지가 이루어지는 형태를 선택해야 한다.

또한, 공격에 의한 사회적인 문제점 도출 등이 발생시에 각각의 보안 솔루션과 보안기기들을 별도로 단일 모듈형태로 도입하는 과정이 반복적으로 이루어지고 있다.

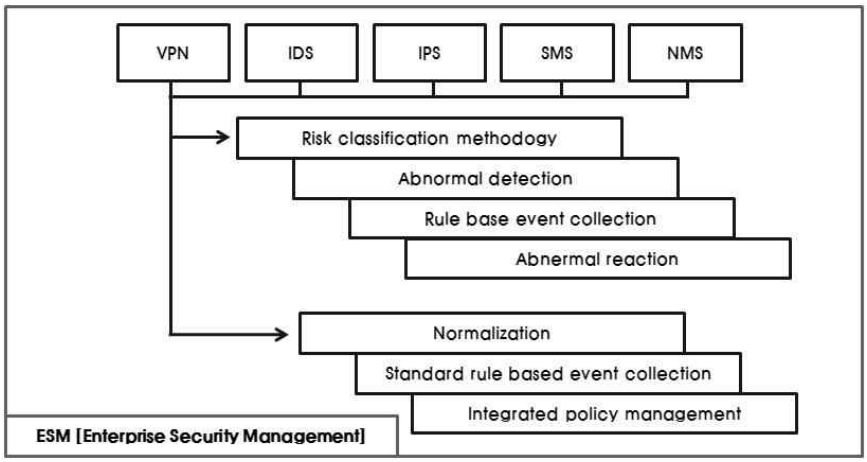
따라서 최종 구성되어진 방어관리를 위한 네트워크 보안 형태가 일정치 않고 다수의 정책과 솔루션 사이에서 공격성 취약점이 발생 가능하므로 본 논문에서는 ONSU-MF와 OSD-MD 두 가지 기법에 대한 최적화 표준 보안기법을 실험한 결과를 제안한다.

4.1 실험환경

보안정책과 기기들을 제안한 두 가지 보안기법으로 물리적으로 구성하고 해당 알고리즘을 탑재한 시스템을 구현함으로써 실험환경을 만든다. 공격 시스템은 Linux기반의 CentOS를 탑재한 데스크탑으로 구성하고 공격 툴은 TCP,

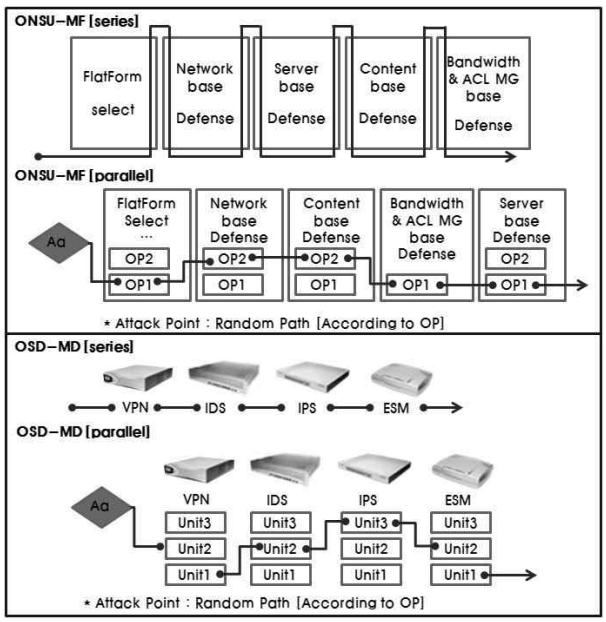


(그림 8) Attack 분석 프로세서 & Defense System Ware 환경설정 프로세서 운영결과



(그림 9) 최근 ONSU-MF기법과 OSD-MD기법 기반의 보안장비 운영현황

UDP, ICMP Flooding 공격 툴인 Flowalyzer Ver. 2.0을 이용한다. 구성된 공격환경에 실험결과를 확인하기 위한 방어기법으로는 (그림 10)과 같이 단순 반복형 공격을 ONSU-MF series, ONSU-MF parallel, OSD-MD series, OSD-MD parallel의 4가지 경우에 따라 공격을 시행함으로써 ONSU-MF와 OSD-MD 방어기법을 반복적용 하는 series 형태와 일시에 적용하는 parallel 형태의 경우로 구분하여, 최종 실험결과를 도출한다. 이번 실험에서는 최초 침입에 대한 병렬 및 직렬 기반의 기법 적용 결과와 보안정책 적용에 따른 구현 결과를 확인한다.



(그림 10) 실험환경

4.2 병렬 및 직렬 기반의 기법 적용 결과분석

현재 운영 중인 보안 네트워크 인프라 기반 하에서 ONSU-MF기법과 OSD-MD기법을 실험함으로써 단순 기법 적용에 따른 방어 비율을 구성하는 부문에서 나아가 직렬 구성과 병렬 구성 형태로 서브 프로세서를 구성하는 단계까지 실험했다.

두 가지 대분류에 하위 각각 서브 분류 기반의 구현에 따른 정책반영 비율, 적정방어 비율 등 각 4가지 기준분류표에 의한 실험결과를 통한 방어기법에 따른 결과는 <표 3>과 같다.

4.3 보안정책 적용에 따른 구현 분석 결과

본 제안과 표준화에서 언급되어진 ONSU-MF기법과 OSD-MD기법으로 방어기법을 분류하기 이전의 보안기기와 정책적용의 경우는 표준화된 네트워크 보안 인프라보다는 단계적인 방어를 위한 구현이 이루어졌기 때문에 각 종 네트워크 인프라 상황을 고려하면, <표 4>와 같이 도입 후 적용되어지는 우선순위를 확인할 수 있다.

ONSU-MF와 OSD-MD기법과 유사한 형태의 기법들이 다양한 경우에 적용되고 있으나, 가장 우선시 해야할 부분인 표준화가 없이 도입과 구현이 이루어지고 있다.

따라서 최종 결과 분석 후 향후 보안정책 적용을 위한 구현시 반드시 확인해야 되는 방어기법 적용 우선순위를 제시함으로써 ONSU-MF와 OSD-MD기법 별로 활용되어지는 순위는 각각 단계별 직렬형태로 구현하는 series 형태가 주를 이룬다.

ONSU-MF기법과 OSD-MD기법의 정책반영 비율과 접근 비율 대비 결과를 기준으로 최종 방어기법 적용시 최적화 방어기법으로 구현하는 기준은 OSD-MD기법의 parallel을 기준으로 ONSU-MF기법의 series 순으로 적용 표준화 우선순위가 <표 5>와 같은 결과를 나타냈다. OSD-MD기법의 parallel 형태를 적용함으로써 가장 최적의 방어형태를 구현한다.

또한, 최종 보안정책 적용에 따른 구현 분석 결과는 (그림 11)과 같이 도출되었으며, 방어기법 적용비율을 OSD-MD기법의 parallel 형태를 적용함으로써 침해비율이 저하되고 침해로 인한 정상적인 서비스 제공에 대한 장애가 현저히 낮아진 결과가 나타났다.

〈표 3〉 ONSU-MF기법과 OSD-MD기법의 서브 기법처리 결과

No	Unit		Appreciation directing	Result's
A1	ONSu-MF	series	정책(Function) 반영 비율	100%
A2			방어 정책(Function) 실행 가능 비율	접근 비율대비 67%
A3			적정방어 비율	60%
A4			침해비율	1 ~ 40% 가능
B1		parallel	정책(Function) 반영 비율	100%
B2			방어 정책(Function) 실행 가능 비율	접근 비율대비 95%
B3			적정방어 비율	92%
B4			침해비율	1 ~ 8%
C1	OSD-MD	series	정책(Function) 반영 비율	100%
C2			방어 정책(Function) 실행 가능 비율	접근 비율대비 89%
C3			적정방어 비율	84%
C4			침해비율	1 ~ 12%
D1		parallel	정책(Function) 반영 비율	100%
D2			방어 정책(Function) 실행 가능 비율	접근 비율대비 99%
D3			적정방어 비율	98%
D4			침해비율	1 ~ 2%

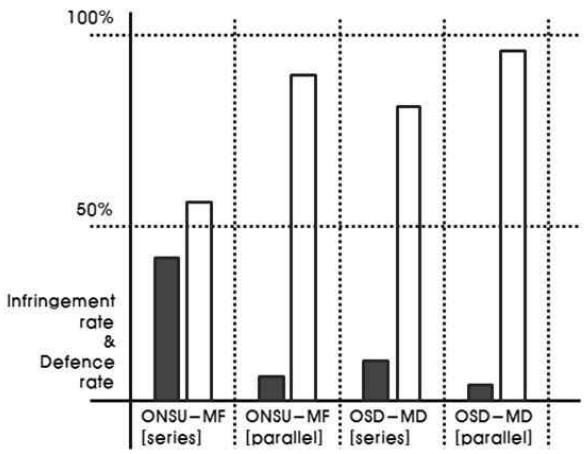
〈표 4〉 과거 적용 우선순위

구분	ONSU-MF		OSD-MD	
	series	parallel	series	parallel
우선[선택]순위	2	1	2	1

〈표 5〉 종합 적용 우선순위

구분	ONSU-MF		OSD-MD	
	series	parallel	series	parallel
우선[선택]순위	4	2	3	1

이러한 결과는 향후 지속적인 보안 솔루션과 기기를 도입하고 구현하는 부문에 있어서 네트워크 인프라 신규 디자인과 재디자인하는 부분에 최적의 보안 인프라 구현을 위한 지표로써 활용되어 질 것이다.



(그림 11) 보안정책 적용에 따른 구현 분석 결과

5. 결 론

본 논문에서는 보안기기 탑재 보안정책을 선정하는 방어기법과 각각의 방어 특성을 가진 보안기기를 활용하는 통합 보안기법을 제시했다. 또한, 논리적으로 각각의 방법론에 대한 우선적용 순위와 최초 유입되는 침해 유형에 따른 개별 또는 종합적인 병합 기반의 방어에 대해서도 논했다.

최종 실험을 기반으로 4가지 경우의 방어 기법을 구현함으로써 보안정책 적용에 따른 구현 분석 결과를 도출했으며, 향후 연구방향으로는 개발 가능한 다양한 보안기기와 탑재 정책을 지속적으로 분류하고 본 논문에서 제시하고 실험한 기법에 적용시켜 물리적으로 최종 누적된 방어결과를 기반으로 ONSU-MF기법과 OSD-MD기법을 보다 구체적으로 표준화 시켜야 한다.

논리적인 부문도 표준화를 위해 더욱 다양한 실험환경을 제시하고 실험결과를 통해 방어의 효율성 증대를 위한 최적의 기법을 표준화하는 필요성과 보안 방어 학습패턴에 대한 빠른 적용모듈을 지원하는 솔루션 역시 지속적인 연구가 필요하다.

참 고 문 헌

[1] Rahul Kumar, Rahul Karanam and Rahul Chowdary Bobba, Raghunath. S, "DDOS DEFENCE MECHANISM", IEEE computer society-2009 International Conference on Future Networks, pp.245-257, 2009.

[2] Hoon Ko and Carlos Ramos, "A Study on Security Framework for Ambient Intelligence Environment", IEEE computer society-2009 Fifth International Conference on Wireless and Mobile Communications, pp.93-98, 2009.

[3] Young-Hwan Cha and Hae-Sool Yang, "Development of Security Evaluate Model and Test Methodology of Enterprise Security Manageent (ESM) Product", The Journal of the Korea Contents Association, Vol.10, No.6, pp.156-165, 2010.

[4] Walter Wong and Pekka Nikander, "Secure Naming in Information-centric Networks", Association for Computing Machinery, 2010.

[5] 인터넷침해대응센터, "인터넷 침해사고 동향 및 분석 월보", 2010년 10월호, pp.2, pp.30, 2010. 10.

[6] Sourav Kumar Dandapat, Bivas Mitraand Niloy Ganguly, Romit Roy Choudhury, "Fair Bandwidth Allocation in Wireless Network Using Max-Flow", Association for Computing Machinery, pp.407-408, 2010.

[7] Zhen YE, Weiwei SHI and Dayong YE, "DDoS Defense Using TCP_IP Header Analysis and Proactive Tests", IEEE computer society-2009 International Conference on Information Technology and Computer Science, pp.548-552, 2009.

[8] Woo-Sung Chun and Dea-Woo Park, "A Study on N-IDS Detection and Packet Analysis regarding a DoS attack", Journal of the Korea society of computer and information, Vol.13, No.6, pp.217-224, 2008.

서 우 석

e-mail : ssws2003@yahoo.co.kr
2006년 숭실대학교 정보과학대학원 정보통신 융합학과(공학석사)
2009년~현 재 숭실대학교 컴퓨터학과 박사과정
관심분야 : 정보보호, 네트워크 보안, 방화벽, Router & Network Design 등

이 규 안

e-mail : leegyuan@hotmail.com
2000년 벽성대학 정보통신과 겸임교수
2006년 숭실대학교 정보과학대학원 (공학석사)
2010년 숭실대학교(공학박사)
2002년 대검찰청 중앙수사부 컴퓨터수사과 근무
2007년 대검찰청 디지털수사담당관실 근무
2011년 서울중앙지방검찰청 첨단범죄수사2부 근무
관심분야 : 유비쿼터스보안, 디지털포렌식, 해상디지털포렌식, 이동통신보안

전 문 석

e-mail : ijcsns@gmail.com
1981년 숭실대학교 전자계산학과(학사)
1986년 University of Maryland Computer Science(석사)
1989년 University of Maryland Computer Science(박사)
1986년~1989년 University of Mary 강사
1989년 Morgan State University 조교수
1989년~1991년 New Mexico State University Physical Science Lab. 책임연구원
1991년~현 재 숭실대학교 컴퓨터학부 정교수
관심분야 : 정보보호, 네트워크 보안, 전자여권, 암호학