네트워크 보안 기술 동향과 전망

김봉현, 조동욱
경남대학교, 충북도립대학교

요 약

최근 들어 인터넷 등 네트워크 기술이 급격하게 발전하면서 다양한 경로를 통한 정보 유출 사고가 빈번하게 발생하고 있다. 이를 방지하기 위해 다양한 방법을 적용한 정보 유출 방지 기술이 개발되고 있으며 이를 기반으로 한 솔루션이 적용되고 있다. 보안 기술은 네트워크 보안과 시스템 보안으로 분류되며 개방형 네트워크 환경에서 불법 행위로부터 정보를 보호하는 기술이 네트워크 보안 기술이다. 네트워크 보안은 데이터 통신에서 발생하는 보안 사고에 대하여 무결성, 기밀성, 가용성을 어떻게 보호하여야 하는지를 논의하면서 관련 기술이 개발되어 왔다. 본 논문에서는 컴퓨터 내부에서 발생하는 보안이 아닌 네트워크를 통해서 발생되는 데이터의 보안 분야의 기술 동향과 향후 전망에 대해 논의하고자 한다.

Ⅰ. 서 론

현대 사회에서 인터넷은 일상 생활에서 언제든지 연결되는 불가분의 필수 요소가 되고 있다. 이렇듯 인터넷에 대한 의존성이 증가하면서 오프라인과 마찬가지로 온라인상에서도 다양한 형태의 사이버 위협들이 기하급수적으로 증가하고 있는 실정이다. 이러한 사이버 위협으로부터 사용자 데이터, 시스템 및 네트워크 자체를 보호하기 위한 다양한 네트워크 보안 기술들이 개발되고 있다. 그러나 이를 위협하는 인터넷 침해사고도 끊이지 않고 있다[1].

최근 들어 사이버 해킹 및 개인정보 유출 사고가 끊이지 않고 있으며, 다양한 정보통신 기술의 발달로 보안침해 사고 및 공격 방법이 더욱 더 진화되고 있다. KISA의 2012년 11월 인터넷 침해사고 동향 및 분석월보에 따르면 2012년 한해 11월까지 악성코드 피해 신고 18,937건이였으며, 해킹사고 접수처리는 18,126건으로 조사되고 있다. 사용자가 웹 브라우저에 URL을 직접 입력하여 정보를 검색할 때 악성코드가 은닉된 웹사이트로 접속을 유도하거나, 웹 하드 등의 사용을 통해 악성코드 등이 유포되는 네트워크 보안 침해 사고가 발생하고 있다. 이에 따라 온라인의 불법 침입자가 중요 정보에 접근할 수 없도록 차단하는 네트워크 보안 기술의 개발 및 이를 적용한 솔루션의 활용이 강조되고 있다[2][3].

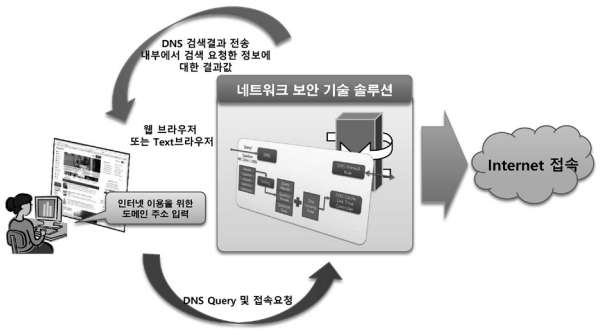

그림 1. 네트워크 보안 기술 솔루션 구성도

네트워크 보안의 필요성은 두 가지로 생각할 수 있다. 첫째, 허가 받지 않은 외부 침입자에게 정보가 유출되지 않도록 하기 위해서다. 보안 데이터가 전달되는 네트워크 경로에서 데이터를 불법적으로 훔쳐내 악용하는 경우가 이에 해당한다. 둘째, 외부 침입자가 보안 데이터의 내용을 조작하지 않도록 보호하기 위해서다. 데이터 조작은 통신하는 사람들 간의 정상적인 데이터 통신을 방해한다[4].

따라서 본 고에서는 네트워크 보안의 중요성을 더욱 강조하기 위해 현재의 네트워크 보안 관련 현황을 살펴보고 네트워크 보안 기술을 내부와 외부 기술로 분류하여 각 기술의 동향과 기능을 분석하고자 한다. 이를 위한 본 고의 구성은 다음과 같다. Ⅱ장에서는 네트워크 보안 기술의 개요와 네트워크 보안 관련 침해사고 현황을 살펴본다. Ⅲ장에서는 주요 네트워크 보안 기술을 내부와 외부 네트워크 보안 기술로 분류하여 각 기술의 동향을 살펴본다. Ⅳ장에서는 네트워크 보안 기술들의 향후 전망을 분석하고 본 고의 결론을 맺는다.

Ⅱ. 네트워크 보안

본 절에서는 네트워크 보안 기술의 개요와 네트워크 보안 관련 침해사고 현황에 대해 살펴보고, 이러한 사고를 방지하기 위한 서비스 요구 사항을 살펴본다.

1. 네트워크 보안 개요

정보의 유출, 변조, 위조, 훼손 등을 방지하기 위한 관리적, 기술적 대응 방법을 정보보안이라 한다. 보안이란 자산의 본래 가치가 손상되지 못하도록 자산을 적절한 방법으로 보호하는 것을 의미한다. 컴퓨터 보안이란 개인이나 기관이 사용하는 컴퓨터와 관련된 모든 것을 안전하게 보호하는 것을 말하는 것으로 일반적으로 시스템의 정보를 보호하는 행위를 말한다. 네트워크 보안이란 말 그대로 TCP/IP 프로토콜을 비롯해 각종 프로토콜이나 네트워크를 통해 연결된 수많은 호스트들 사이에서 정보의 유출과 불법적인 서비스 이용을 방지하는 것이다.

이러한 정보보안은 공급자 측면에서 내 · 외부의 위협요인들로부터 네트워크 및 시스템 등의 정보자산을 보호, 운영하기 위한 행위와 사용자 측면에서 개인정보 유출, 남용 등을 방지하기 위한 행위로 분류된다. 특히, 내 · 외부의 위협요인들로부터 정보를 보호하는 보안 분야에서는 보호 주체에 따라 네트워크 보안과 시스템 보안으로 분류한다.

네트워크 보안은 개방형 네트워크 환경에서 전달되는 정보의 위조, 변조, 조작, 유출, 무단침입 등의 불법 행위로부터 정보를 보호하는 것을 의미한다. 즉, 네트워크 경계에서 침입자로부터 보호 기능을 제공하는 것으로 네트워크 하부 구조에서의 기본적인 보안 기술을 의미한다[4][5].

네트워크 보안을 위협하는 형태는 다음의 4가지로 분류할 수 있다.

① 인증에 대한 위협 : 제3자가 정보와 데이터의 전송을 가로막아(Interruption;흐름차단) 시스템의 일부를 파괴하거나 사용할 수 없게 하는 인증에 대한 위협을 할 수 있다.

② 기밀성에 대한 위협 : 허가받지 않은 제3자가 전송 중간에 정보와 데이터를 가로채어(Interception) 기밀성에 대한 위협을 할 수 있다.

③ 수정에 따른 무결성 위협 : 제3자가 시스템의 자원에 불법적으로 접근하여 데이터를 수정(Modification)함으로써 무결성에 대한 위협을 할 수 있다.

④ 위조에 의한 신뢰성 위협 : 제3자가 시스템에 불법적으로 접근하여 거짓 정보 등을 삽입하여 위조(Fabrication)함으로써 신뢰성에 대한 위협을 할 수 있다.

또한, 네트워크에 대한 공격 형태는 다음과 같이 3가지로 분류할 수 있다.

① 수동적인 공격 : 네트워크에 흐르는 정보를 제3자가 알아내서 자신의 이익을 취하는데 이용하는 것으로, 정보의 내용이 아니라 정보의 흐름 그 자체를 분석하여 어떤 사실을 유추해 내고자 하는 것이다.

② 능동적인 공격 : 좀더 과감하게 정보의 흐름을 중간에서 가로채어 그 내용을 변조하여 공격자가 자신의 이익을 추구하고자 하는 것이다. A가 B에게 정보를 아예 보낼 수 없게 통신회선을 절단하여 제3자가 상대적인 이득을 취하고자 하는 것이다.

③ 위장(Masquerade) : 사실은 A가 아니면서 A인 것처럼 B에게 보냄으로써 제3자가 이득을 취하는 것으로 이것도 능동적 공격이다.

2. 침해사고 현황

국내의 보안 위협에 대한 통계 자료를 살펴보면 〈표 1〉과 같이 지난 2012년 11월 인터넷침해대응센터 자료를 보면 2012년 한해 11월까지 국내의 해킹사고 접수 처리는 18,126건, 악성코드 피해신고는 18,937건이며, 〈그림 1〉과 같이 해킹사고 접수 처리는 2005년 이후부터 신고건수가 감소하고 있으나, 악성코드 피해신고는 2008년을 기점으로 계속 증가하고 있는 실정이다[6][7][8].

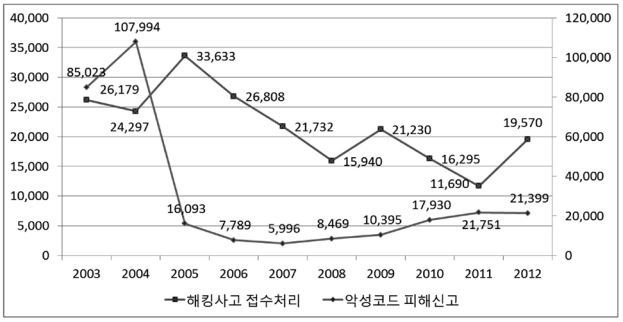

그림 2. 보안 침해사고 처리 통계 (2003년~2011년)

또한, 국외의 보안 위협에 대한 통계 자료를 살펴보면 다음과 같다. 〈그림 3〉과 〈그림 4〉는2012년 매월 새롭게 발견된 위협 URL의 증가폭과 피싱 URL의 증가폭을 나타낸 것이다.

보안업체 McAfee의 2012년 3분기 Threats Report에 따르면, 전세계 2012년 3분기에 악성 코드를 및 피싱 사이트로 분리되는 위협 URL의 총 수가 43,400,000 건으로 집계되었다. 이는 2012년 2분기 대비 20%가 증가한 수이며, 이러한 URL의 도메인 네임은 23,700,000 건을 나타내며 이전 대비 최대 5%가 증가했다. 또한 새롭게 매월 새롭게 발견된 위협 URL 수는

표 1. 2012년도 월별 침해사고 접수처리 통계

type	2011 year	2012 year											total
		1	2	3	4	5	6	7	8	9	10	11	
Malignant code damage reporting	21,751	1,443	1,186	1,685	2,164	2,138	2,394	1,638	1,472	,1339	1,419	2,059	18,937
Hacking incident receipt processing	11,690	1,510	1,210	1,702	1,419	1,534	2,174	1,937	2,173	1,273	1,608	1,586	18,126
• Spam relay	3,727	429	395	474	621	693	598	485	434	400	812	668	6,009
• Phishing stopover	365	36	37	38	39	37	34	30	29	41	42	36	399
• Simple intrusion attempts	2,961	202	184	159	106	206	394	240	614	304	191	155	2,755
• Others hacking	2,783	233	307	415	515	488	796	1,000	1.013	431	440	355	5,993
• Homepage falsification	1,854	610	287	616	138	110	352	182	83	97	123	372	2,970
Malicious Bot infection rate	0.52%	0.6%	0.6%	0.6%	0.7%	0.7%	0.7%	0.6%	0.7%	0.7%	0.7%	0.8%	0.68%

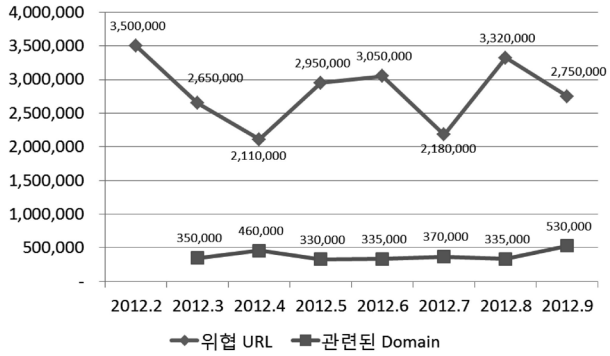

그림 3. 2012년도 월별 발견된 위협 URL 현황

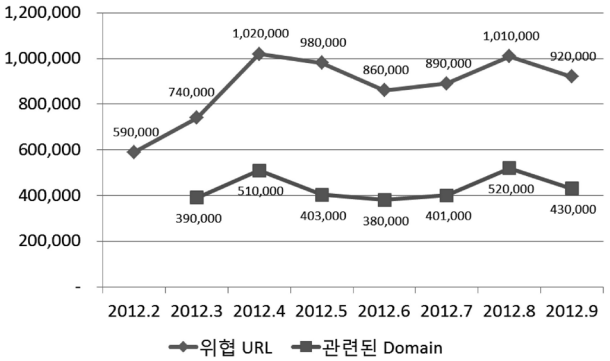

그림 4. 2012년도 월별 발견된 피싱 URL 현황

평균 2,700,000건이라 하였고, 고유한 IP 주소에 110,000건의 별개의 도메인이 연결되는 등의 새로운 추세의 위협도메인이 생겼다고 발표하였다[9~13].

3. 침해사고 사례

국내의 경우, 2013년 2월 전자신문에 보도된 보안이슈를 보면 신종 금융사기 수법인 '파밍' 기술의 급증한다고 보도하였다. 이는 〈그림 5〉와 같이 최초 사용자에게 악성코드를 유포하여 유저가 정상적인 주소로 은행사이트에 접속해도 가짜 사이트에 연결되는 금융사기 수법이다.

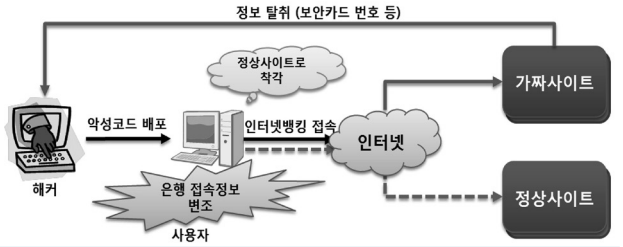

그림 5. 신종 금융사기 수법인 파밍 개요도

또한, 2013년 2월 보안뉴스에 보도된 보안기사에 따르면 한글 제로데이 취약점 및 대형 포털 사이트의 업데이트 등을 통해 악성코드를 유포하여 추가 DDoS 공격을 유발하도록 보안 위협을 증가시키고 있는 상황이며, 지난 2009년 7월 7월 국가 주요 정부기관의 DDoS공격 및 2011년 1월에 도메인과 호스팅 전문 업체인 후이즈의 DDoS 공격 및 악성코드 유포를 통한 좀비PC 감염을 통한 DDoS공격 등 DDoS 공격은 아직도 유효하게 진행되고 있는 상황이다[14].

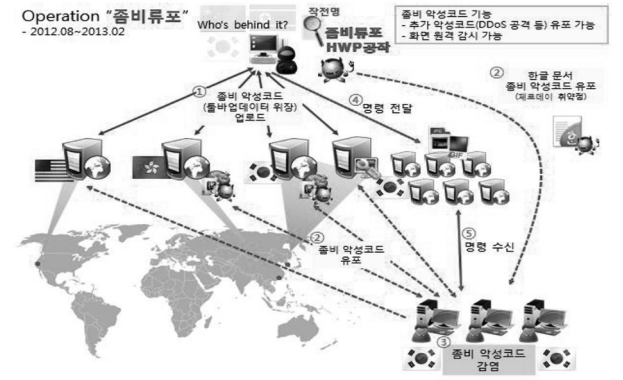

그림 6. '좀비류포, HWP공작'이란 작전명으로 진행된 좀비 악성코드 공격의 도식화

국외의 경우, 2012년 10월 foxnew.com에 따르면, 워싱턴의 백악관 컴퓨터에 중국해킹 공격을 확인하였으며, 이는 정부 고

위관부, 유명인, 군인 등과 같은 특정인을 대상으로 이들의 개인정보를 캐내기 위한 스피어 피싱이라 지칭하는 피싱공격으로써, 악의적인 웹사이트의 접속 또는 PDF, Exel, Word 첨부파일 등을 통해 악성코드를 유포하여 실시되었다고 보도하였다.

2007년 처음 등장해 작년 11월까지 전 세계 100개국 420만대의 PC를 감염시켜 1천400만달러(158억원) 상당의 이익을 취한 에스토니아 해커는 DNS 주소를 변경해 인터넷 접속장애를 일으키는 악성코드인 DNS changer를 유포시켰으며, 이렇게 DNS changer는 사용자가 인터넷 익스플로러 등 웹 브라우저에 도메인 네임을 입력할 때 서버는 해커들이 재정적 이득을 취할 수 있는 다른 사이트로 접속하게 만드는 악성코드이다. 이 또한 웹사이트 등을 통해 악성코드 유포로 인한 사례이다.

그림 7. DNS 체인저 악성코드를 이용해 인터넷 접속 장애를 일으키는 과정

위와 같은 국내외 다양한 보안 위협 사례는 대다수가 인터넷을 통한 악성코드 감염 및 피싱 사고로 이어지고 있다. 매스컴의 대대적인 보도와 개인정보 유출에 대한 국민적 관심이 증가하고 있고, 모바일 웹과 클라우드 환경, 빅데이터 등 침해 강도 및 영역이 점차 증가하고 있어 개인의 프라이버시 침해에서부터 국가 경제 및 안보에까지 총체적으로 위협을 하고 있는 실정이다[15].

최근에는 악성코드의 제작, 유포, 추가공격이 굉장히 쉬워졌으며, 변종 또한 기하급수적으로 많아지고 있다. 이러한 위협적인 웹사이트 접속과 그에 따른 악성코드 감염으로 악의적인 해킹이나 산업 스파이에 의한 정보유출, 내부 직원의 회사기밀, 고객정보 유출 등의 컴퓨터를 이용한 범죄가 급증하고 있다.

이와 같은 상황속에서 침해사고가 발생하였을 경우 가해자보다 피해자가 더 많은 비난을 받는 사회적 분위기가 조성되고 있다. 즉, 침해사고는 무조건 피해자의 과실이라는 인식이 자리잡고 있기 때문에 다양한 보안 솔루션들을 개발, 적용하여 완벽한 예방을 추구하려는 노력이 증가되고 있다.

그러나 보안 시스템은 특정 위협에 대한 통제에 불과하기 때문에 이를 통한 침해사고 차단은 100% 완벽할 수 없다. 즉, 보안 시스템도 업무에 필요한 접근경로에 대해서는 개방을 허용할 수 밖에 없기에 완벽한 침해 차단이 어렵다. 또한, 감시를 통한 탐지인 IDS도 널리 알려진 패턴이나 명백한 비정상적 행위에 대한 탐지가 가능한 것이기 때문에 침입탐지 우회기법 등을 통한 침해사고 탐지에는 한계가 있다.

따라서 이를 근본적으로 해결하기 위해서는 사용자 중심의 행위 기반을 제어하는 형태가 절대적으로 필요하다.

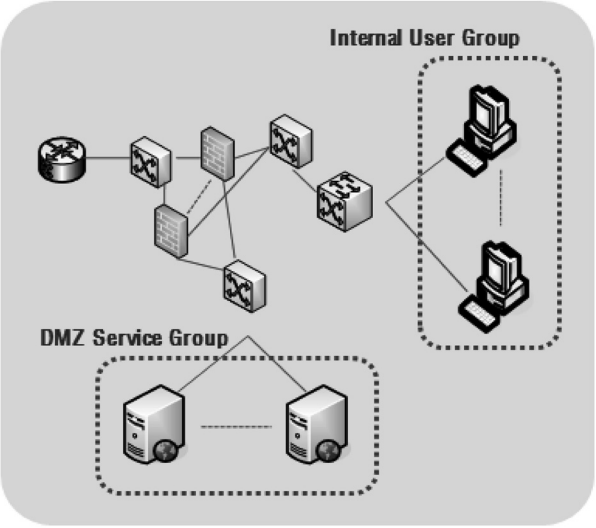

그림 8. 사용자 중심의 행위기반 제어 구성도

Ⅲ. 기술 동향

네트워크 보안 기술은 크게 외부 네트워크 보안과 내부 네트워크 보안으로 분류할 수 있다. 외부 네트워크 보안은 공유해야 하는 자료에 대하여 외부로 전달하는 과정에서 유출되는 자료를 어떻게 보안을 해야 하는지가 가장 큰 이슈이다. 이를 위한 방법은 자료를 외부에 노출되어도 해석이 불가능하게 하는 방법이 대표적인 방법이다. 이에 반해 내부 네트워크 보안은 열려있는 자료에 대한 보안을 하여야 하는 과제를 안고 있다.

1. VPN

VPN(Virtual Private Network)은 구간 암호화 솔루션으로 트랜젝션 보안이라고도 한다. VPN 기술은 공중망 인프라를 공유하여 구축된 가상사설망을 의미한다. 과거 VPN은 PSTN 전용회선을 통한 사설망, 최근 들어서는 ATM이나 FR 망을 통한 VPN으로 그 구축 기술이 변천해왔다. 이제 인터넷이라는 공중 네트

워크를 공유하여 경제적이며 안전하고 신뢰할 수 있는 IP VPN을 구축할 수 있는 기술, 표준, 수요 등 여건이 성숙되었다.

IP VPN으로 기업은 본사와 지사를 연결하는 intranet, 협력사와 연결되는 extranet, 그리고 최근 들어 급증하고 있는 이동근무자와 재택근무자를 회사에 안전하게 연결시킬 수 있는 원격 접속망 등을 경제적으로 구축할 수 있게 되었다[16].

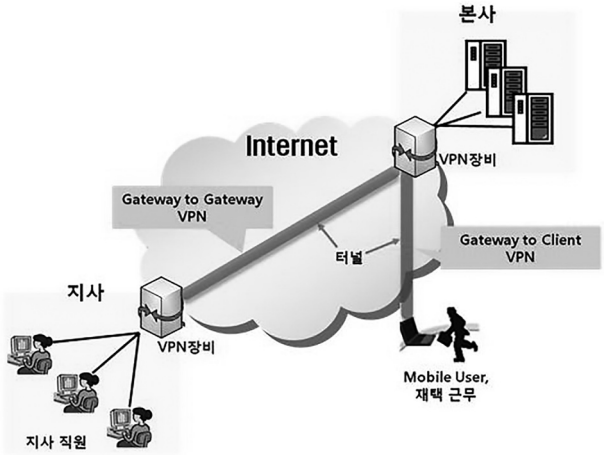

그림 9. VPN 구현 방식

VPN 구현방식은 Gateway to Gateway(GtoG) 및 Gateway to Client(GtoC)방식으로 분류할 수 있다. GtoG VPN 방식은 본사 및 각 지사 별로 VPN장비를 구축하여 VPN장비간에 터널을 제공하는 방식으로 VPN 서비스를 이용하는 지사 직원 및 본사 서버에는 VPN과 관련된 어떠한 애플리케이션이나 설정은 필요가 없다. 즉, 본사 및 지사의 VPN장비 간 인터넷 망에는 암호화된 패킷이 전송되며, VPN장비를 거치면서 복호화된 패킷이 본사 서버 및 지사직원에게 전달되므로, 본사 서버 및 지사 직원은 일상적인 방식의 통신을 진행하면서 인터넷 망에는 자동으로 눈에 띄지 않게 암호화된 통신이 전송되는 것이 GtoG VPN의 개념이다. 이전에는 데이터링크 계층에서 VPN기능을 제공하는 PPTP/L2TP이 주로 사용되었으나, 근래에는 네트워크 계층에서 VPN기능을 제공하는 IPSec VPN이 GtoG VPN 구현에 주로 사용되고 있다[17].

2. DRM

DRM(Digital Rights Management) 기술은 디지털 콘텐츠의 불법유통과 복제를 방지하고, 적법한 사용자만이 주어진 권한 내에서 콘텐츠를 사용케 하여 디지털 콘텐츠 저작권을 관리하는 기술로서 디지털 콘텐츠에 대한 불법적인 사용을 효과적으로 차단할 수 있는 기술이지만 아직까지 표준화된 모습을 갖추지 못하고 있기 때문에, 현재 시장에서는 여러 개의 DRM 솔루션들이 공존하고 있는 상태이다. 이러한 이유에서 많은 디지털 콘텐츠들은 통일화되지 않은 여러 DRM 솔루션을 통해 보호를 받고 있다. 각 사용자 기기에 탑재된 DRM은 이를 지원하는 콘텐츠 제공자들의 콘텐츠만을 이용할 수 있도록 제한하기 때문에 사용자에게서 선택의 기회를 박탈하고 있다. 이를 해결하기 위해 콘텐츠 제공자가 각각의 DRM 별로 콘텐츠를 따로 준비하여 제공한다든가, 기기 제조업체가 복수 개의 DRM 클라이언트를 탑재하는 등의 번거로움이 발생하게 된다. 이는 관리 및 비용 등의 문제뿐만 아니라 각 DRM 간의 충돌로 인한 시스템 불안정을 초래할 수 있는 문제점을 지닌다.

이 때문에 최근 DRM 기술은 특정 서비스를 지원하기 위한 기술 개발보다는 다양한 서비스 환경에서 DRM 사이의 상호호환성 지원을 위한 기술 개발이 활발히 이루어지고 있다. 특히, 상이한 망구조의 통합과 서비스, 디바이스, 콘텐츠의 융합과 같은 디지털 컨버전스 현상이 가속화되고 있는 디지털 홈 환경에서 DRM 기술이 콘텐츠 서비스의 장벽으로 작용할 것으로 예상되는바, 이를 해결하기 위한 표준 및 기술 개발이 진행되고 있다[18][19].

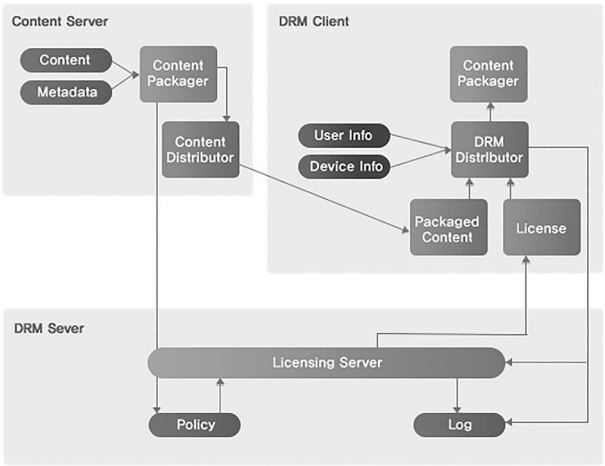

그림 10. DRM 시스템 모델

3. DLP

DLP(Data Loss Prevention) 기술은 내부정보 유출방지 기술로 내부자에 의한 정보 유출방지 기능을 제공하는 통합 솔루션 개념이다. 즉, 기업 구성원, 프로세스, 기술의 결합을 통해 고객 또는 직원 기록 등의 개인 신원확인 정보(PII), 재무제표, 마케팅 계획과 같은 기업 정보, 제품 계획, 소스 코드와 같은 지적 재산(IP)을 포함하는 기밀 정보 등이 기업 밖으로 유출되는 것을 방지하는 솔루션이다.

따라서 다양한 기술을 적용하고 있는데 일반적으로 적용하는

기술로는 접근제어, 암호화, 필터링, 활동감시 등이 있으며 접근제어, 필터링 등의 2가지 기술분야는 현재까지도 활발하게 기술 개발이 수행되고 있다. 또한, 최근에는 정보 유출이 내부자에 의한 유출 사고가 대다수를 차지하고 있는 실정이어서 이에 맞는 솔루션으로 DLP 기술이 개발되고 있다. 최근의 DLP 기술은 가상화, 지능화, 안전성, 포괄성의 4가지 특징에 맞는 방향으로 개발되고 있다.

DLP는 이미 이메일 게이트웨이, 웹프록시, 암호화 솔루션을 비롯한 다양한 보안 솔루션과 통합돼 있지만 기존 보안 제품 기능 중의 하나로 DLP가 제공되는 것은 아니다. DLP의 모니터링과 검색 기능은 기존 인프라 내에서 제공되고 관리 및 리포팅은 중앙의 DLP 정책 플랫폼에서 이루어지므로 기업은 정보가 어디에 있으며 어떻게 이용되고 있고 정보 손실 방지를 위한 정책을 어떻게 실행해야 하는 지와 같은 내용을 전체적으로 이해할 수 있다. 엔드포인트 보호, 백업 스토리지, 이메일 아카이브 기술 등의 영역의 통합도 가능하다[20][21].

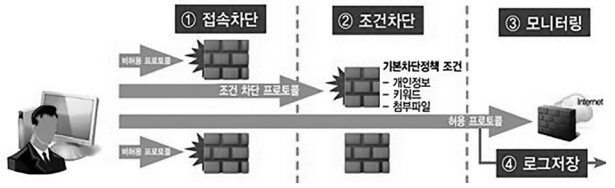

그림 11. DLP 시스템 운영도

DLP 시장은 아직 초기 단계에 있다. 그러나 모든 비즈니스에서 DLP가 필수적이라는 것은 확실하다. 시만텍은 DLP 솔루션을 통해 기업의 데이터 이용과 위험 관리 방법을 변화시키고 있으며 수십만 명의 직원이 있는 기업에서 실제 DLP를 도입한 후 데이터 보호 프로세스를 자동화하고 손실 위험을 현저히 줄이고 있다. 점차 많은 기업들이 DLP를 통한 정보 이용과 보호의 변화를 이해하게 되면 다른 보안 솔루션과 마찬가지로 DLP의 채택도 기하급수적으로 증가할 것이다. 결국 모든 기업이 DLP 도입을 통해 정보를 안전하게 보호하고 정보의 손실 또는 유출되는 것을 방지할 수 있게 될 것이다.

4. 세대별 기술 동향

1세대 내부 네트워크 기술은 침입차단시스템, 침입탐지시스템, 바이러스월, 구간 암호화 솔루션(트랜젝션 보안), QoS시스템 등이 있다. 1세대는 초급 단계의 보안으로 필수적인 사항이라고 할 수 있다. 여기에 침입 탐지는 최근에는 빅데이터 시장과 병합하여 통합 보안시장에서 분석을 위한 필수 데이터를 제공하고 있는 추세이다.

2 세대 내부 네트워크 기술은 침입방지시스템, 스팸차단 시스템 등이 있다. 2 세대에서는 1 세대 솔루션의 기능과 성능이 개선된 사항과 함께 추가적 확대 되었다. 여기서 침입방지시스템은 침입차단시스템과 침입탐지시스템 그리고 웜 차단기능이 포함되어 데이터 탐지 기술이 추가되었다. 또한 스팸차단 시스템과 같은 각종 서비스(메일 서비스)에 대한 보안이 강화되고 있다. 이는 메일을 통하여 유입되는 스팸에 바이러스와 웜 그리고 악성 좀비가 감염을 유도 하고 있기 때문이다.

3 세대 내부 네트워크 기술은 웹 침입차단시스템(웹 방화벽), 통합보안시스템(UTM), 데이터베이스 접근/권한 차단솔루션, DDos 등이 있다. 1 세대의 보안 장비들이 거대 트래픽 1기가급, 10기가급, 50기가급 등을 처리 할 수 있는 성능을 보유하기 시작했다. 보안시스템을 이루는 장비의 하드웨어 성능이 갈수록 높아지고 소형화 되고 있다. 또한 2세대에 보여주고 있던 서비스 시작을 겨냥한 보안솔루션들이 다양하게 출시되고 있다.

이중 데이터베이스 접근/권한 차단 솔루션은 데이터베이스에 접근하는 사용자를 비롯해서 관련 프로세스까지 제어하는 기능을 제공하고 있어 자료 유출에 대한 기능이 강화되었다.

그리고 UTM으로 통합 보안시스템은 기본적인 침입차단 시스템, 침입방지 시스템, 바이러스, 스팸차단 시스템 등등이 포함된 중소형급 네트워크에 관리비용을 절약할 수 있는 모델이 나와 시장에 진입을 하였다.

마지막으로 4 세대 내부 네트워크 기술은 어플리케이션 침입차단시스템, 보안감사용 솔루션, 악성코드 유포지 차단, APT솔루션, 좀비탐지 및 차단 솔루션 등이 있다.

기존 보안 시스템의 구축과 더불어 내부 어플리케이션의 제어까지 하는 솔루션이 출시되어 내부 사용자가 본의 아니게 사용하는 P2P, 토렌토, 원격접속 등등과 같은 솔루션을 제어하도록 하는 어플리케이션 솔루션이 나오고 있다. 그리고 외부 사용자 및 외부 지원 인력에 대한 네트워크 통제를 하는 보안감사용 솔루션이 나와 외부에서 내부 서비스 시스템에 접근하여 작업을 하는 내용에 대한 감시와 제어를 하는 솔루션이 출시되고 있다[22][23].

Ⅳ. 향후 전망 및 결론

현재까지 우리가 사용하는 데이터 통신 방식은 개방형 환경에서 모든 것을 통제하고 제어하는 기능이라고 하겠다. 그러다 보면 사용자 및 서비스 시스템의 유지관리를 위한 비용이 계속해서 들고 있는 실정이다. 이는 우리가 사용하는 오픈방식(개방형 서비스)에서 폐쇄형 방식으로 변경이 필요할지도 모른다. 최근 몇 년 동안 우리나라에서는 망을 분리하는 사업들이 꾸준히

이루어지고 있다. 이는 다른 말로 표현하면 개방 시스템과 폐쇄 시스템을 독립적으로 사용하도록 하는 방법이다.

지금까지는 보안 솔루션의 강화로 보유하고 있는 또는 서비스 하고 있는 자료에 대하여 보다 안전하게 지켜야 한다는 수동적인 관점의 솔루션들이 대다수를 이루고 있었다. 이는 네트워크 보안 영역에서 확연히 들어난다. 초기에 침입탐지 시스템과 침입방지 시스템들이 그 대표적인 솔루션들이다. 여기에 DRM, DLP 등 또한 자료의 유통에 대한 보안을 어떻게 해야 하는지의 관점의 솔루션들이다.

그러나 최근 2~3년 전부터는 네트워크 영역에서 데이터를 추출하여 분석하고, 분석된 데이터를 갖고 보안 및 서비스에 적용할 수 있는 방법들을 연구하고 있다. 최근에는 이를 빅데이터 분석 솔루션이라는 명명하에 시장에 진입을 하고 있다. 이는 초기부터 해왔던 컨설팅 영역의 정보들이 솔루션화 해서 데이터를 분석해야 한다는 쪽으로 변환된 것이라고 생각할 수 있다.

따라서 향후 개발해야 할 네트워크 보안 기술은 서비스(자산성을 갖는 제품)의 평가를 위한 솔루션이라고 할 수 있다. 이를 통하여 네트워크 보안에서 어떻게 서비스에 대한 평가를 솔루션을 적용할지에 대한 정책적인 부분이 지능적으로 나오리라고 생각한다. 다시 말해서 외부 및 내부 사용자에게 제공할 서비스에 대하여 안전성 평가를 1차적으로 하여야 한다. 이는 내부 및 외부 사용자들에게 서비스를 제공하고 일어날 수 있는 보안사고의 범위를 평가하고 해당 사고 발생시 경제적인 피해액 등을 산출하여 서비스에 대한 자산 가치를 구분하는 부분이 필요한 것이다. 그로 인해 서비스 중요도의 평가가 이루어질 것이며, 공개 필요 유무도 빠르게 정의가 될 것이다. 그렇게 되면 해당 서비스가 가져올 위험에 대한 사전 분석이 될 것이다. 이는 바로 보안 솔루션에 정책적으로 적용되어 외부에서 해당 서비스의 접근이 통제될 것이다.

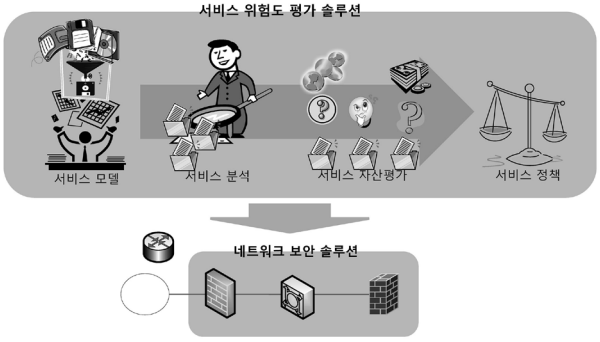

그림 12. 차세대 네트워크 보안 솔루션 전망

이는 현재까지 나와 있는 네트워크 보안 솔루션으로 할 수 있는 범위가 아니다. 현재 나와 있는 네트워크 보안 솔루션에 고도의 보안 지식을 습득한 전문가 집단에서 관련 서비스에 대한 평가 지침을 개발하고 이를 적용하는 방법 등을 연구하여 서비스 위험도 정책을 만들어 적용하는 서비스 위험도 평가 솔루션을 개발해야 할 것이다. 즉, 기존 네트워크 보안 솔루션에 지능적인 서비스 정책이 적용되는 솔루션을 개발해야 할 것이다. 그렇게 되면 서비스 위험도 평가에 대한 이해도가 높아질 것이며, 무분별하게 서비스를 네트워크 서비스 망에 올리지 않을 것이다.

전체적으로 서비스 폐쇄형으로 변화가 와야 하며, 기업이든 기관이든 정보 서비스 수준을 제고하는 과정이 반드시 필요할 것이며, 이를 단순히 전산 담당자의 결정을 하는 시스템이 아니 평가 시스템을 반드시 거쳐서 자산의 평가가 이루어지고 이 평가 결과에 따라 보안 솔루션에 골고루 적용되어야 할 것이다.

참 고 문 헌

[1] Korean Internet & Security Agency, KISA Report, 2012.

[2] B. G. Kyoun, A study on the improvement of the computer security incident management, ungkyunkwan Univ. A Master's Degree Paper, 2011.

[3] D. G. Song, Hacking Infringement Accidents Analysis, Ji&Son Publishers, Korea, 2009.

[4] KISA, 2007년 국내 정보보호산업 시장 및 동향 조사, 2008.

[5] Korean Intellectual Property Office(KIPO), (http://www.kipo.go.kr/)

[6] KISA, Trends report monthly malicious code detection of concealed site, 2012.

[7] KISA, Trends and analysis monthly of internet infringement accidents, 2012.

[8] IDC Korea, IDC Market Analysis: Korea Security Software 2008-2012.

[9] McAfee Threats Report: Third Quarter, 2012.

[10] T. Ma, On the Security of A Novel Elliptic Curve Dynamic Access Control System, IJSIA Vol.3 No.1, 2009.

[11] F. Alkhateeb, A. M. Manasrah and A. R. Bsoul, Bank Web Sites Phishing Detection and Notification System Based on Semantic Web technologies, IJSIA Vol.6 No.4, 2012.

[12] E. Hooper, Efficient and Intelligent Network

Infrastructure Protection Strategies for Complex Attacks, IDS Evasions, Insertions and Distributed Denial of Service, IJSIA Vol.1 No.1, 2007.

[13] Khairallah, Michael, Security System Design And Implementation Guide : The Design and Implementation of Electronic Security Systems, Butterworth-Heinemann, 2005.

[14] J. Y. Kang, Phishing/Pharming Examples and Countermeasure Analysis, Journal of Information Science Society, 2013.

[15] Market Trends and Forecast for Firewall and IP Virtual Private Network Equipment: Worldwide, 2001-2006," Market Trend, Gartner, Oct. 2002.

[16] C. Kaufman, et al., "Code-preserving simplifications and improvements to IKE", draft-kaufman-ipsec-improveike-00.txt, 2001.

[17] H. Ould-Brahim, et al., "Network based IP VPN Architecture using Virtual Routers", draft-ietf-ppvpn-vr-00.txt, 2001.

[18] OMA, "Service and Content Protection for Mobile Broadcast Services," 2007.

[19] OMA, "Mobile Broadcast Services - XML Schema for OMA DRM 2.0 Extensions for BCAST(XBS),"2007.

[20] Curtin-Mestre K., Room S., Yngve S., "Privacy Concern with Adopting DLP Technology," RSA Conference Europe, 2009.

[21] G. Y. Kim, A Security Monitoring System for Security Information Sharing and Cooperative Countermeasure, Journal of the Institute of Electronics Engineers, Vol.50 No.2, 2013.

[22] A. Belenky, N. Ansari, On IP Traceback IEEE Communication Magazine, vol. 41, pp. 142 - 153, July 2003.

[23] Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson, Practical Network Support for IP Traceback, Technical Report UW-CSE-00-02-01, Department of Computer Science and Engineering, University of Washington, Seattle.

약 력

김 봉 현

2000년 한밭대학교 전자계산학 공학사
2002년 한밭대학교 전자계산학 공학석사
2009년 한밭대학교 컴퓨터공학 공학박사
2000년~2003년 ㈜한빛넥스젠 기업부설연구소 연구소장
2004년~2012년 ㈜에이텍정보기술 연구기획이사
2012년~현재 경남대학교 컴퓨터공학과 조교수
관심분야: 생체신호분석, 정보보안, IT-의료 융합기술

조 동 욱

1983년 한양대학교 전자공학 공학사
1985년 한양대학교 전자공학 공학석사
1989년 한양대학교 전자통신공학 공학박사
1982년~1983년 신도리코 기술연구소 연구원
1991년~2000년 서원대학교 부교수
2000년~2002년 한국전자통신연구원 초빙연구원
2000년~현재 충북도립대학교 전자정보계열 부교수
관심분야: BIT융합기술, 생체신호분석, 통신보안