Diskless와 Stateless 보안정책 기반의 고속화 동기 네트워크 인프라 구현에 관한 연구

서우석* · 전문석**

A Study on the Realization of Diskless and Stateless Security Policy Based High-speed Synchronous Network Infrastructure

Woo-Seok Seo* · Moon-Seog Jun**

요 약

2011년 네트워크 정보 서비스 분야 중 많은 보안 기술이 접목되고 보안 정책들을 필요로 하는 서비스 중 Cloud Computing의 하드웨어 플랫폼 서비스인 Infrastructure as a Service가 제공되고 있다. 기존 중앙 집중화 방식 서비스와 제공되는 하드웨어 범주에 대한 사양과 기술적인 부분이 다소 유사하지만, 특정한 네트워크라는 공간적 제한사항을 벗어나 공중망을 대상으로 서비스를 한다는 가장 큰 차이점이 있다. 정보보안 기술 역시 제공 되어지는 하드웨어 플랫폼의 안정성을 확보하기 위한 기술로 동반성장하고 있다. 현재 지원되는 하드웨어의 경우는 Internet Data Center가 기존에 제공하던 서버, 디스크(백업 디스크) 등을 가상화함으로써 공급되고 제공되고 있으며, 서비스되는 하드웨어 플랫폼이 다소 한정적이다. 물론 제공되는 서비스에 대한 보안부문의 영역도 Center내에 국한되거나 클라이언트와의 연결 공중망에 대한 TCP/IP 기반의 SSL(Secure Sockets Layer) 등으로 미시적인 접속보안 정책이 이용되고 있다. 따라서 본 논문에서 서비스 영역을 보안장비로 확대하고 Diskless와 Stateless 보안정책 기반의 고속화 동기 네트워크 인프라를 제안함으로써 방어정책 구현을 위한 현실적인 보안기법을 제공하고자 한다.

ABSTRACT

Among the network information services combined with a number of security technologies and required security policies, Infrastructure as a Service, a hardware plat-form service of Cloud Computing, has been provided since 2011. It is more or less similar to the existing central concentration method services, in terms of the specifications and technical aspects for given hardware category, but it is entirely different from them in that it overcomes the spatial limitations of specific network and targets the public network. Information security technology has also been prospering so that it could ensure the stability of offered hardware plat-forms. As currently supported hardware, Internet Data Center has been provided by virtualizing the previously offered servers and discs (backup discs), but the hardware plat-forms offered are somewhat limited. Meanwhile, the areas of security fields for offered services are confined to the center or include the TCP/IP-based SSL (Secure Sockets Layer) for the public network connected with clients, which shows that microscopic access security policies have been used. Therefore, this study was aimed to provide a realistic security mechanism for realizing defense policy, by expanding service areas into security devices and suggesting Diskless and Stateless security policy based high-speed synchronous network infrastructure.

키워드

Diskless & Stateless SP, High-speed SNI, Iaas
Diskless & Stateless 보안정책, 고속화 동기 네트워크 인프라, 인프라 자원 서비스

* 숭실대학교 일반대학원 컴퓨터학과(ssws2003@yahoo.co.kr), ** 교신저자 : 숭실대학교 정교수(ijcsns@gmail.com)
접수일자 : 2011. 08. 22 심사(수정)일자 : 2011. 09. 23 게재확정일자 : 2011. 10. 12

Ⅰ. 서 론

과거 공개되어진 공중망은 단순한 콘텐츠와 같은 페이퍼 자료들을 공유하거나 상호 교환하는 등의 정보교류의 장이었으나, 2011년 현재는 다양한 기능과 기술 그리고 특정 목적과 결과도출을 위한 정보의 흐름을 보인다. 이는 정보의 홍수라는 표현으로도 쓰여질 수 있을 만큼 엄청난 정보와 자료, 데이터가 잠깐의 서핑으로도 공개되어지고 출력되어 질 수 있음을 의미한다.

즉, 정보보호에 대한 관심과 보호를 위한 제반기술과 기능이 한층 부각되고 공중망에 적용되어지고 운영된 시점이 불과 몇 년밖에 되지 않았음을 의미하기도 한다. 따라서 과거에 페이퍼 자료로써 공중망에 배포되고 올려 졌던 정보가 재생산되고 가공됨으로 인해서 개인정보가 유출되는 현상 등의 장애를 유발하고 있다.

이러한 보안상의 장애와 침해를 차단하기 위한 다양한 기술로써 Firewall, VPN(Virtual Private Network), IDS(Intrusion Detection System), IPS(Intrusion Prevention System), ESM(Enterprise Security Management) 등 침해공격에 대한 방어목적으로 구축되고 운영되어지고 있으나, 소규모 네트워크를 구성하고 운영하는 사이트의 경우에는 다양한 보안장비를 모두 도입하고 정책을 구현하기에 경제적인 부분이 문제가 되고 있다.

따라서 본 논문에서는 공중망을 이용해 제공되고 서비스 되는 네트워크 보안장비들에 대한 보안정책과 운영기술 및 기능을 불법적인 공격으로 인한 침해를 받을 수 있는 다양한 클라이언트 서비스 이용 사이트에서 실시간으로 Diskless 보안정책과 Stateless 보안정책 기반의 고속화 동기 네트워크 보안 인프라 서비스를 제공함으로써 보안 효율성과 안정성, 경제성을 확보하고자 한다.

본 논문의 구성은 2장에서는 네트워크 접근 침해기관 및 운영체제 침해현황, 보안관제 기업용 네트워크 장비 분야별 운영현황 및 Cloud Computing의 하드웨어 플랫폼 서비스 보안적용 현황에 대해 분석하고, 3장에서는 고속화 동기 네트워크 인프라 기반의 침입 방어 기법 제안에 대해 설명하며, 4장에서는 제안한 네트워크 인프라를 실험하고 결과를 도출한다. 마지막으로 5장에서는 논문의 결론과 향후 연구 과제를 제시한다.

Ⅱ. 관련연구

2.1 네트워크 접근 침해기관 및 운영체제 침해현황

2009년 7.7 DDoS(Distributed Denial of Service attack) 인터넷 대란을 겪으면서 보안시장은 급속도로 발전했으며, 2011년 3월에는 개인정보보호를 위한 법률적인 토대를 마련하기도 했다. 또한 2011년 9월 30일자로 오랜 시간동안 진통을 겪은 정보보호법이 시행된다. 이처럼 단계적으로 정보보호에 대한 인식과 변화를 추구함에도 불구하고 2011년 8월에는 콘텐츠 커뮤니케이션을 주도하는 사이트가 사상 최대 규모의 해킹사고가 발생했고 이어 국내 글로벌 IT분야 기업에서도 불법적인 접근을 통한 해킹으로 35만 명의 개인정보가 유출됐다[1].

공격성향은 불특정 다수를 대상으로 하는 공격에서 개인, 대학, 연구소 등과 같이 공격범위가 한정되지 않고 또한 제한되지 않음을 표 1에서와 같이 최근 6개월 이전의 공격 기관별 분류현황에서 확인할 수 있다. 이는 정보를 얻기 위한 목적을 위해서라면, 어떠한 기관과 기업도 공격의 대상에서 벗어나지 못함을 나타낸다[2].

표 1. 네트워크 접근 가능 기관 해킹사고 피해 기관별 분류 현황

Table 1. Summary of classifying hacking accidents in organizations with possible network accessibility by victimized organization

기관	2011년						
	1월	2월	3월	4월	5월	6월	합계
개인	615	480	619	641	708	588	3,651
기업	392	358	356	338	328	343	2,115
대학	8	8	21	15	24	21	97
비영리	10	8	6	5	1	4	34
연구소	0	0	0	0	0	1	1
총계	1,025	854	1,002	999	1,061	957	5,898

각 기관의 피해와 침해 분류현황 확인은 향후 정보보안에 대한 기술부분에서 방어 등급을 향상시키고 더욱 연구해야하는 분야이며, 표 2는 한국인터넷진흥원 인터넷침해대응센터의 인터넷 침해사고 동향 및 분석 월보를 참조한 자료로써 어떠한 운영체제를 이용하는 기관들이 침해를 당했는지 확인하는 중요한 불법

접근 차단을 위한 Key가 된다[2].

운영체제 침해사고 분류현황을 분석해보면, 가장 많은 보안정책과 기술이 적용되는 운영체제임에도 불구하고 침해를 당하고 있는 것을 확인할 수 있다[3].

표 2. 네트워크 서비스 운영 서버별 탑재 운영체제 해킹사고 피해 분류 현황
Table 2. Summary of classifying the damage of hacking accidents occurring in mounted operating systems by network service operation server

기관	2011년						
	1월	2월	3월	4월	5월	6월	합계
Windows	733	602	711	734	853	678	4,311
Linux	167	136	133	89	85	85	695
Solaris	2	0	11	0	0	0	13
Etc	123	116	147	176	123	194	879
합계	1,025	854	1,002	999	1,061	957	5,898

2.2 보안관제 기업용 네트워크 장비 분야별 운영현황

2011년 보안기기와 솔루션 등의 많은 보안부분에 대한 인프라와 인력 투자를 아낌없이 제공하고 보안기반 시설에 대한 새로운 인식의 변화로 인한 구축과 구현을 많은 기업과 기관들이 서로 앞 다투어 구축하고 있다. 하지만 금년 8월에도 대규모 커뮤니티 사이트가 해킹에 따른 개인정보의 유출과 같은 사고들이 빈번히 발생하고 있다.

표 3은 세계적으로 네트워크 장비의 분야별 운영과 적용되어 활용되고 있는 장비를 확인하고 향후 지속적인 정보보안을 구현하고 개발하기 위한 방향선정에 도움이 되는 장비별 운영 증가율을 나타낸다. Application Acceleration Equipment로부터 SSL VPN Equipment에 이르기까지 총 6가지 구분자를 두고 2009년부터 2010년까지의 네트워크 장비 운영 비중을 확인했다[4][5[6]].

표 3. 네트워크 장비별 세계적인 분야별 운영과 적용, 활용현황
Table 3. Summary of operation, application and utilization by network device and by globally used field

구분	2009년	2010년	전년대비 증가율[%]	비중 (2010)[%]
Application Acceleration Equipment	2,235	2,964	32.6	8.1
Enterprise Ethernet Switches	16,065	20,321	26.5	55.3
Enterprise WAN Edge Equipment	7,842	8,854	12.9	24.1
Enterprise Wireless LAN Equipment	1,967	2,517	27.9	6.8
IPS Equipment	1,204	1,447	20.2	3.9
SSL VPN Equipment	583	651	11.7	1.8

* 단위 : 백만 달러 / 자료 : Gartner(2011b) - www.gartner.com [1)]

2.3 Cloud Computing의 하드웨어 플랫폼 서비스 보안적용 현황

본 논문에서 제시하는 기술과 유사한 개념을 가진 Cloud Computing은 Diskless와 Stateless 기능을 기본적으로 수용하고 있으면서, 현재 가장 많은 온라인상에 소프트웨어 플랫폼과 하드웨어 플랫폼을 제공하는 서비스 형태이다.

따라서 정보보안을 위한 기술과 기능이 필요한 분야로 대두되고 있다. 그러나 온라인상에서 지원되는 서비스에 대한 관리자들의 인식은 다소 부정적임을 단편적으로 나타낸다. 사용자의 입장에서는 장소 및 시간에 제약을 받지 않는 서비스인 Cloud Computing에 매료되어 기하급수적으로 서비스 영역과 사용비율이 증가하고 있으나, 관리자들은 해당 서비스의 정보보안을 위한 인프라 재점검과 안정성을 확보하기 위한 솔루션 개발에 전력을 다하고 있다.

표 4는 Cloud Computing 서비스에 대한 보안의식을 비율로써 표현하고 있다[7][8].

표 4. Cloud Computing의 보안서비스 적용 현황
Table 4. Summary of applying security services of Cloud Computing

구분	미국[%]	유럽[%]
My organization views the security of our cloud service as a competitive advantage	19	18

1) 참고문헌 [5]의 참고자료 상의 원본 출처명기

My organization's cloud services substantially protect and secure the confidential or sensitive information of our customers	27	25
My organization considers cloud computing security as one of our most important responsibilities	25	30

* 출처 : KISA(한국인터넷진흥원) 2)

III. 고속화 동기 네트워크 인프라 기반의 침입 방어 기법 제안

본 논문에서 제안하는 Diskless 보안정책 기반의 네트워크 인프라와 Stateless 보안정책 기반의 네트워크를 단계별로 해석하고 공격에 대한 방어를 정의한다. 또한 최종 실험과 제안 방어기법인 Diskless와 Stateless를 융합한 고속화 동기 네트워크 인프라를 활용해서 공격에 대한 방어기법을 재해석하고 각 기능과 솔루션을 속성별로 정의하고 확인한다.

3.1 네트워크 접근 침해기관 및 운영체제 침해현황

제안하는 보안정책 기법의 첫 번째 단계인 Diskless 네트워크 보안 정책 기반에 대한 공격과 방어 처리는 그림 1과 같이 다양한 네트워크 인프라를 대상으로 하는 VPN, IDS, IPS, Firewall 장비를 최초 네트워크 패킷 유입 경로에 설치하고 이후 각 장비에 대한 어떠한 보안정책도 장비 내에 저장하는 등의 일련의 보안정책 업로드를 포함한 S-POST(Security-Power On Self Test) 과정을 시행하지 않고 Load-Balancing System내에 존재하는 Disk를 1:1로 매칭 시켜 정책 탑재 하드웨어 플랫폼을 할당한다.

이후 할당된 하드웨어 플랫폼인 RAM Disk 또는 Solid State Drive를 네트워크 보안장비의 보안정책과 방어 솔루션이 탑재되는 저장 공간으로 구성하고 동기화시킴으로써 침해에 따른 네트워크 보안장비 상에 탑재된 정책이 파기되어도 재설정이 가능하도록 설정값 구성 테이블을 두고 정책의 인위적인 변경이 발생시 재설정되는 과정이 발생하도록 구성하여, 피해 방어를 위한 기본적인 하드웨어 플랫폼을 구성한다.

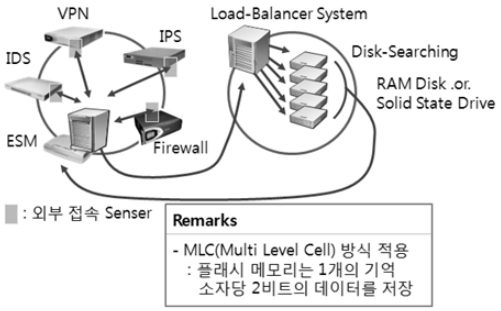

그림 1. Diskless Hardware Plat-Form 기반의 네트워크 보안기기 운영
Fig. 1 Operation of Diskless Hardware Plat-Form Based Network Security Devices

3.2 Stateless 네트워크 보안 Tool을 이용한 공격 방어

각각의 네트워크 보안장비별 고속화 동기 하드웨어 플랫폼을 연결한 이후에 적용되어지는 방어기법으로 Base Security Policy System에 의해 불법적인 접근을 기록하고 데이터베이스화함으로써 향후 동일 접근 또는 제3의 변형된, 유사한 접근이 발생 시에 Case by Case로 고속화 하드웨어 플랫폼에 탑재하게 되는 보안정책에 대한 방어기법이다.

다양한 경우의 수가 존재하지만 침해정보를 주기적으로 저장하고 데이터베이스화함으로써 패턴을 정의하고 각 정의된 패턴에 따른 보안정책의 경우 속성과 솔루션을 구성하고 이를 탑재 방어 및 재구성 탑재 방어하는 등의 방어정책을 그림 2와 같이 소프트웨어 플랫폼으로 구현한다.

이때에 Diskless 기법과 Stateless 기법을 안정적으로 빠르게 동기화함에 따라 본 제안 방어기법의 성능과 효율성 비율이 정해진다. 또한 각 네트워크 장비에는 S-POST 과정을 통해서 각 장비가 갖는 특유의 방어정책에 대한 기본적인 기능을 탑재하는 것을 1단계로 구성한다. 예를 들어 VPN 같은 경우 최초 장비 초기화와 함께 기본적인 Network Transfer Line Access Control이 탑재되고 향후 Case 별 추가 보안정책 탑재를 순차적으로 진행한다.

2) 참고문헌 [7]의 참고자료 상의 원본 출처명기

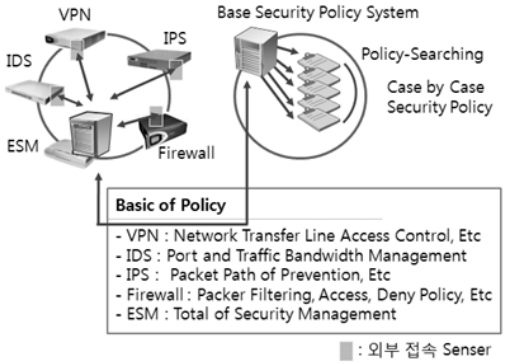

그림 2. Stateless Software Plat-Form 기반의 네트워크 보안정책 운영

Fig. 2 Operation of Stateless Software Plat-Form Based Network Security Policy

3.3 Diskless와 Stateless 기반의 하이브리드 융합 고속화 동기 네트워크 인프라를 활용한 공격 방어

Diskless와 Stateless 방어기법을 순차적으로 적용함으로써 하이브리드 형태로 첫 번째 융합 고속화 하드웨어 플랫폼 기반을 구성하고 두 번째로는 보안정책에 대한 탑재과정인 소프트웨어 플랫폼을 적용하는 최종 정보보안을 위한 네트워크 인프라의 적정성과 방어형태를 확인한다.

고속화 기반 기술을 적용하는 방어기법으로 고속화 기반 기술은 최초 외부 공격성 패킷 접근에 따른 Fusion-Process Algorithm 구성으로 하드웨어 기반의 Disk 상의 Case by Case 보안정책을 고속으로 보안기기의 Flash Memory 탑재와 구성을 통한 방어하는 방법이다.

또한, 그림 3과 같이 순차적인 방어단계는 1단계로는 각 보안기기의 Flash Memory 상에 가장 기본적인 방어정책 운영하고 2단계에서는 접근 패킷의 성향 또는 공격성에 따라 Flash Memory의 보안정책을 사용할 것인가를 판단한다.

다음으로 3단계와 4단계는 일반적인 접근과 공격성 접근으로 구분해서 Flash Memory 보안정책 적용과 Load-Balancer System Algorithm과 Base Security Policy System Algorithm, Fusion-Process Algorithm을 적용하는 단계로 구성함으로써 최종 방어를 구현하는 방안이다.

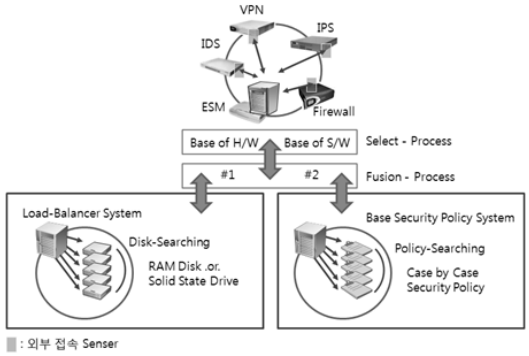

그림 3. Diskless H/W와 Stateless S/W Plat-Form 융합기반의 네트워크 보안정책 운영

Fig. 3 Operation, suggestion and experimental environments of Diskless H/W and Stateless Operation of S/W Plat-Form fusion-based network security policies

Ⅳ. 동기 네트워크 인프라 방어 기법에 대한 공격과 방어

본 논문에서 최종 제안하고자 하는 하이브리드 융합 고속화 동기 네트워크 인프라에 대한 제안사항에 따른 실험을 통해 고속화 동기 네트워크 인프라 환경을 확인하고 세부적인 솔루션 탑재와 적용을 위한 제안 알고리즘을 구성함으로써 현재 운영되는 방어 장비 또는 기법과 제안하는 기법과의 비교를 통한 결과를 도출한다.

4.1 제안과 실험환경 구성

제안되어진 실험환경을 그림 4와 같이 구성하고 공격을 감행하는 클라이언트를 외부 네트워크에 위치시킨다. 다양한 공격 실험보다는 대역폭을 대상으로 하는 ping 공격을 시행한다. ping 공격을 시행하는 목적은 외부로부터 접근하는 경로를 대상으로 하는 공격 Tool보다는 서비스를 제공하는 서버를 대상으로 직접 공격하는 방법을 선택해서 제안하는 환경에 적절한 공격과 정확한 결과를 산출하기 위함이다.

따라서 각 보안장비에는 최초 구축 시에 설정된 보안환경을 변경하지 않고 별도의 관제 시스템에서 정책을 부여하는 방식을 적용한다. 다만, 첫 번째 제안하는 조건인 보안 네트워크 장비 이외의 관제 시스템의 정책 탑재 하드웨어 플랫폼인 디스크를 RAM Disk 또는 SSD의 고속 장비로 구성한다. 또한 두 번

째 정책 정보는 각 디스크에 탑재하기 위한 네트워크 보안장비별 적용 가능한 분류를 하고 관제 시스템에 사전 탑재 후 필요에 따라 적용한다.

결과 도출을 위한 부가적인 결과로는 트래픽 부하량을 측정하는 부분까지 확인하고 제안된 기법과의 객관적인 비교평가를 확인한다.

* *공격 Client System 구성 - Linux 기반의 Ping of Death 공격 Tool 탑재*
* *관제 System 구성 - CentOS 탑재 후 각 네트워크 장비별 초기 방어 Tool 탑재*

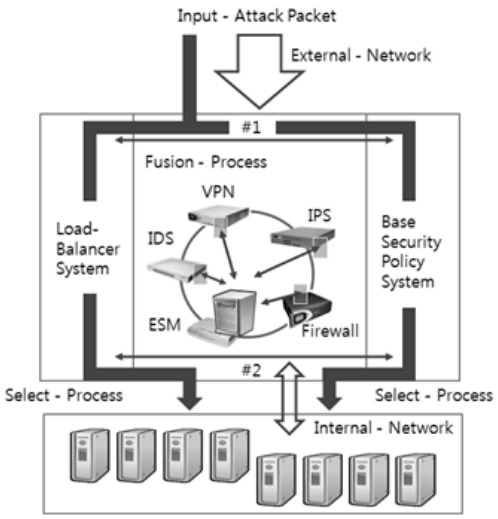

그림 4. 제안과 실험환경
Fig. 4 Suggestions and experimental environments

4.2 고속화 동기 네트워크 인프라 환경 공격

네트워크 보안 장비에 대한 고속화 하드웨어 플랫폼인 구성은 그림 5와 같이 접근 패킷에 따른 보안정책 탑재 구현방법의 차이를 구성한다. 즉, 최초 구축되는 보안장비의 하드웨어 정책저장 플랫폼인 Flash Memory를 이용하여, 정책을 구동하는 방식을 활용하는 반면, 제안하는 방어기법에서는 고속화 및 정책탑재를 위한 동기화 구현을 위해 RAM Disk 또는 SSD를 하드웨어 플랫폼으로 구현함으로써 기존의 네트워크 인프라와의 차이점을 둔다.

정상적인 접근을 원하는 패킷의 경우는 기존의 장비 초기 설정 값에 따른 방어와 트래픽 조정을 시행하고 이외의 비정상적인 접근에 대한 패킷은 제안하는 방어기법을 적용함으로써 기존의 장비와의 일부 호환성을 제공한다.

물론 침해 패턴과 학습되어진 데이터베이스를 장기간에 걸쳐 습득하고 분석함으로써 Case by Case 정책 적용을 위한 소프트웨어 플랫폼을 구현해야 한다. 하지만, 패턴 학습 데이터베이스를 분석해야하는 제한된 환경과 기간이 소요되는 문제점이 있다. 따라서 다양한 보안 네트워크 인프라를 구성하는 장비 제조사 또는 솔루션 개발 정보를 상호 공유해야하는 어려운 문제점 또한 있다. 이는 향후 연구해야 할 또 다른 과제가 될 것이다.

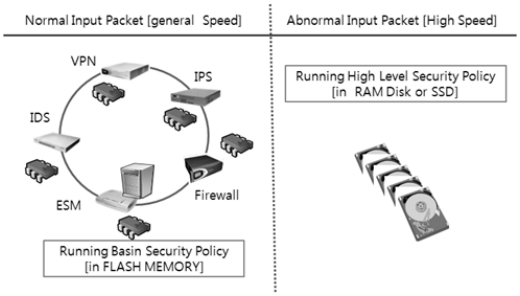

그림 5. 접근 Packet에 따른 보안정책 탑재 구현방법의 차이
Fig. 5 Differences in the methods of mounting security policies between access packets

4.3 공격에 대한 방어 정책과 제안 알고리즘

방어기법의 적용을 위한 2가지 단계에 대한 구현 알고리즘을 제안하고 요약함으로써 결과를 도출하는데, 활용하고 개발의 영역을 확대하기 위한 기본정보로 활용한다.

하이브리드 융합 고속화 동기 네트워크 인프라 구성의 외부로부터의 최초 접근하는 패킷을 분리하고 해당되는 정책적용을 위한 경로 설정을 하는 Select-Process Algorithm과 하드웨어 및 소프트웨어 방어 플랫폼을 조합하는 Fusion-Process Algorithm을 기술했다.

* *Select-Process Algorithm*
  define DISK "based of Hardware - Flash Memory
  define DISK "based of Software - RAM Disk or SSD
  input Packet
  op approach progress
    searching H/W_base attack and S/W_base attack
    if searching_value is H/W

running [Flash Memory] in security policy
else running [Load-Balancer SA]
end
[SA : System Algorithm]

Select-Process Algorithm은 하드웨어 또는 소프트웨어 플랫폼을 선정하는 알고리이며,

* *Fusion-Process Algorithm*
join op Load-Balancer SA and Base Security Policy SA

Fusion-Process Algorithm은 제안하는 2가지 플랫폼의 방어기법을 융합함으로써 고속화된 하드웨어 플랫폼과 정적 보안정책을 선정하는 소프트웨어 플랫폼을 동기화하는 알고리즘이다.

* *Load-Balancer System Algorithm*
define PATH{P_1 = VPN, P_2 = IDS, P_3 = IPS, P_4 = Firewall, P_5 = ESM}
define DISK "loading security policy" - RAM Disk or SSD
start load-balancing SA module
input Packet
op loading balancing progress
searching approach PATH(P_1, P_2, P_3, P_4, P_5) || matching operating security PATH
open matching PATH
searching DISK(RAM Disk, SSD)
selecting DISK
ready DISK
close matching PATH
end load-balancing SA module and jump security policy SA
[SA : System Algorithm]

Load-Balancer System Algorithm은 유입되는 또는 공격성향을 가진 접근에 대한 각 네트워크 보안장비별 특성을 분석하고 해당 접근 제어가 가능한 장비로의 Forwarding을 위한 장비선정 알고리즘이며, 최종 알고리즘에 의해 RAM Disk 또는 SSD에서 최종 공격 패턴 데이터베이스와 일치하는 Case by Case 보안정책을 탑재시키는 알고리즘을 구현한다.

* *Base Security Policy System Algorithm*
define POLICY - Pattern{PP_1 = VPN, PP_2 = IDS, PP_3 = IPS, PP_4 = Firewall, PP_5 = ESM}
define PP "each of Unit - loading security policy" - PUT RAM Disk or SSD
input Packet
select PP
start PUT disk = PP
running PP
defense attack - based of PP
end Base Security Policy SA
[SA : System Algorithm]

4.4 공격에 대한 결과 분석

최종 제안기법에 따른 실험결과를 분석함에 있어서 표 5와 같은 같이 기존 정보보안 장비를 구축한 경우와 Diskless 및 Stateless 기반의 고속화, 동기화 기법을 적용한 차이가 도출됐다.

해당 표를 분석해 보면, 접속 지원속도 부문에서는 오히려 낮은 전송속도의 경우에는 기존 네트워크 인프라보다 방어를 위한 지원속도가 낮았다. 그러나 정보보안을 위한 정책을 탑재하는 하드웨어 플랫폼을 고속화된 기기로 구성함에 따라 허용 가능한 패킷의 범위와 접속 세션의 폭이 확장됨을 알 수 있다. 또한 침해방어 비율의 오차를 기존 인프라보다 현저히 낮게 구성 가능했다.

다만, 고속화 하드웨어 인프라 구현을 위한 플랫폼 구축에 대한 경제성이 기존의 인프라보다 높음으로 인해 향후 지속 가능한 개발 영역과 과제를 도출하는데, 다소 장애가 있음을 확인했다.

표 5. 일반적인 보안장비 운영과 제안 보안기법 비교결과
Table 5. Operation of general security devices and results of comparing suggested security mechanisms

구분	각 보안기기별 운영[방어]형태	Diskless와 Stateless 기반의 고속화 제안[방어]형태
접속 지원속도	Maga, Giga, Tera bps 지원	Giga, Tera bps 지원
지원 보안정책 저장매체	HDD[IDE, EIDE, SATA]	RAM DISK, SSD

보안정책 저장매체 구현		1개 기억소자 당 1비트 데이터 처리	MLC(Multi Level Cell) 방식 채택 [1개 기억소자 당 2비트 데이터 처리]
적용 범위	네트워크 규모	소, 중, 대 규모 [불특정]	소, 중규모[특정 목적을 위한 네트워크]
	허용가능 패킷 [대역폭]	Min 2Gbps / MAX 3Gbps	Min 1Gbps / MAX 4Gbps
	허용가능 세션	1,000,000 ~1,500,000	1,000,000 ~2,000,000
	침해 방어비율	50~90%	초기 접근 방어비율이 80% 이상이면, 지속적인 접근 방어비율은 95% 이상 구현
	무한접근 방어	지원 / 제한적 지원	지원 / 선택적 허용 지원
	구현비용 및 구현시장성	저가~고가 / 대중화	고가 / 대중화 시점[정책 탑재 고속화 DISK 및 Memory 구현 부분 고가]

V. 결 론

본 논문에서는 고속화 기반의 하드웨어 인프라 플랫폼과 정책 적용 기반의 소프트웨어 플랫폼을 동기화 하는 융합된 네트워크 인프라를 이용한 방어기법을 제안하고 있다.

첫 번째 제안하고 실험한 결과에 따르면, 기존의 보안 네트워크 인프라 구현 시에 얻어지는 방어 결과보다 방어비율 상의 오차를 줄임으로써 향후 지속적인 연구개발로 오차를 줄일 수 있는 토대를 마련했으며, 두 번째로는 각 보안 네트워크 장비들에 대한 정책 탑재를 위한 기법을 소프트웨어적인 플랫폼으로 제안함으로써 모든 보안 정책을 사전에 탑재하고 공격만을 기다리는 형태에서 장애별 Case by Case 가능한 방안을 확인했다.

마지막으로 앞선 2가지 조건이 만족함과 동시에 가장 최적의 접근 대역폭을 확보해줌으로써 접근허용 패킷과 접속 세션의 범위를 확대 가능했다.

따라서 향후 연구방향으로는 실험환경을 대상으로 공격하는 Tool을 더욱 다양화해서 각각의 공격 형태에 따른 대역폭 감소비율과 공격에 따른 방어비율을 얻음으로써 고속화 융합 동기 보안 네트워크에 대한 결과 값을 표준화하고 소규모 네트워크로부터 대규모 네트워크까지 적용이 가능한 실험을 재 구현할 수 있도록 연구의 영역을 확대해야 한다.

또한 하드웨어 인프라 플랫폼 구현을 위한 시장 경제성 문제점을 파악하고 미래 보안시장을 확인하고 보안 기법 적용과 구축 및 구현을 위한 경제적 융통성이 확보하는 부분까지 연구의 범주로 넣어야 한다.

참고 문헌

[1] 헤럴드 경제(헤럴드 생생뉴스), http://biz.heraldm.com/common/Detail.jsp?newsMLId=20110820000042, “갈수록 빈번해지는 해킹사고…대책 없나”, onlinenews@heraldm.com, 2011, 8.

[2] 한국인터넷진흥원 인터넷침해대응센터, “인터넷 침해사고 동향 및 분석 월보”, pp. 7-8, 6, 2011.

[3] 김지훈, 조시행, “사이버 환경에서의 보안위협”, 한국정보보호학회 논문지, 20권, 4호, pp. 11-20, 2010.

[4] 오정숙, 정보통신정책연구원, “국내외 네트워크 장비 시장 현황 및 시사점”, 방송통신정책, 23권 9호, pp. 35-52, 5, 2011.

[5] 은성경, “클라우드 컴퓨팅 보안 기술 동향”, 한국정보보호학회 논문지, 20권, 2호, pp. 27-31, 2010.

[6] 박경욱, 김경옥, 반경진, 김응곤, “클라우드 기반 센서 데이터 관리 시스템 설계 및 구현”, 한국전자통신학회 논문지, 5권, 6호, pp. 672-677, 2010.

[7] ZDNet Korea, http://www.zdnet.co.kr/news/news_view.asp?artice_id=20110728163354&type=xml, “클라우드 보안 기상도 ‘흐림’…보안의식 수준↓”, 김희연 기자, 8, 2011.

[8] 주헌식, 김종완, “통합 보안 시스템에서의 효율적인 보안 정책 관리 모델”, 한국컴퓨터정보학회 논문지, 15권, 9호, pp. 99-107, 2010.

저자 소개

서우석(Woo-Seok Seo)

2006년 숭실대학교 정보과학대학원 정보통신융합학과(공학석사)
2009년 - 현재 숭실대학교 일반대학원 컴퓨터학과 (박사과정)
※ 관심분야 : 정보보호, 네트워크 보안, 방화벽, Router & Network Design 등

전문석(Moon-Seog Jun)

1981년 숭실대학교 전자계산학과 졸업
1986년 University of Maryland Computer Science 석사
1989년 University of Maryland Computer Science 박사
1986년 9월 - 1989년 12월 University of Mary 강사
1989년 3월 - 7월 Morgan State University 조교수
1989년 9월 - 1991년 2월 New Mexico State University Physical Science Lab. 책임연구원
1991년 3월 - 현재 숭실대학교 정교수
※ 관심분야 : 정보보호, 네트워크 보안, 전자여권, 암호학