디지털 정보 보안에 관한 연구

고 훈* 장 의 진** 신 용 태***

◈ 목 차 ◈

1. 서 론

인터넷의 초고속 성장과 더불어 컴퓨터의 대량 보급으로 인해 전세계는 하나의 거대한 네트워크로 연결된 공동체가 되었다. 이를 기반으로 최근에는 인터넷을 통한 다양하고 많은 콘텐츠들이 개발되고 있다. 그러나 디지털 데이터의 특성상 복제가 쉽고 또한, 불법적으로 복제된 콘텐츠가 인터넷을 통해 빠르게 배포되고 있는 상황이다. 특히 해킹기술, 불법 복사 기술 등이 발전하면서 이러한 문제점들이 더욱 확산되고 있는 추세이다. 정부 및 관련 단체에서 이에 대한 대비책으로 디지털정보에 대한 보호를 위해 법적인 제도를 마련하여 시행되고 있지만, 디지털 정보의 해킹과 불법 복제가 더욱 증가되고 있는 추세이다. 게다가 대부분의 인터넷 사용자를 보면 정보보안에 대한 인식이 상당히 부족한 상태이다. 컴퓨터가 보안에 무방비한 상태에서 각종 프로그램의 설치 및 사용하여 보안에 취약하다는 것이다. 특히 사용자가 비전문가이고, 컴퓨터 네트워크 중개로 유통되는 정보의 불법적 사용이 증가됨에 따라 정보보안에 대한 대책이 새로운 문제점으로 등장하였다. 정보네트워크는 세계적인 규모로 빠르게 발전하여, 네트워크에 실린 개인의 정보가 어느 한 순간에 국경을 넘어 유통이 가능해짐에 따라서, 특정 나라의 정보시스템에서 발생한 피해가 다른 나라의 정보시스템으로 전파될 위험성이 확대되고 있다. 이런 문제를 감안하여 정보보안 및 사생활침해 대책에 있어 국내뿐만 아니라 국제적으로도 협조하여 대책을 강구하고 있다. 미국, 일본 등의 선진국들 및 기타 많은 국가들이 전산시스템 안전대책기준이나 정보처리 서비스 업자에 대한 안전대책을 실시하고 있다.

일반화된 정보시스템의 보급으로 많은 정보의 신속한 처리가 가능해짐에 따라서 다양한 개인정보의 중요 정보를 수집하거나, 저장, 그리고 이런 정보를 이용하는 발생률이 증가하고 있어, 개인 및 사업자에 관한 각종 정보가 자신도 모르는 사이에 처리되어 예상치 못한 결과를 초래하고 있다. 이에 이러한 문제에 대한 근본적인 해결이 없이는 디지털 정보화 사회의 안정적인 유지 및 전개는 기대 할 수 없게 될 것이다. 따라서 본 논문의 목적은 디지털 정보보안에 대한 개념을 확실히 정의하고 이에 관한 기술 및 방법을 조명함으로써 디지털 정보 보안에 관한 주의를 환기하고자 한다.

2. 디지털 보안

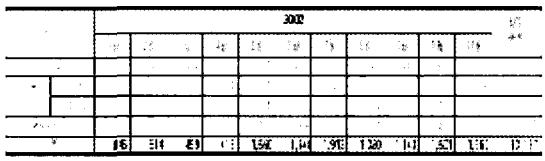
2.1 디지털 보안이란?

* 대진대학교 컴퓨터공학과 강의교수
** (주)디지캡스 연구원
*** 숭실대학교 컴퓨터학과 부교수

디지털보안이란 컴퓨터와 인터넷상에서 사용되는 모든 디지털정보를 안전하게 보호하는 것을 말한다. 즉 정보통신상에서의 디지털정보 그리고 컴퓨터 내의 디지털정보에 대한 제3자의 간섭으로부터 보호하는 것을 의미한다. 디지털정보의 보호를 위한 법적인 제도가 만들어 졌음에도 불구하고 디지털정보보안에 문제점이 계속 증가하고 있는 요인으로는 다음과 같은 것들이 있다. 첫째, 인터넷사용 자체가 개방적이라는 것이다. 전 세계에서 많은 사람들이 시공간 초월한 정보의 공유라는 장점이 있지만 그 만큼 전송되는 동안의 정보유출과 네트워크로 연결되어 있기 때문에 타 지역에서의 손쉬운 해킹기법들이 발달이 연계되어 정보유출이 쉬워졌다는 점이다. 둘째, 인터넷의 기반이 되는 프로토콜인 TCP/IP 등 기타의 인터넷을 위한 프로토콜들이 공개되어 있다는 점이다. 셋째, 해커들의 정보 교환이 쉽게 이뤄지고 있다는 사실이다. 굳이 해커가 아니라도 해킹에 관심 있는 사람이라면 인터넷상에 공개되어 있는 해킹 프로그램, 해킹 기법들에 대해서 쉽게 습득할 수 있다. 인터넷상에서는 전체적은 검열이 불가능할 정도로 엄청나게 많은 해킹관련 게시판이 운영되고 있는 상황이다. 따라서, 이러한 이유로 인해서, 디지털보안이란 의미는 예전처럼 기술적인 측면의 관점에서 벗어나서 컴퓨터 사용자, 웹 관리자들의 보안 마인드에 우선적인 과제로 인식해야 할 것이다.

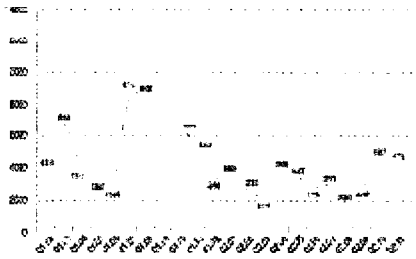
2.2 해킹 피해현황

'해커(hacker)'라는 용어는 1960년대 중반 미국 MIT공과대학에서 학생들 사이에 사용하였던 은어였다. 의미는 '아무런 이득을 바라지 않고 무수한 시행착오를 통해 시스템에 대한 정보를 탐구하는 사람' 이란 뜻이었다. 이러한 좋은 뜻이 부정적인 의미를 갖기 시작한 것은 1980년대에 들어서면서였다. 컴퓨터와 네트워크가 빠르게 발전하면서 다른 컴퓨터의 보안장치를 뚫고 들어가 정보를 훔치거나 시스템을 파괴하는 사람들이 나타나기 시작하였다. 아래의 그림 1은 2002년도 1월~11월 달까지의 해킹 피해현황이다.



(그림 1) 2002년 해킹피해현황
※ 자료 : 한국정보보호진흥원

그림 2는 같은 기간내의 바이러스 피해 현황이다.



(그림 2) 2002년 바이러스 피해현황
※ 자료 : 한국정보보호진흥원

위의 자료에서 보듯이 해킹과 바이러스는 꾸준히 증가하고 있다.

2.3 해킹 유형

해커가 특정 호스트나 네트워크 전체를 공격하는 데에도 여러 가지 형태로 나타난다. 대표적으로 루트의 권한 도용, 시스템 거부공격이 있다. 먼저 루트권한 도용은 일단 루트권한을 얻으며 시스템 내에서 불가능한 기능이 없기 때문에 대부분의 해커들이 노리는 형태이다. 그리고 서비스 거부공격(DoS:Denial of Service)는 웹상에서 인터넷 서비스를 제공하는 특정 서버를 공격하여 아예 그 서버의 본 임무인 서비스를 불가능하게 하는 형태이다.

2.4 해킹 종류

대표적인 해킹 방법으로 분류하자면 아래와 같은 방법이 있다.

2.4.1 스니핑

네트워크 보안에도 전화도청처럼 네트워크에서 주고받는 패킷을 Sniffer등의 툴을 이용하여 몰래 훔쳐볼 수가 있다. 현재 LAN의 lwnfb를 이루고 있는 이더넷(Ethernet)의 경우 IP 목적지 주소가 가리키는 호스트의 MAC(Media Access Control)을 알기 위하여 해당 IP 주소가 가리키는 서브 네트워크에 지정된 패킷을 Broadcast하게 된다. 일반적인경우 해당 IP 주소만 패킷을 받아들이게 되고 다른 호스트들은 이 패킷을 무시하게 되지만 Promiscuous Mode를 지원하는 네트워크 어댑터가 작동되어 있을 경우 서브넷을 통과하는 모든 패킷을 볼 수 있게 된다. 네트워크 보안 관리자는 어댑터들이 Promiscuous Mode로 설정되어 있는지 점검하고 이를 관리하여야 한다. 물론 Switching Hub를 사용함으로써 어느 정도 Sniffering은 막을 수 있다. 하지만 근본적인 해결책은 아니며 가장 좋은 대안은 암호화를 하여 전송패킷이 Sniffering 된다 하여도 그 정보의 내용을 파악할 수 없도록 하여야 한다.

2.4.2 스푸핑

네트워크 상에서 특정사용자를 지칭하거나 이를 나타내기 위해서 여려 형태의 방법이 있다. 보통 암호에 의한 인증이나 자신의 IP 혹은 호스트 이름에 의한 인증 과정을 통한 연결이 일반적인 방법이다. 스푸핑이란 마치 로그인 화면 같은 프로그램을 통해 사용자로 하여금 패스워드와 계정을 입력하게 패스워드를 알아내는 방식이다. 이러한 형태의 스푸칭으로 대표적인 것이 Connection Hijacking과 IP Spoofing, Sequence Number Prediction 등으로 주로 IP레빌에서 속이는 방법을 이용한다. 예를 들어 대상이 되는 호스트의 IP를 똑같이 주게 되면 Duplicate IP Address라는 에러가 발생하고 서버 시스템은 잠시 네트워크가 멈추게 되는데, 이 순간에 가짜 IP를 다시 한번 이용해 다른 시스템으로 하여금 자신이 대상이 되는 호스트로 보이게 하는 착각을 일으키게 한다. 이런 방식은 IP 뿐만 아니라 DNS와 같은 곳에서도 똑같이 적용된다.

2.4.3 TCP SYN 플로딩

Denial of Service의 일종으로 TCP 연결 시 Half-Open을 이용하여 TCP 연결을 방해하는 공격이다. 문제가 될 수 있는 것은 Half-Open 상태이다. 만약 클라이언트가 마지막 Ack를 보내지 않는다면 서버에서는 Half-Open 상태에서 계속 머무르게 된다. 이 상태의 서버에서는 TCP 연결을 위해서 자신의 메모리에 데이터를 주고받거나 연결 상태를 유지하기 위한 데이터 영역을 확보한다. 그런데 Half-Open 상태가 계속 발생하게 된다면 결국 메모리는 모자를 것이고, 서버 시스템에는 다음부터 오는 모든 TCP 연결 요청을 거부하게 된다. 이 경우 새로 요청되는 클라이언트로부터 연결만 문제가 있을 뿐이지 이미 만들어진 TCP 연결이나, 나가는 패킷에는 영향을 주지 못한다. 그러나 어떤 경우에는 메모리의 부족이 시스템 크래쉬(crash)나, 시스템이 오작동 하도록 만들기도 한다.

2.4.4 버퍼 오버플로

버퍼오버플로우를 이해하기 위해서는 먼저 프로그램이 실행되는 과정에 대한 이해와 스택에 대한 지식이 필요하다. 하나의 프로그램을 이루고 있는 함수 중 어떤 하나의 함수가 실행된다고 가정 했을 때, 프로그램이 실행되기 위해서는 프로그램의 코드가 메모리에 로딩된 후 CPU를 거쳐 실행되게 되며 메모리에 자리하게 된다. 버퍼오버플로우와 관계있는 영역은 바로 STACK 영역으로서 STACK영역에 위치하게 되는 동적 변수의 값이 할당된 영역크기 이상으로 입력되고 그 데이터의 한계를 체크하지 않을 경우 정상적인 영역을 넘어 리턴어드레스의 영역까지 데이터가 입력되게 되는데 이것은 함수의 실행 후 돌아올 어드레스가 변경되는 것을 뜻한다. 이 경우, 돌아올 주소에 임의의 명령어를 놓아둘 경우 해커가 원하는 명령어를 마음대로 실행할 수 있게 되는데 이것을 바로 버퍼오버플로우라고 하는 것이다. 따라서 외부로 접근 가능한 서비스는 버퍼오버플로우의 가능성이 있는 것이기 때문에 항상 최소한의 서비스만을 open하도록 하는 것이 중요하며 open된 서비스의 경우에도 항상 새로운 취약점이 발견되었는지 여부를 확

인하여야 한다. 대표적인 버퍼오버플로우 취약점들은 아래와 같다.

· bind 버퍼오버플로우 취약점
· rpc.statd 버퍼오버플로우 취약점
· Windows NT IIS 취약점

2.4.5 취약성을 이용한 공격

소프트웨어를 개발하는 사람이라면 누구나 알고 있듯이 프로그램에는 버그라는 것이 있다. 버그는 간단한 것에서부터 시스템을 다운시키는 등 아주 심각한 것까지 다양하게 있는데, 재미있는 사실은 대부분의 사람들이 같은 부분에서 실수를 한다는 것이다. 취약성을 이용한 공격은 바로 이런 특징을 이용한 것이다. CERT 등의 많은 기관에서 매일 새로운 취약성을 발표하고 있다. 이에 대처하기 위해서 시스템 개발 회사 등에서 제품 발표 시 취약성을 해결하기 위한 방안을 제시하고는 있지만 실제로 이를 적용하는 시스템들은 그렇게 많지 않기 때문에 대부분의 시스템들이 취약성을 가지고 있다고 할 수 있다. 만약 네트워크를 통한 접근을 허용하는 취약성이 있다면 이것은 바로 해킹을 시도하여 성공할 수 있는 확률을 아주 높여주는 것으로 아주 위험하다고 할 수 있다. 보안 소프트웨어도 이런 취약성이 존재하기 때문에 보안 소프트웨어로 시스템을 안전하게 보호하는 장치를 하였다고 자신하여도 시스템들이 지속적으로 해킹의 대상이 되고 해킹 당해서 결과가 계속 나오는 이유도 바로 이런 취약성을 지속적으로 해결하기 위한 노력을 게을리하기 때문에 발생된다고 할 수 있다.

2.4.6 서비스 거부공격

서비스거부(Denial of Service)공격, 즉 시스템의 정상적인 동작을 방해하여 사용자에 대한 서비스의 제공을 거부하게 만드는 공격 또한 기존의 다른 어떤 종류의 위협에 못지않게 심각한 것이라고 할 수 있다. 더구나 이 같은 서비스거부공격은 시스템 침입과 같은 다른 유형의 공격에 비해 공격의 흔적을 거의 남기지 않기 때문에 가해자를 찾기가 어렵기 때문에 보다 큰 위협이 되고 있다. 왜냐하면 공격자의 위치가 추적될 염려가 비교적 적기 때문에 다른 공격 수단에 비해 남용될 소지가 많기 때문이다.
이 외에도 취약점 시스템에 해킹 프로그램 서버를 설치해 놓고 정보를 수집하는 백도어와 트로이 목마가 있고, 어떤 프로그램이 임시 파일을 만드는 특성을 이용하는 Race Condition 방법 등이 있다. 그리고 디지털 콘텐츠의 저작권 보호 및 유통 인프라 시스템을 구축하는데 필수적인 기술인 DRM(Digital Rights Management)가 있다.

3. 디지털 보안기술 요소

디지털 정보의 안전성 및 보호뿐만 아니라 강력한 보안 기능을 이용한 불법 복제와 무분별한 불법 유통을 막아주는 다양한 기술이 개발되어야 한다. 이를 위해서 현재 디지털 정보 보호를 위한 보안서비스들이 필요 되고 있다.

· 기밀성(confidentiality)
· 정확성(accuracy)
· 사용자인증(authentication)
· 데이터 무결성 보장(integrity)
· 부인봉쇄(non-repudiation)
· 접근제어(access control)
· 가용성(availability)
· 유용성(utility)

위에 열거한 기술들 제공해 주기 위해서 필요한 기능들이 암호화기술, 인증기술 등이 있다. 디지털 정보를 보호하는 가장 기본적인 기술이 암호화기술이다. 암호화 기술이란 특정키를 보유한 사람만이 특정정보를 볼 수 있도록 하는 기술이다. 현재의 암호화기술로는 대칭 키 방식과 비대칭 키 방식이 있다. 대칭 키 방식은 암호화할 때의 키와 복호화할 때의 키가 서로 같다. 대칭 키 방식의 장점으로는 암호화하는데 비대칭 키 방식보다는 빠르지만 키의 분배 및 관리하는 데에 문제점이 발생할 수 있다. 따라서 키 전달 과정에서 보안상의 문제점이 있다. 이에 비해 비

대칭 키 방식은 암호화할 때의 키와 복호화할 때의 키가 서로 다르기 때문에 키의 분배를 효과적으로 해줄 수 있다는 장점이 있지만, 암호화하는데 처리하는 시간이 대칭 키 방식보다 느리다는 단점이 있다.

인증기술은 디지털 정보의 이용자가 적법한지 아닌지를 확인하기 위한 과정으로 다양한 기술들이 활용되고 있다. 가장 간단하고 쉬운 방법으로 많이 사용되고 있는 ID와 비밀번호를 이용하는 방법이 있지만, 최근 백도어 해킹 방법 등에 의해서 많이 노출될 수 있다. 이외에도 최근에 활발히 연구가 진행 중인 생체인증 기술을 이용하여 지문인식이나 홍채인식, 정맥인식, 영상인식과 같은 방법이 있다.

4. 디지털 보안기술

디지털 정보 보안기술은 크게 네트워크 시스템에 접속하는 것을 차단하는 기술과 정보내용 자체를 보호하는 기술, 이렇게 두 가지로 분류할 수 있다.

4.1 네트워크 접속 차단 기술

네트워크 접속 차단 기술로는 방화벽(Firewall)과 침입차단시스템(IDS)등이 있다.

4.1.1 방화벽

소프방화벽은 네트워 게이트웨이 서버에 위치하고 있는 일련의 연관된 프로그램들로서, 다른 네트웍의 사용자들로부터 사설 네트웍의 자원들을 보호해준다. 방화벽은 외부인이 자신의 공개되지 않은 자원에 접근하는 것을 막고, 자기회사의 직원들이 접속해야할 외부의 자원들을 통제하기 위해 기업의 인트라넷과 인터넷 사이에 설치된다. 기본적으로 방화벽은 라우터 프로그램과 밀접하게 동작함으로써, 모든 네트웍 패킷들을 그들의 수신처로 전달할 것인지를 결정하기 위해 검사하고, 여과한다. 또한 방화벽은 워크스테이션 사용자 대신 네트웍에 요청을 해주는 프럭시 서버의 기능을 아예 포함하거나 또는 함께 상호 협력하여 동작한다. 방화벽은 네트웍의 다른 부분들과는 별개로, 특별히 지정된 컴퓨터에 설치되는 경우가 많은데, 이는 들어오는 요구가 사설 네트웍 자원으로 곧바로 전달되지 않도록 하기 위한 것이다. 방화벽의 차폐방법에는 몇 가지가 있다. 단순한 방법 중 하나는 들어오는 요구가 받아들일 만한 도메인 이름이나 IP 주소로부터 오는 것인지를 확인하는 것이다. 이동중인 사용자들을 위해서는 보안접속절차나 인증확인 등을 통해 사설 네트웍에 원격접속 할 수 있도록 허용한다. 방화벽 제품들을 만드는 회사들이 꽤 있다. 방화벽에 포함되어야할 기능으로는, 사용기록, 보고, 공격이 시작된 시점에서의 자동경보, 그리고 방화벽의 제어를 위한 그래픽사용자 인터페이스 등이 있다. 방화벽의 종류에는 아래와 같은 종류가 있다.

- 패킷 필터링 방식
- 어플리케이션 게이트웨이 방식
- 써킷 게이트웨이 방식
- 하이브리드 방식

패킷 필터링 방식은 OSI 모델에서 네트웍 층(IP 프로토콜)과 전송 층(TCP 프로토콜)에서 패킷의 출발지 및 목적지 IP 주소 정보, 각 서비스의 Port 번호, TCP Sync 비트를 이용한 접속제어를 한다.

어폴리케이션 게이트웨이 방식은 각 서비스별 프락시를 이용하여 패킷 필터링 방식처럼 IP주소 및 TCP Port를 이용하여 네트웍 접근 제어를 할 수 있으며, 추가로 사용자 인증 및 파일 전송 시 바이러스 검색 기능과 같은 기타 부가적인 서비스를 지원한다.

써킷 게이트웨이 방식은 방화벽을 통해서 내부 시스템으로 접속하기 위해서는 먼저 클라이언트 측에 써킷 프락시를 인식할 수 있는 수정된 클라이언트 프로그램이 필요하다. 따라서, 수정된 클라이언트 프로그램이 설치되어 있는 클라이언트만 써킷 형성이 가능하다.

하이브리드 방식은 이 방화벽은 서비스의 종류에 따라서 사용자의 편의성, 보안성 등을 고려하여 방화벽 기능을 선택적으로 부여할 수 있지만,

서비스의 종류에 따라서 다양한 보안 정책을 부여함으로써 구축 및 관리에 어려움이 따를 수 있다.

4.1.2 침입차단시스템(IDS)

IDS는 Intrusion Detection System(침입탐지시스템)의 약자로, 단순한 접근 제어 기능을 넘어서 침입의 패턴 데이터베이스와 Expert System을 사용해 네트워크나 시스템의 사용을 실시간 모니터링하고 침입을 탐지하는 보안 시스템이다. IDS는 허가되지 않은 사용자로부터 접속, 정보의 조작, 오용, 남용 등 컴퓨터 시스템 또는 네트워크 상에서 시도됐거나 진행 중인 불법적인 예방에 실패한 경우 취할 수 있는 방법으로 의심스러운 행위를 감시하여 가능한 침입자를 조기에 발견하고 실시간 처리를 목적으로 하는 시스템이다. 침입이란 시스템에 대한 고의적 불법적인 행위를 말하며 시스템의 불법침입, 중요정보의 유출 및 변경, 훼손, 불법적인 사용, 그리고 컴퓨터 바이러스 및 서비스거부 등과 같은 구체적인 형태로 나타난다. 침입탐지시스템은 이러한 불법적인 침입행위를 신속하게 감지하고 대응하는 소프트웨어를 말하며 간단하게는 로그파일분석에서부터 복잡한 실시간 침입탐지시스템까지 다양한 소프트웨어가 존재한다.

4.1.5 VPN 기술

VPN은 공중 통신망 기반시설을 터널링 프로토콜과 보안 절차 등을 사용하여 개별기업의 목적에 맞게 구성한 데이터 네트웍이다. 가상 사설망은 오직 한 회사에 의해서만 사용될 수 있는 자체망이나 전용회선과 대비되는 개념이다. VPN은 모든 회사들이 저마다 개별적으로 회선을 임차하는 것보다, 공중망을 공유함으로써 비용은 낮추면서도 전용회선과 거의 동등한 서비스를 제공하려는 아이디어에서 출발하였다. 전화회사들은 음성 메시지에 대해 보안이 유지되는 공유자원을 제공한다. 가상 사설망은 데이터를 위해서도 역시 보안이 유지되는 공중망 자원의 공유를 가능하도록 한다. 오늘날 가상 사설망을 원하는 회사들은 주로 엑스트라넷이나 넓은 지역에 퍼져있는 지사들 간의 인트라넷에 이를 이용한다. 가상 사설망은 공중망을 통해 데이터를 송신하기 전에 데이터를 암호화하고, 수신측에서 복호화한다 (암호를 다시 푼다). 암호화는 데이터뿐 아니라, 부가적인 차원의 보안으로서 송수신지의 네트웍 주소도 포함된다. 마이크로소프트, 3Com그리고 몇몇 다른 회사들이 PPTP라는 표준 프로토콜을 제안하였으며, 마이크로소프트는 이 프로토콜을 윈도우NT 서버에 내장시켰다. 마이크로소프트의 PPTP와 같은 VPN 소프트웨어는 대개 회사의 방화벽 서버에 설치되는 보안 소프트웨어도 마찬가지로 지원한다.

4.2 암호화 응용 기술

암호의 기본적인 기능은 다음과 같다. 첫째 기밀성 부여. 기밀성이라는 것은 어떤 비밀 정보가 있을 때 권한이 있는 사람을 제외한 모든 다른 사람이 읽을 수 없는 형태로 바꾸는 것을 말한다. 두번째로는 무결성이 있다. 무결성이란 데이터를 생성한 후에 나중에 이 데이터가 변경되지 않았다는 것을 증명하는 것이다. 세번째로는 인증이 있다. 우리가 실생활에서 문서에 서명을 하듯이 전자 문서에 전자서명을 함으로서 인증을 제공한다. 암호화에는 대칭키 방법과 비대칭키 방법이 있다.

4.2.1 비밀키 방식

암호 작성 및 해독 기법에서, 개인키란 암호 / 복호를 위해 비밀 메시지를 교환하는 당사자만이 알고 있는 키이다. 전통적으로 비밀키를 이용한 암호 작성 및 해독 기법에서, 키는 각 메시지를 암호화하고 복호화할 수 있도록 전달자에 의해 공유될 수 있었다. 그러나, 이 시스템의 최대 약점은 만약 한쪽 편이 키를 잃어버리거나 도난당하면, 그 암호화 시스템은 깨지고 만다는 데 있다. 보다 최근의 대안은, 공개키와 개인키의 조합을 사용하는 것이다. 이 시스템에서, 공개키는 개인키와 함께 사용된다.

4.2.2 공개키 암호화 방식

통신을 할 때 암호는 송신자와 수신자가 같은 비밀키를 이용하므로, 송신자는 문서를 암호화해

서 송신하고 수신자는 수신한 암호문을 같은 비밀키를 이용하여 복호화 한다. 이러한 방법은 잘 알려진 대칭키 암호화 방법이다. 이 방식에서의 문제점은 아무도 모르게 송신자와 수신자가 공통의 비밀키를 어떻게 결정하느냐 이다. 만약 그들이 물리적으로 멀리 떨어진 곳에 있다면 그들은 믿을 수 있는 운반자나 전화, 또는 다른 전송수단을 이용하여 비밀키의 유출을 막으면서 키를 분배해야 한다. 그러나 누군가가 이 비밀키를 중간에서 가로채서 알아내면 그는 모든 편지를 읽을 수 있고, 암호화되고 인증된 모든 데이터를 변조 할 수 있게 된다. 키의 생성, 전송, 보관을 키관리라 한다. 모든 암호시스템은 키관리 문제를 가진다. 따라서 모든 비밀키 암호화 시스템은 모든 키를 비밀로 하여한 한다. 개방형 시스템에서 많은 사용자가 있을 때 비밀키 암호화 시스템은 각 사용자마다 각기 다른 공통키를 가져야 하므로 키관리에서 문제점을 가지게 된다. 공개키 암호화 시스템의 개념은 1976년 Whitfield Diffie와 Martin Hellman 에 의해서 키관리 문제점의 해법으로서 제안되었다. 그들이 주장하는 시스템에서 키는 쌍으로 존재하고, 하나는 공개키 다른 하나는 비밀키라 말한다. 각 사용자의 공개키는 공개되고 비밀키는 비밀로 한다. 모든 통신은 공개키를 포함하고 비밀키는 포함하지 않으므로 전송자와 수신자간의 키분배문제는 없어졌다. 누구나 공개키를 이용하여 비밀정보를 보낼수 있다. 그러나 비밀키를 가진 사람만이 이 정보를 복호화해낼수 있다. 게다가 공개키 암호는 데이터 암호뿐만 아니라 인증에서도 사용될 수 있다.

4.2.3 키관리

키의 생성, 전송, 보관을 키관리라 한다. 모든 암호시스템에는 키가 사용된다. 키의 관리를 어떻게 하느냐에 따라서 보안정도가 달라진다. 공개키 알고리즘이던지 블럭 알고리즘이던지 비밀키를 생성하기 위해서는 랜덤 넘버가 필요하다. 랜덤 넘버를 생성하기 위해서 다이오드의 노이즈와 같은 하드웨어를 이용하거나 사람이 키보드를 치는 시간 등을 이용하기도 했다. 그러나 이러한 것들은 랜덤이 아니라는 것이 증명되었다. 이로서 랜덤 시드로부터 랜덤 넘버를 생성하는 의사 랜덤 넘버 생성기가 제안되었다. 이것은 모든 랜덤넘버가 같은 확률로서 생성된다. 이렇게 생성된 키는 일정한 기간만 사용되고 소멸되어야 한다. 그 이유는 암호분석 때문이다. 우리는 암호문을 생성할 때 키를 사용한다. 이때 공격자는 비밀키를 찾아낼 수 있을 만큼 많은 암호문을 저장한다. 그러면 공격자는 당신의 모든 암호문을 읽을 수 있을 것이다. 키의 생명기간을 갖는 또 다른 이유는 보관된 키를 공격자가 알아낼 수 있다는 점이다. 주기적으로 키를 바꾸어 주지 않는다면 자신도 모르게 어떠한 공격자가 자신의 키를 알고 있을 수 있다.

4.2.4 암호 프로토콜

정보화 사회에서는 종이 문서에 기반을 둔 기존의 모든 업무가 고도로 발달된 통신처리 및 정보처리 기술에 의해 전자문서에 기반을 둔 새로운 형태의 업무로 전환된다. 그러나 현재의 업무가 정보화 사회에 알맞은 전자적인 방법을 이용한 업무로 변환되기 위해서는 해결해야 할 몇 가지 문제가 있다. 예를 들어, 현재의 부동산 계약 관계를 자세히 고찰해 보면 다음과 같은 안전성에 관련된 중요한 특성을 내포하고 있음을 알 수 있다.

- 계약 당사자간의 상대방의 신분 확인 (주민등록증)
- 계약 문서의 확인 (문서 인증)
- 계약 도장의 인증(인감 증명)
- 동시성 (동일한 장소에서 동시에 계약서에 인감을 날인)

물론 정보화 사회에서는 전자계약도 위의 특성을 만족시켜야 한다. 계약 당사자간의 상대방의 신분을 확인하는 것이 개인 식별 문제, 계약 문서의 내용을 확인하는 것이 인증문제, 인감도장을 전자적으로 실현하는 것이 전자서명 문제이다. 특히 통신망을 통하여 전자적으로 동시성 문제를 해결하는 것은 매우 어려운 문제들로써 현실적으로 불가능해 보이기도 한다. 이와 같이 안전성에 관련된 많은 문제들을 해결해 주는 분

야가 암호 프로토콜이다.

암호 프로토콜은 기존의 통신 프로토콜에 정보 보호 이론을 부가하여 고도의 정보처리 및 통신을 하는 프로토콜을 의미한다. 따라서 암호 프로토콜은 단순히 암호 알고리즘과는 달리 서로 모르는 송신자라도 수신자라도 통신망을 이용하여 서로의 목적을 이룰 수 있도록 하는 상호 통신 알고리즘을 의미한다.

암호 프로토콜의 예는 동전 던지기(coin flipping), 오브리쉬어스 트랜스퍼(oblivious transfer, 알아채지 못하는 전송), 영지식 상호 증명(ZKIP: Zero Knowledge Interactive Proof) 등이 있다. 특히 영지식 상호 증명 기술은 암호 프로토콜의 안전성에 관한 모델로 통칭되기도 하며, 영지식 상호 증명 방식의 암호 프로토콜은 많은 응용 분야를 가지고 있다. 영지식이란 그 지식을 누출하지 않고 상호 증명할 수 있는 기법이다. 물론 전자투표 등의 경우에도 암호 프로토콜 기술은 필수적이다.

4.2.5 IPSec 기술

IP Security. 네트워크나 네트워크 통신의 패킷 처리 계층에서의 보안을 위한 표준이다. IPSec은 데이터 송신자의 인증과 데이터 무결성을 제공하는 AH(Authentication Header)와, 송신자의 인증 및 데이터 무결성과 암호화를 함께 제공하는 ESP(Encapsulating Security Payload) 등, 두 종류의 보안 서비스를 제공한다. 이러한 각 서비스에 관련된 명확한 정보는 IP 패킷 헤더의 뒤를 잇는, 헤더 속의 패킷에 삽입된다. ISAKMP/Oakley 프로토콜과 같은 별개의 키 프로토콜들이 선택될 수 있다.

4.2.6 SSL 기술

SSL은 WWW(World Wide Web)를 통해 정보를 전송할 때 보안을 위해 서버에서 사용되는 암호화 시스템이다. SSL 사용가능 서버는 중요한 데이터를 클라이언트에 전송하기 전에 암호문으로 만들어 정보를 가로챈 제삼자가 데이터를 읽을 수 없도록 한다. 클라이언트는 서버로부터 데이터를 받은 후 암호를 해독하여 데이터를 읽는다. 웹 서버에서 SSL을 사용하면 클라이언트와 서버 사이에 전송된 정보의 보안을 유지하고, 또한 클라이언트가 서버를 인식하여 인증할 수 있도록 도와준다. 일단 서버가 디지털 인증을 갖게 되면, Netscape Navigator 및 Microsoft Internet Explorer와 같은 SSL 사용가능 브라우저가 SSL을 사용하여 서버와 보안 통신을 할 수 있다. 사용자는 SSL을 사용하여 쉽게 인터넷 또는 개인 인트라넷을 통해 보안 가능 웹사이트를 구축할 수 있다. SSL을 통해 HTTP를 지원하지 않는 브라우저는 HTTPS를 사용하는 URL을 요청할 수 없다. SSL 사용불가능 브라우저는 보안 통신이 필요한 양식의 제출을 허용하지 않는다. SSL은 보안 데이터 교환을 사용하여 클라이언트와 서버간에 보안 연결을 시작한다. 보안 데이터 교환 도중 클라이언트와 서버는 세션에 사용될 보안키와 암호화에 사용될 알고리즘에 동의한다. 클라이언트는 서버를 인증하며, 서버는 선택적으로 클라이언트 인증을 요청할 수 있다. 데이터 교환 이후, SSL은 다음을 포함하는 서버 응답과 HTTPS 요청의 모든 정보를 암호화하고 해독하는데 사용된다.

- 클라이언트가 요청하는 URL
- 제출되는 모든 형식의 내용
- 사용자 이름 및 암호와 같은 액세스 권한 정보
- 클라이언트와 서버 사이에 전송된 모든 데이터

HTTPS는 SSL과 HTTP를 결합하는 고유 프로토콜 이니다. SSL 보호 문서에 연결되는 HTML 문서에서 https://를 앵커로 지정해야 한다. 클라이언트 사용자는 SSL 보호 문서를 요청하기 위해 https://를 지정하여 URL을 열 수도 있다. HTTPS (HTTP + SSL)와 HTTP가 각각 다른 프로토콜이며 서로 다른 포트(각각, 443과 80)를 사용하기 때문에 동시에 SSL과 비-SSL 요청을 수행할 수 있다. 이 기능을 통해 특정 정보는 보안 요청을 하는 브라우저에만 제공하면서 보안이 없는 사용자에게 정보를 제공할 수 있다. 이 기능으로 소매업체는 사용자로 하여금 보안 없이 상품을 조회하도록 한 후, 보안을 사용하여 주문 양식을 채우고 신용 카드 번호를 전송하도록 한다.

5. 최근 기술 동향

정보보호 발전 과정은 크게 4단계로 구분할 수 있다. 첫 번째는 1970년 이전을 정보보호 산업 태동기라 분류하고 이때는 전화, 텔렉스 등에 의해 전송되는 국가기관의 통신 내용을 보호하기 위한 통신 장비가 발전되었다. 1970년대 후반에 데이터 암호표준(DES)을 미국 국립 표준국이 국가 표준으로 지정하였다. 1980년대부터 1990년대 초반까지를 정보보호 산업 형성기라 한다. 이때는 컴퓨터와 커뮤니케이션의 통합과 함께 정보보호 부문의 산업화가 강력하게 추진되었고 DES방식의 데이터 암호화 제품 및 사용자 인증 제품을 주로 사용하던 시기였다. 1990년대 중반부터 200년대 초반까지를 정보보호 산업 성장기라 하겠다. 이 기간에는 인터넷의 보급이 빠르게 확산되었고 정보통신 시스템의 이용 증가에 따라서 디지털 정보에 대한 문제점, 즉 해킹사고와 바이러스가 사회적인 문제점으로 발생한 시기였다. 따라서 이를 해결하기 위한 침입차단시스템, 방화벽, 바이러스 백신 등의 개발이 활기를 띠고 있다. 2000년대 이후를 정보보호 산업 안정기라 하고 있지만, 오히려 정보보호 관점에 봤을 땐, 빈번한 해킹사고, 개인정보 유출 등 인터넷의 많은 단점이 크게 대두되고 있다. 정보통신부는 최근 발생했던 '1.25 인터넷대란'을 계기로 정보보호 취약 부분에 대한 점검을 강화하는 동시에 중장기적인 정보보호대책 및 정보보호 기술개발을 위한 대책을 수립해 추진하기로 했다. 정보통신부가 밝힌 정보보호 기술 개발로는 크게 공통기반 기술과 시스템/네트워크 보호기술, 그리고 응용서비스 보호기술로 나누어진다.

먼저 공통 기반 기술 부문은
· 생체인식처리기술
· 생체인식알고리듬
· 스텔스 정보보호 프로토콜
· 유니버설 고속 보안 프로세서
· 기가비트급 차세대 암호처리 프로세서
· 암호알로기듬연산 고속화 기술
· 암호알고리듬 연산 고속화 기술
· 무선인터넷을 위한 PKI 구축기술 등이 있다.

시스템/네트워크 보호기술 부분은
· 차세대 능동형 네트워크 정보보호 시스템
· 차세대 이동정보 보호기술
· 인터넷 멀티캐스트 보안
· 인터넷 정보보호 소프트웨어 기술
· MT2000용 무선인터넷 보안 및 USIM 칩 세트
· 차세대 무선인터넷 정보보호기술
등을 개발하는데 중점을 두고 있다.

이외에 응용 서비스 보호기술 개발 부분은
· 차세대 전자거래 정보보호 기술
· 가입자 단말 정보보호 기술
· 차세대 전자지불 기술
· 안전한 전자계약/입찰/투표 시스템 개발
등을 포함하고 있다.

6. 결 론

지금까지 빠르게 발전하는 인터넷에서 발생하는 여러 가지 문제점들에 대해서 알아보았다. 또한 이를 해결하기 위한 여러 가지 방안 및 보안 기술에 대해서도 살펴보았다. 인터넷상의 많은 문제점들은 이전의 단순히 타인의 홈페이지에 불법적으로 접속하여 그림이나 글자를 바꾸는 차원을 뛰어 넘어 이제는 은행이나 금융의 네트워크 망을 이용하여 불법적으로 타인의 금융정보를 얻어내는 불법행위가 증가하고 있다. 많은 개발업체에서 이런 불법행위를 방지하기 위한 많은 기술들을 개발하고 있다. 그러나 대부분의 많은 은행을 포함한 많은 기업들은 정보보안에 대한 마인드가 굉장히 부족한 상태이다.
정보보호 산업은 주요 정보통신 기반 구조로서 안전과 보안 등 국가안보에 직결되는 속성상 다른 산업과는 달리 국가가 직접 육성하는 추세이다. 정부가 적극적인 정보보호 산업에 대한 발전 방안을 계획한 대로 얼마나 잘 이루어 내느냐가 중요하다. 그러기 위해서는 암호알고리즘 등 정보보안 핵심기술의 확보 및 개발, 표준화, 보안 담당의 전문인력 양성, 보다 강력한 법체계 수립 및 시행이 중요하며 마지막으로 업체들은 이미 개발해 놓은 보안 제품들에 대해서 계속적으로 아낌없는 투자로 제품에 대한 품질을 향상시켜야 할 것이다. 정부는 전문인력의 중요성을 감안해 4개의 대학정보보호연구센터(ITRC)에 통해 암호, 인증, 시스템 보호, 네트워크 보호기술 분

야의 전문가 양성을 추진하고 있으나 산업 성장에 비춰보면 그 수가 턱없이 모자라는 실정이다. 또한 질 높은 정보보호인력을 양성하는 방안을 좀 더 구체적으로 마련해야 할 것이다.
그렇지만 무엇보다도 보안담당자의 끊임없는 시스템의 보안감시가 필요하다라고 할 수 있겠다.

참 고 문 헌

[1] "정보보호산업 시장동향 및 전망, 주간기술동향", 한국전자통신연구소, 1055호, 2002.
[2] 성태경, "인터넷 정보보안에 관한 연구", 산업연구 제11집, 1999. pp241~246
[3] 이문구, "침입 차단 시스템을 위한 FTP 프록시 보안 모델의 구현", 한국통신정보보호학회 논문지 제 10권 제2호, 2000.6
[4] National Bureau of Standards, "Data Encryption Standard," Federal Information Processing Standards Publication 46, Jan. 1977.
[5] IST, NIST SP 800-16, "Information Technology Security Training Requirement", 1998.
[6] S. Bellovin and M. Merritt. "Augmented Encrypted Key Exchange : A Password-Based Protocol Secure against Dictionary Attacks and Password File Compromise," ACM Conference on Computer and Communications Security 1993,pp. 244~250.
[7] Richard E. Smith "Internet Cryptography" Addison Wesley, 5th-Edition, 2002.

◐ 저 자 소 개 ◑

고 훈

1998년 호원대학교 컴퓨터학과 (학사)
2000년 숭실대학교 컴퓨터학과 통신연구실 (석사)
2002년 숭실대학교 컴퓨터학과 통신연구실 (박사수료)
2000년~2002년 (주)지오나스 선임연구원
2002년~현재 : 대진대학교 컴퓨터공학과 강의교수
2003년~현재 : 한국정보보호학회 편집위원
관심분야 : 암호화프로토콜, 정보보안, 인터넷보안, 전자서명, 네트워크 보안

장 의 진

1999년 숭실대학교 컴퓨터학과 (학사)
2002년 숭실대학교 컴퓨터학과 통신연구실 (석사)
2002년~현재 : 디지캡 기술연구소 선임연구원
관심분야 : DRM, 네트워크 보안, 암호화 프로토콜, 정보보안, 인터넷보안, 전자서명

신 용 태

1985년 한양대학교 산업공학 (학사)
1990년 Univ. of Iowa (전산학석사)
1994년 Univ. of Iowa (전산학 박사)
1994년~1994년 Univ. of Iowa computer Science Dept. 객원교수
1994년~1995년 : Michigan State Univ Computer Science Dept. 객원교수
1995년~현재 : 숭실대학교 컴퓨터학과 부교수
2000년~현재 : (주) 디지캡 대표이사
관심분야 : 암호화프로토콜, 정보보안, 인터넷보안, DRM