제주교육대학교 논문집 (2004)
제33집 pp. 343~357

보안 시스템의 주요 동향에 관한 연구
An Study on Main Trend of Information Security System

김종훈*, 김종진**, 이면재**

〈목 차〉

〈개 요〉

정보화는 지식 사회를 도래하게 만들었지만 해킹·바이러스 유포, 정보시스템에 대한 불법 침입, 인터넷을 통한 범죄 등의 역기능이 갈수록 심각해지고 있다.

따라서 본 논문은 정보 보안 실태 조사와 문제점을 고찰하고 현재 정보 보안과 관

* 제주교육대학교 컴퓨터교육과 교수
** 홍익대학교 컴퓨터공학과 박사과정 수료

련된 시스템의 추세를 살펴보았다. 이것은 추후 정보 보안을 설계하는데 도움을 줄 수 있다.

〈ABSTRACT〉

While the informatization makes knowledge society, it has been caused to negative effects such as hacking, virus propagation, illegal intrusion in information system, cyber crime.

In this paper, we consider current status and problem of information security, trend of information security system. This is helpful to design of information security.

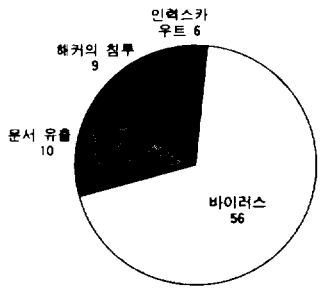
1. 서 론

정보통신이 국가와 사회의 주요한 기반이 되면서 모든 경제 주체들의 생활방식이 크게 변화하고 있으며 지식과 정보가 사회발전의 원동력이 되는 지식사회로 발전하고 있다. 정보화 사회의 도래로 전반적으로 국가·사회의 정보시스템에 대한 의존도가 높아지고 있는 반면 해킹·바이러스 유포, 정보시스템에 대한 불법 침입 및 마비, 프라이버시 침해 및 개인정보 오남용, 인터넷을 통한 범죄, 암호기술의 부정 사용, 전자상거래의 안전 및 신뢰성 저해, 불건전 정보의 유통 등 정보화의 역기능이 갈수록 심각해지고 있다.

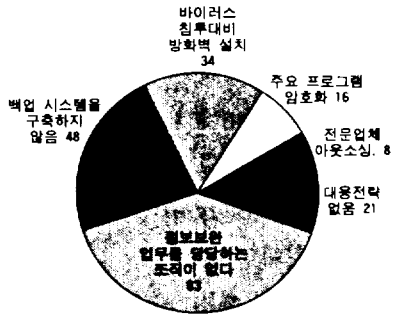
인터넷 활용은 개방성과 확장성이라는 본질에 의해 해킹 및 바이러스에 취약할 수밖에 없으며 인터넷 관련 기기와 각종 소프트웨어 역시 보안성이 완벽하지 못하다는 한계를 지니고 있다.

현재, 우리나라의 경우 해킹사고는 해마다 증가하고 있는 실정이며, 우리나라를 해킹의 경유지로 이용하는 경우가 증가하고 있는 실정이다.

이러한 정보화 역기능의 증가로 공공기관은 물론 민간영역의 기업이나 개인들까지도 정보보안에 대한 필요성을 인식하기 시작하였다. (그림 1)은 우리나라 정보 보안을 위협하는 요소 비교이다[1]. 바이러스나 사내 중요 문서 외부 유출, 그리고 해커에 의



(그림 1) 우리나라 정보 보안을 위협하는 요소 비교



(그림 2) 정보 보안 위협 요소에 대한 기업들의 대책 비교

한 사내 침투가 정보 보안에서 심각한 위협 요소가 되고 있음을 알수 있다. (그림 2)는 정보 보안 위협 요소에 대한 기업들의 대책 비교이다. 방화벽 설치, 암호화등 정보 보안에 대해 기본적인 방어 대책만 구축했음을 알고 아무런 대책도 강구하지 않은 기업도 21%나 되었다.

기업 정보에 대한 문제는 기업의 경쟁력과 국가 산업 경쟁력에 밀접한 관련이 있다. 기업의 기밀이 유출되면 해당 제품에 대한 경쟁력이 저하 될 수 있으며 이로 인해 국가 경쟁력도 저하될 수 있기 때문이다.

본 논문에서는 정보 보안 실태 조사와 문제점을 분석하고 현재 정보 보안과 관련된 장비의 추세를 살펴보았다. 이것은 추후 정보를 보안하려는 기업에게 도움을 줄 수 있다.

본 논문의 구성은 2절에서 현재 정보 보안 장비의 역할과 문제점, 그리고 추세를 설명하고 3절에서는 결론 및 추후 연구 방향을 기술하였다.

2. 정보 보안 장비의 역할과 문제점, 그리고 추이

현재 보안 시스템의 종류로는 IDS, IPS, 방화벽(firewall), 바이러스 월(Virus Wall), 무선 네트워크에 대한 보안 등을 들 수 있다.

2.1 IDS

IDS(Intrusion Detection System, 침입탐지 시스템)으로 외부 공격에 대한 탐지 역할을 수행한다. 공격, 침입, 원하지 않는 트래픽을 구별할 수 있다는 점에서 가치가 있으

며, 일부 IDS는 TCP 리셋 기능을 가지고 공격차단을 시도하기도 한다[2].

침입탐지를 하기 위해 관찰하고 있는 대상에 따라[3]

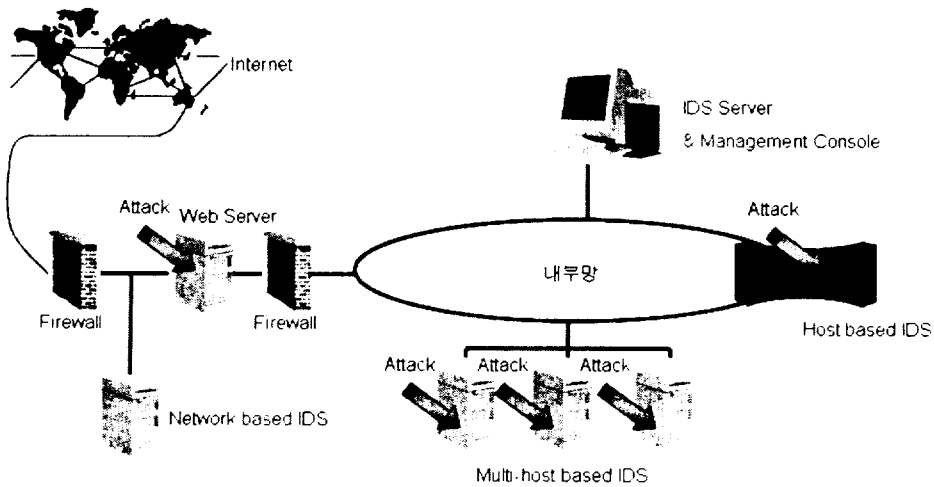
① HIDS(Host-based IDS) - 단일 시스템(Host,컴퓨터)에서 일어나고 있는 일련의 활동들을 감시하고 침입 발생에 대해 탐지하는 IDS

② NIDS(Network-based IDS) - Network상에서 일어나는 활동들을 감시하고 침입 시도를 탐지하는 IDS

③ 멀티호스트 - 여러 시스템으로부터 활동들을 감시하고 침입 시도를 탐지하는 IDS

④ Hybrid type - HIDS방식과 NIDS방식의 혼합 형태의 IDS 등이 있다.

[그림3]은 IDS가 관찰하고 있는 대상의 위치에 따라 구성한 것이다[4].



(그림 3) IDS의 구성도

2.1.1 IDS의 문제점

IDS의 경우에는 공격의 사후 탐지용으로 개발되었기 때문에 탐지만 가능하고 예방이나 차단은 어렵고, 점차로 고도화되는 공격을 막기에는 어려운 특징이 있다.

또한 서명 기반 방식을 채택함으로써, 암호화된 형태의 공격을 탐지할 수 없고, 모든 공격의 변종을 탐지하기가 쉽지 않은 단점이 있다.

즉, IDS는 기존의 공격에 대한 탐지만 가능하며, 이에 대한 해결책으로 제시되는 것이 바로 IPS(침입방지시스템)이다.

2.1.2 IDS의 현재 추이

현재 IDS의 제품의 경우 국내의 20여개와 해외의 10여개의 있으며, 네트워크 기반과 다른 보안시스템이 연동되어야 되는 특징을 지니고 있다.

〈표 1〉은 국외와 국내 IDS의 시장 규모이다[5]. IDS의 시장 규모가 증가되는 것을 알 수 있다.

〈표 1〉 국외와 국내 IDS의 시장 규모

구 분	1999	2000	2001	2002	2003	2004
국 외 ($ millions)	115.7	234.2	350.8	443.5	519.1	570.1
국 내 (₩ 백만)	-	19,300	38,662	49,549	62,937	79,000

2.2 IPS

IPS(Intrusion Prevention System, 침입 방지 시스템)는 외부의 침입을 감지함과 동시에 이를 실시간으로 차단하는 이른바 능동형 보안시스템이라 할 수 있다.

IDS는 기존의 공격에 대한 탐지만 가능하였지만, IPS는 능동적 침입방지가 가능할 뿐만 아니라, 트래픽을 조절할 수 있으며, 보안 정책의 수립도 가능한 장점이 있다. IPS는 공격 시그니처를 찾아내 네트워크에 연결된 기기에서 수상한 활동이 이루어지는지를 감시하여, 자동으로 해결 조치를 취함으로써 그것을 중단시키는 보안 솔루션이다.

IPS는 수동적인 방어 개념의 방화벽이나 IDS와는 달리 침입유도시스템이 지닌 지능적 기능과 적극적으로 자동 대처하는 능동적인 기능이 합쳐진 개념이다.

2.2.1 IPS 특징

IPS는 바이러스 웜이나 불법침입/분산서비스 거부공격(DDoS:Distributed Denial of Service)등의 비정상적인 이상신호를 발견 즉시 인공지능적으로 적절한 조취를 취한다는 점에서 방화벽이나 IDS와 차별성을 갖는다.

IDS는 이미 알려져 있는 공격 시그니처를 감시하면서 수상한 네트워크 활동을 찾아내는 것이 목적이며, 이상한 네트워크 활동을 찾아냈을 경우 해당 운영 직원에게 경고 메시지를 보내고 침입의 진전 상황을 기록하고 보고하는 것으로 끝나 문제를 즉각적으로 처리하지 못하는 반면 IPS는 침입경고 이전에 공격을 중단시키는 것이 목적이다.

현재의 정보보안 시스템과는 달리 IPS는 탐지 능력과 차단 능력을 결합한 것으로 알려지지 않는 공격 패턴에 효과적인 대응을 하고 동시에 명확한 공격에 대해서는 사전 방어 조치를 취한다.

● IPS의 장점

① 방화벽에서 취약한 요소를 보완할 수 있는 2단계의 방어(방화벽, IPS)를 제공한다.

② DoS/DDoS 등과 같은 공격을 차단시킴으로써 보안 인프라와 네트워크의 영향을 제거한다.

③ 공격에 대한 조사로 인해 소요되는 관리자 운영 부담을 없앤다.

④ 차단은 TCP 리셋 기능처럼 TCP에 한정되지 않고 모든 트래픽(IP, TCP, UDP 등)을 대상으로 한다.

IPS는 IDS에 비해 가격측면에서 비싼 편이며, 여러 가지의 장점에도 불구하고 현재 어떤 기능들을 갖추고 있어야 IPS라고 부를 수 있는가에 대한 기준이 상당히 모호하다. 예를 들어 IPS의 웜, 바이러스 차단, 네트워크 트래픽 조절 등의 기능으로 인해 바이러스 월도, 스위치도, IDS도 모두 약간의 기능을 추가하면 IPS라고 부를 수 있는 제품으로 바뀔 수 있다는 것이다[6].

2.2.2 IPS의 현재 추이

작년 하반기부터 외국 보안 업체를 중심으로 IPS 제품이 출시되기 시작되었고, 성능에 대한 검증이 어느 정도 완료됨에 따라 시장이 활성화 되고 있으며, 특히 IPS 국내 공통평가기준(CC)인증제가 2004년 4월 시행 됨으로써 가격 경쟁력이 생기게 되었다.

이러한 IPS는 기업 시장의 양대 축인 통신업체(SK텔레콤, KT)와 금융기관(국민, 우리, 신한, 하나, 한미은행 등)을 중심으로 전면 도입되고 있는 추세이다.

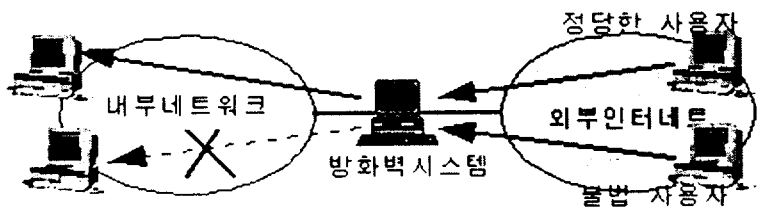
웜이나 해킹이 급증하면서 현 시점에서는 IPS가 가장 효과적인 방어 대안으로 부상하고 있다[6][7].

● 현재 IPS 구축시 요구되는 사항

① 정확하게 탐지하고 공격을 정밀하게 차단하는 인라인 장치이여야 한다.
② 라인 속도로 동작하여 네트워크 성능 또는 가용성에 악영향을 주지 않아야 한다.
③ 보안관리 환경 안에 통합되어야 한다.
④ 미래의 공격에 대한 방어를 쉽게 수용할 수 있어야 한다.
⑤ 빠른 투자회수가 가능하도록 효과적인 비용이여야 한다.

2.3 방화벽

방화벽은 외부의 공격으로부터 시스템을 보호하도록 고안된 접근 통제 방법으로, 들어오고 나가는 모든 통신을 통제함으로써 내부의 네트워크의 사용자가 외부의 또 다른 사용자 혹은 서버(server)와 통신을 한다면 사용자의 메시지는 방화벽을 통하게 되고 방화벽은 또 다른 사용자 혹은 서버에게 메시지를 전달한다. (그림 4)는 방화벽 시스템의 예이다.



(그림 4) 방화벽 시스템

2.3.1 방화벽의 문제점

방화벽은 내부의 중요한 자원과 외부 세계와의 경계를 생성하고, 정책기반의 접근제어를 효과적으로 제공하고 있지만 네트워크 사용 목적상 열린 포트를 가지게 되며, HTTP 웜, DoS공격, 변형 프로토콜을 통한 공격에는 효과적으로 막지 못하는 단점이 있다. 방화벽은 이러한 공격으로 인해 네트워크의 병목현상과 가용성을 떨어뜨리는 요인이 될 수 있다[8][9].

① 바이러스를 막을 수 없다.

방화벽은 보통 패킷의 IP 주소와 포트 번호로 접근 제어를 한다. 물론 좀더 높은 수준의 접근 제어가 가능하나 패킷 안의 데이터 내용 자체를 검사하지 않는 것이 보통

이다. 방화벽의 경우 보통 두 네트워크 사이에 존재하며, 높은 트래픽을 처리해야 하므로 데이터 자체의 내용까지 검사하면, 큰 오버헤드(overhead)가 발생하고 네트워크 대역폭에 큰 손실을 가져오기 때문이다.

② 악의적인 내부 사용자의 공격을 막을 수 없다.

방화벽은 보통 신뢰되지 않은 외부 네트워크(outbound network)로부터 신뢰되는 내부 네트워크(inbound network)를 보호하기 위한 것이 주목적이다. 따라서 경계에 대한 보안 정책을 수행할 뿐 내부 공격자에 대한 보안정책의 적용이 불가능하다.

③ 자신을 통과하지 않은 통신에 대한 제어 역시 불가능하다.

만약 내부 사용자가 방화벽을 통과하는 통신 선로가 아닌 무선이나 사설 통신 선로를 이용하여 통신을 한다면 공격자는 방화벽을 우회하여 이를 통해 내부 네트워크로 접속할 수 있으며, 내부 사용자 역시 방화벽을 우회하여 외부로 허용되지 않은 접속을 시도할 수 있다.

④ 전혀 새로운 형태의 공격을 막을 수 없다.

방화벽은 예측된 접속에 대한 규칙을 세우고 이에 대해서만 방어하기 때문에 새로운 형태의 공격에 대해서는 능동적인 적용이 불가능하다. 실제로 많은 해킹 공격이 방화벽을 우회하거나 통과하는 데 성공하여 공격을 실행한다.

2.3.2 방화벽의 현재 추이

시스코의 경우 방화벽 시장에 97년 진출하였으며 VPN, IDS, IPS 및 보안장비를 통합 관리할 수 있는 매니지먼트 솔루션을 보유하고 있다.

그 외에 주니퍼네트워크코리아, 시만텍, 넷스크린 등이 방화벽 대표적인 업체인데, 방화벽, VPN, IDP(IPS) 등의 기능이 통합된 통합보안장비를 제공하고 있다[10].

방화벽의 상용 제품은 하드웨어 플랫폼, 컨설팅, 네트워크 재설계 등으로 인한 비용이 많이 발생하므로 비용에 해당하는 완벽한 보안 해결책을 제공받는 것이 중요하다.

방화벽이 완전한 보안을 제공하는 것은 아니며, 단지 인터넷 등의 전산망에서의 보안 격리만을 제공할 뿐이다. 따라서 비효율적인 운영과 완전하지 않은 정책은 큰 문제가 될 수 있다.

● **방화벽 구축시 고려 사항[11].**

① 해당 조직이 어떻게 시스템을 운영할 것인지에 대한 정책을 반영하는가?

매우 중요한 네트워크에서의 작업을 제외하고는 모든 접속을 거부하는 식의 시스템을 운영할 것인가 아니면 덜 위협적인 방법으로 접속해 오는 트래픽에 대해 조사하고 점검하는 방식으로 시스템을 운영할 것인가라는 선택을 할 수 있다. 이러한 선택은 보안 결정권자에 달려있다.

② 어느 정도 수준의 감시, 백업 및 제어를 원하는가?

첫번째 문제로서 기관이 받아들일 수 있는 위험 수준이 세워졌다면, 이제 어떤 것을 감시하고, 허용하고, 거부할 것인가라는 체크리스트를 작성해야 한다. 즉, 기관의 전체적인 목적을 결정하고 위험 평가에 근거한 필요성 분석을 하며, 구현하고자 계획하여 사양을 마련했던 목록과 구별될 수 있는 문제점을 가려낸다.

③ 경제적인 문제이다.

우리가 여기에서 정확하게 지적할 수 있지는 못하지만 이것을 구매하는데 드는 비용과 구현에 드는 비용을 정확하게 정량적으로 산출하는 것이 중요하다. 예를 들어 완전한 방화벽 제품의 구매 비용은 무료에서 100,000 달러에 이를 수 있으며, 방화벽 시스템의 우선 설치 및 구현에 드는 비용 뿐 아니라 지속적으로 드는 비용과 지원비 등을 계산해야 한다.

④ 기술적인 측면에서 몇 가지 결정해야 할 것들

기관 내부의 네트워크와 네트워크 서비스 제공자 사이에서의 고정적 트래픽 라우팅 서비스 등에 대해서도 결정하야 한다. 트래픽라우팅은 라우터에서의 IP 수준의 스크린 규칙이나 혹은 프락시게이트웨이나 서비스에서의 응용 수준 등에서 구현되어야 한다.

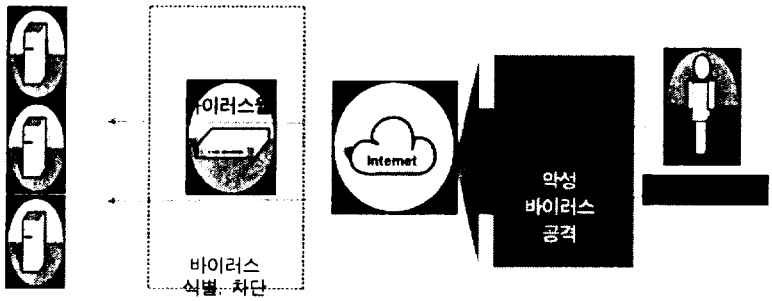
⑤ telnet, ftp, news 등의 프락시를 설치되는 외부에 노출된 기계가 외부 네트워크에 둘 것인가 혹은 하나 이상의 내부 기계와 통신을 허용하는 필터링으로서의 스크린 라우터를 만들 것인가를 결정하는 것

각각의 접근 방식은 장단점이 있는데, 프락시 기계가 고급 수준의 기록성과 잠재적인 보안 기능을 많이 구현해야 하는 만큼 또한 비용이 많이 요구되기 때문이다. 프락시는 요구되는 서비스 마다 따로 설계되어야 하며, 편리성과 보안에 드는 비용은 상대적이다.

2.4 바이러스 월

최근에 코드, 님다 등 악성 바이러스로 인한 공격으로 서버 자원의 성능 및 가용 자원에 대한 이용율이 저하되고 있는데, 바이러스 월은 이러한 악성 바이러스로부터 시

스템의 자원을 보호하는 역할을 수행한다. (그림 5)는 바이러스 월이다.



(그림 5) 바이러스 월(Virus Wall)

2.4.1 바이러스 월의 추세

엑스큐어넷은 조흥은행에 바이러스 백신 솔루션인 "비너스 바이러스 월"을 공급하고 있으며, 데이콤은 보라시큐어넷과 바이러스 월 서비스를 결합한 "보라시 바이러스 월"서비스를 제공하고 있다[12][13].

또한 "e메일 바이러스 월"이 출시되고 있는데, 이는 코드레드(CodeRed)와 님다(NIMDA)바이러스가 우리나라를 비롯한 전 세계 e메일 사용자들에게 엄청난 피해를 끼치자 이러한 피해를 막기 위해 대안으로 제시된 것이다[14].

이러한 "e메일 바이러스 월"은 실시간 e메일을 감시하여 바이러스에 감염되지 않도록 막는 제품인데, 감염된 파일이 메일을 통해 PC에 들어오지 못하게 하는 것이 주 임무이다. 특히 파일 뿐 아니라 제목과 본문 내용까지 필터링할 수 있는 것이 장점이며, 차단 목록을 정하면 위험한 e메일을 사전에 막을 수도 있다.

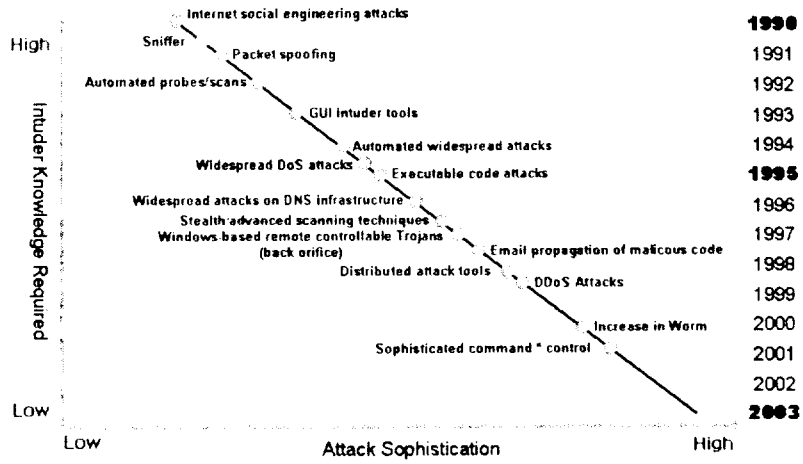
이렇듯 바이러스 월은 기업으로 확대되고 있는 추세이며, 대표적인 것으로 "e메일 바이러스 월"을 들 수 있다.

2.5 무선 네트워크 보안

무선 네트워크 사용이 급증하고 있는 추세이다. 이러한 무선 네트워크를 사용하기 위해서는 내부의 유선 네트워크에 액세스 포인트 (AP, Access Point)를 설치하여야 하여야 하는데 네트워크의 전송 가능 길이가 짧을수록 보안 측면에서 좋다.

있는 최신 인증 알고리즘을 기본으로 제공해 주며, 액세스 포인트를 통해 불법사용자가 사내 망에 접근할 수 없도록 차단하는 것이 특징이다.

(그림 6)은 네트워크 보안의 공격 경향을 보여주고 있는데, 그림에서와 같이 공격을 위해 요구되는 지식은 점차 줄어들고, 공격의 정밀도는 높아지는 경향이 있다[15].



(그림 6) 네트워크 보안의 공격 경향

*한국정보보호진흥원/2003. 7.

2.5.1 무선 네트워크 보안의 문제점

무선 네트워크 사용이 급증하고 있으나, 보안이 매우 취약해 이로 인해 생기는 위험 또한 기하급수적으로 늘어가고 있는 실정이다. 이러한 무선 네트워크는 유선 네트워크의 모든 보안 문제를 그대로 지니고 있으며 무선이라는 점 때문에 더욱 위험한데, 유선 네트워크에 비해 통신의 한계가 분명하지 않으며 방향성이 없기 때문에 클라이언트가 어느 거리, 어느 방향에서 접속하는지에 대한 정보를 얻을 수가 없다.

무선 랜의 경우 다음과 같은 이유 때문에 보안에 취약하다[16].

① 가짜 AP(Access Point) - 가짜 무선랜은 네트워크 관리자들이 통제하지 못하는 구체적인 AP로만 여겨졌으나, 오늘날 가짜 무선랜에는 노트북 컴퓨터와 무선랜 카드가 장착된 핸드헬드 기기, 바코드 스캐너와 프린터, 복사기 등 모든 무선랜 기기가 포함될 수 있다.

이러한 기기들은 거의 보안 조치가 취해지지 않은 상태이기 때문에 침입할 수 있는 입구를 쉽게 찾아낼 수 있으며, 또한 침입자들은 기업을 해킹하기 위해 악의적으로 이

런 것을 만들 수도 있다.

② 소프트 AP-얼마전까지만 해도 하드웨어 AP만이 보안의 초점이었다. 그러나 무선 네트워크 기능이 장착된 노트북 컴퓨터들은 조금만 사양을 고치면 호스트 AP역할을 수행할 수 있으며 PC텔의 소프트웨어와 같은 일반 프리웨어로도 쉽게 AP기능을 구현할 수 있다.

일명 '소프트AP'라고 알려져 있는 노트북 컴퓨터들은 가짜 AP보다도 찾아내기가 더 어려우며, 소프트 AP는 유선 네트워크 스캐닝 프로그램으로 볼 때 일반 사용자로 보이기 때문에 매우 위험하다.

③ 우연한 만남-이웃의 AP라든지 아니면 가까운 층의 무선 네트워크가 다른 회사의 공간과 겹쳐 무선 네트워크 기기들이 우연히 연결되어 있는 것을 말하는데, 기기들이 이웃 네트워크와 연결되면 이웃 사용자도 네트워크에 들어올 수 있다. 지금은 이웃 무선랜과 우연히 겹치는 것도 보안상 문제점으로 받아들여진다.

④ 악의적인 만남-어떤 회사의 노트북 컴퓨터를 소프트 AP나 다른 노트북 컴퓨터와 같은 악의적인 용도에 사용되는 기기에 연결되도록 유인하는 경우를 말한다. 또한 악의를 띤 노트북 컴퓨터가 보안으로 통제된 AP에 연결되는 경우도 마찬가지이다.

일단 악의적인 만남이 이뤄지면 해커는 무선 네트워크 기기를 발판으로 기업 네트워크의 서버라든지 다른 시스템을 공격할 수 있게 된다.

⑤ 가짜 네트워크-가짜 무선 네트워크, 혹은 AP에 연결되지 않고 2대 컴퓨터 간에 존재하는 P2P 네트워킹은 무선랜 보안에 있어 또다른 문제점인데, 이러한 가짜 네트워크들은 자동적으로 만들어질 수도 있고 의도적인 경우도 있다. 가짜 네트워크에는 인증이라든지 암호화 여부를 살펴볼 때 거의 보안이 돼있지 않다고 볼 수 있으며 결국 침입자들이 아무것도 모르는 사용자의 컴퓨터에 접속해 개인 문서라든지 공개하고 싶지 않은 정보를 빼어갈 수 있다.

● **무선 네트워크의 대응책[17][18].**

① AP보호를 위해서는 전파가 건물 내에 한정되도록 전파 출력을 조정하고, 창이나 외부에 접한 벽이 아닌 건물 안쪽의 중심부쯤에 설치하는 것이 좋으며, 쉽게 눈에 띄지 않는 곳이어야 한다.

② AP의 기본 계정의 패스워드를 반드시 재설정해야 한다.

③ AP에 대한 설정 사항으로 먼저 DHCP(Dynamic Host Configuration Protocol:IP

주소및 다른 TCP/IP 매개변수를 할당하기 위한 메커니즘으로, Host 전용 정보를 조정하고 송신하기 위한 프로토콜)를 정지시키는 것이 좋으며, 보통 AP를 검색하여, IP주소를 자동 할당하게 되면, 사설 네트워크에 대한 정보 없이도 무선 랜에 접속이 가능하다. 편리하기 때문에 무선 랜을 운용하는 곳이 많으나 보안상 매우 위험하다.

④ AP에 접근 가능한 MAC주소를 기록하여 여기에 기록된 MAC주소 이외의 다른 무선 랜 카드에 의한 접속을 차단하도록 설정하는 것이다. 실제로 꽤 효과적이다.

⑤ SSID(Service Set Identifier)는 도메인 이름으로 1차적인 접근 제어를 한다. SSID는 AP와 무선 랜 클라이언트 모두 기본적으로 any로 설정되어 있어, 아무런 설정을 해주지 않는다면 기본적으로 접속이 가능하다. SSID를 설정했다고 안심할 수는 없는데, SSID가 AP에서 브로드캐스트되기 때문에 스니퍼로 이를 캡처해서 확인해본다면 SSID는 금방 노출되기 때문이다.

⑥ WEP을 이용한 보안 설정을 한다.

그러나 WEP(Wired Equivalent Privacy)는 상호 인증을 제공하지 않기 때문에 AP는 클라이언트를 인증할 수 있으나 클라이언트는 AP를 인증할 수 없다. 따라서 공격자가 AP를 임의로 설치하는 경우 이에 대한 보안 대책이 없으며, WEP키를 주기적으로 변경하지 않고 사용할 경우 스니핑으로 암호화된 정보를 읽어낼 수 있다. 보통 WEP는 40비트의 키를 제공하며, 64비트 이하의 WEP키를 사용할 경우 30분 이내에 복호화가 가능하다.

⑦ 노트북 등의 AP접속 장비의 분실이다. 무선 랜 장비들은 보통 매우 가볍기 때문에 이러한 장비의 분실은 결국 외부인의 접속을 가능하게 한다.

2.5.2 무선 네트워크 보안의 현재 추이

현재 엑서스테크놀러지(주)가 개발한 제품은 모든 서버에 무선 네트워크의 보안상 취약점을 해결할 수 있는 최신 인증 알고리즘을 제공하고 있으며, AP를 통해 불법사용자가 사내 망에 접근할 수 없도록 차단하고 있다[19].

무선 네트워크는 보안상 허점이 많은 관계로 프로토콜 자체의 보안 기능을 제외한 다른 조치로서 제안된 것이 EAP(Extensible Authentication Protocol)와 802.1X를 이용한 인증 시스템이다. 여기에서 EAP는 무선 네트워크의 클라이언트와 RADIUS (Remote Authentication Dial-in User Service)서버간의 통신을 가능하게 하는 프로토콜이며, 802.1X는 포트에 대한 접근을 통제하는 프로토콜이다[20].

3. 결론 및 추후 연구방향

본 논문에서는 정보 보안의 위협 요소와 이에 대한 대책이 부족함을 살펴보고 정보 보안을 하기 위해 필요한 시스템으로 IDS, IPS, 방화벽, 바이러스 월의 역할과 문제점과 추세를 기술하였다. 현재의 추세는 IPS, 방화벽, 그리고 바이러스 월이 통합되는 보안 시스템 구축을 선호하고 있다. 또한 무선 네트워크에 대한 사용이 증가되고 있기 때문에 무선 네트워크에 대한 보안상의 문제점과 이에 대한 보안 대책도 기술하였다.

추후에는 각 기업에 적합한 통합적인 정보 보안 장비에 대해 연구를 할 예정이다.

《참고문헌》

[1] 이권효, 제조업체 "기업 내부정보 유출경험" 56%, 동아일보, 2004. 5. 15

[2] http://210.218.3.30/files/leesb__05/292,4,IDS의 기능

[3] http://ce.kyungil.ac.kr/~hskim/339,19

[4] http://www.penta.co.kr/ppt/penta2002/Siren XG.ppt

[5] http://www.penta.co.kr/ppt/penta2002/264,11,IDS 시장 동향

[6] http://blog.naver.com/cheguebara/120003639079

[7] 장동준, "보안시장 IPS가 뜬다." 전자신문, 2004. 5. 28

[8] 양대일, 이승재 공저 "정보 보안 개론과 실습" 한빛미디어, 2003. 11, p.448~468

[9] http://bravo.kwangju.ac.kr/%7Essroh/lecture/1076,32,방화벽 시스템의 구성요소

[10] http://blog.naver.com/pgmr24.do?Redirect=Log&logNo=80003341426

[11] http://kmh.ync.ac.kr/encycl/terms/termsF/firewall2.htm

[12] http://www.datanet.co.kr/archive/file/시큐어소프트.ppt

[13] http://www.dt.co.kr/print.html?gisaid=200307280201136069900 4

[14] http://www.hackersnews.org/data/2003/09__1/0930__34.html

[15] http://www.inews24.com/php/news__view

[16] Anil Khatod, "무선랜 보안 위협 상상 그 이상", http://www.zdnet.co.kr, 2004. 6. 1

[17] 양대일, 이승재 공저 "정보 보안 개론과 실습" 한빛미디어, 2003. 11, p.436~444

[18] http://www.securitytechnet.com/resource/hot-topic/wlan/20011015

[19] http://www.waycos.co.kr/Korean/Download/online/335,3,무선 네트워크 보안을 위한 방안들

[20] http://dcs.chonbuk.ac.kr/~ghcho/publications/정보과학0204.hwp