이것만은 알아야 할 네트워크 보안 이야기

Part 4. VPN _ 암호와 검증과 인증의 결정판

글. 이선응 아이크래프트 수석

연재 목차

이번 시간에는 VPN에 대해 소개하도록 하겠다. VPN은 Virtual Private Network의 약자로 가상사설망을 뜻한다. 독립된 하나의 건물 안에 구성된 네트워크나 대학 캠퍼스같이 짧은 거리에 모여 있는 건물 간에 연결된 네트워크를 보통 LAN(Local Area Network)이라고 한다. 그리고 이런 LAN들을 연결한 망을 WAN(Wide Area Network)이라고 한다. [그림 1]과 같이 서울, 부산, 대전 방송국은 하나의 LAN으로 구성되어 있고, 이렇게 여러 개의 방송국 LAN을 연결하는 망을 WAN이라고 할 수 있다. LAN은 단말 장비를 길어야 수십 미터에서 100M 범위를 스위치라는 장비를 통해 연결하기 때문에 비교적 구성이 쉬운 편이다. 하지만 WAN의 경우 LAN 그룹 간의 거리가 수십 ~ 수백 km 단위로 떨어져 있기 때문에 이런 망을 구성하기 위해서는 큰 비용이 발생한다. 일반적으로는 KT 같은 망 사업자의 네트워크망을 임대하여 구성하기 때문에 낮은 속도에 비해 많은 임차 비용이 발생하게 된다. 2000년 초~중반에는 1.5Mbps의 속도를 제공하는 임대사설망을 운영하기 위해서 한 달에 150만 원을 지불한 적도 있었다.

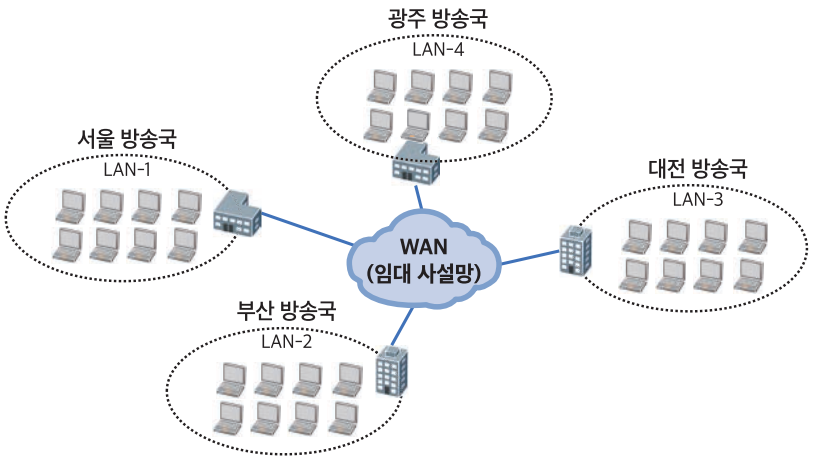

그림 1. LAN과 WAN의 범위

이런 비용적인 문제를 해결하기 위해 등장한 기술이 VPN이다. 인터넷의 보급이 급속도로 늘어나면서, 모든 조직은 저렴한 비용으로 인터넷 연결이 가능하게 되었다. 인터넷망은 일종의 공공망이라고 할 수 있다. 저렴한 비용에 빠른 속도로 통신이 가능한 장점이 있는 반면에, 누구나 접속할 수 있어 사설망에 비해 기업들의 업무 트래픽을 보내기에는 보안성이 떨어지는 단점이 있었다. VPN 기술은 인터넷망을 사용할 때 발생할 수 있는 자료 유출의 문제를 해결하기 위해 별도의 장비를 통해 트래픽을 암호화해서 송신하고, 수신하는 장비에서 암호화를 풀어서 클라이언트에 데이터를 전달하는 방식으로 동작한다. [그림 2]와 같이 별도의 VPN 장비를 각 지역국사별로 설치하여 인터넷에 연결하고, 국사 간의 통신은 VPN을 통해 이루어지게 구성할 수 있다. VPN 장비를 이용하게 되면, 별도의 전용선을 사용하므로 망 임대료를 절감할 수 있고, 인터넷을 사용하므로 낮은 비용 대비 높은 통신 속도를 장점으로 누릴 수 있다. 그림의 빨간색 파이프는 실제로 터널을 만드는 것이 아니라 VPN 장비 간에 트래픽을 주고받을 때 트래픽이 암호화되어 전송되는 것을 논리적으로 표현한 것이다.

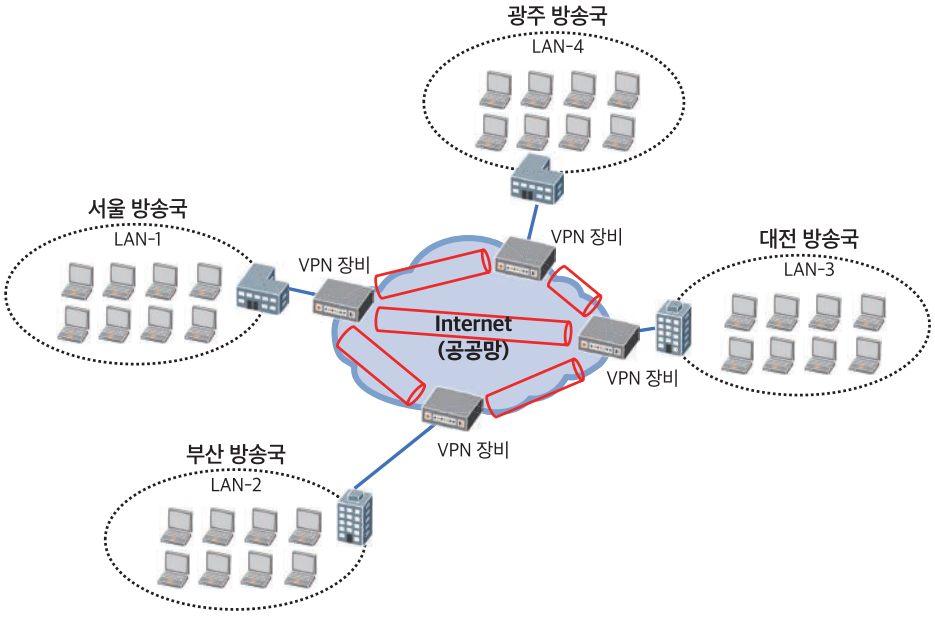

그림 2. 인터넷(공공망)을 이용한 VPN 통신 방식

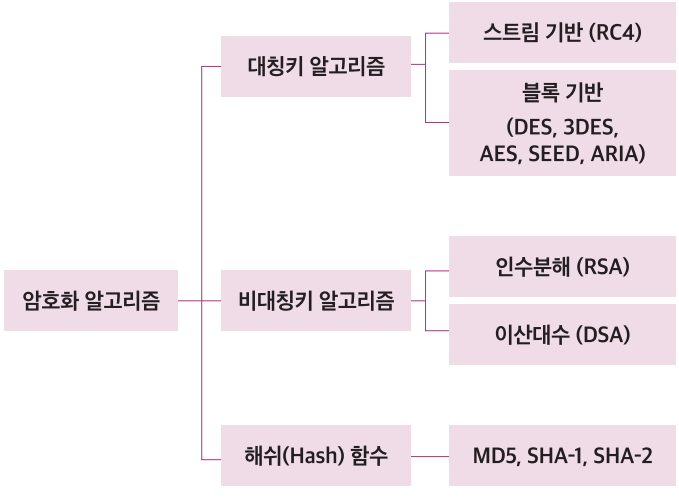

그림 3. 암호화 알고리즘의 종류

VPN 장비 간에 어떻게 트래픽이 암호화되고 복호화(암호를 푸는 것)되는지 알아보기 전에 암호 알고리즘에 대한 간략하게 설명이 필요할 것 같다. 문서를 암호화하기 위해서는 key가 필요하다. 열쇠를 잠그기 위해 키가 필요하고, 열쇠를 풀기 위해서도 동일한 키가 필요하듯이 문서를 암호화하기 위해서는 어떤 방식으로 암호화할지 결정하는 암호화 알고리즘 종류와 암호화에 사용할 키값이 필요하다. [그림 3]과 같이 현재 많이 사용하고 있는 암호화 알고리즘을 표시하였다. 크게 데이터를 암호화하기 위한 대칭키, 비대칭키 알고리즘과 데이터가 전송되는 중에 조작되었는지 여부를 확인할 때 사용하는 해쉬함수가 있다.

먼저 대칭키 알고리즘에 대해 알아보자. 데이터를 암호화할 때 무작위값으로 생성된 특정한 길이의 문자열을 키로 사용하여 원하는 파일을 암호화할 때 사용하고, 동일한 키로 복호화할 수 있는 방식이 대칭키 방식이다. 그에 비해 암호화할 때 사용하는 키와 복호화할 때 사용하는 키가 다르면 비대칭키 방식이라고 한다. [그림 4]와 같이 평문을 암호화할 때 사용했던 키로 복호화할 때도 사용할 수 있는 방식이 대칭키 방식이다. 데이터를 암/복호화하는 속도 측면에서 대칭키가 비대칭키 방식에 비해 월등히 빨라 데이터를 암호화해서 전송할 때 이 방식이 주로 사용된다. 우리가 사용하는 VPN뿐만 아니라 인터넷뱅킹, 전자메일, HTTPS 등 대부분의 데이터 암호화에는 대칭키 방식을 사용한다. 이 방식은 암/복호화에 양쪽이 동일한 키를 사용하기 위해 통신이 필요한 양자 간 온라인으로 키를 전송해야 하는데, 이때 중간에서 누군가 키를 가로채는 문제를 예방하기 위해 키 관리가 매우 중요하다. 그래서 이런 대칭키를 안전하게 전송하기 위해 사용되는 기술이 바로 비대칭키 방식이다.

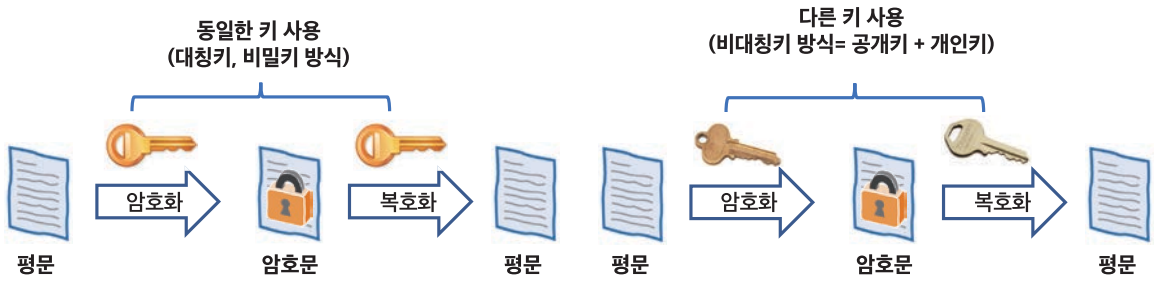

그림 4. 암호화를 위한 대칭키, 비대칭키 비교

비대칭키 방식은 2개의 키가 쌍으로 동작한다. 예를 들면 공개키를 이용하여 암호화하면 그것과 쌍을 이루는 개인키로만 풀 수 있으며, 반대로 개인키로 암호화하면 쌍으로 이루어진 공개키로만 암호를 풀 수 있다. 2개의 키는 보통 공개키와 개인키로 불린다. 말 그대도 공개키는 아무나 사용할 수 있는 키이고, 개인키는 개인만 사용할 수 있게 개인이 보관하는 키로, 외부로 노출되지 않게 관리되어야 하는 키이다. 이 비대칭키 방식은 크게 2가지 목적으로 사용된다.

[그림 5]와 같이 A의 개인키로 암호화해서 B에게 보내면 B는 A의 공개키를 이용해서 복호화할 수 있다. 공개키는 말 그대도 B뿐만 아니라 누구라도 구할 수 있는 키이기 때문에 A의 공개키를 통해서 누구나 복호화가 가능하다. 이렇게 복호화가 된다는 것은 A만이 자신의 개인키로 암호화했다는 말이기 때문에 A가 작성한 문서라는 것이 증명된다. 일반 문서 대신에 인증서를 보내게 되면, A의 신분을 증명할 수 있는 인증수단으로 사용할 수 있는 것이다. 그래서 이 방식을 다른 말로 전자서명이라고 하며 온라인상에서 본인임을 증명하는 목적으로 사용되고 있다.

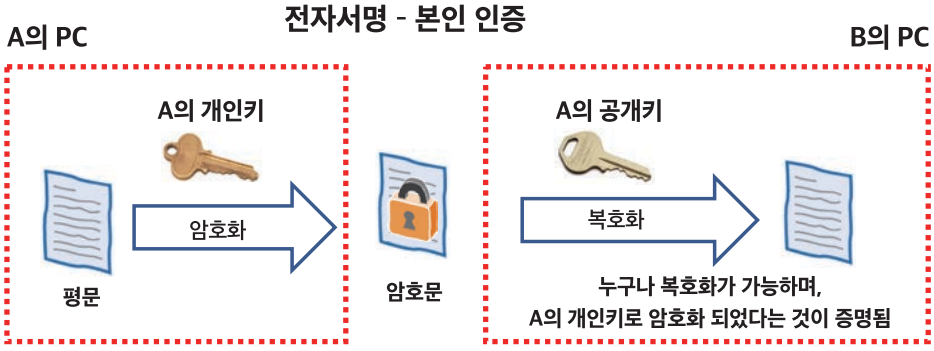

그림 5. 비대칭키를 이용한 전자서명(본인인증)

2번째 목적은 [그림 6]과 같이 B라는 사용자가 A에게 문서를 보낼 때 A의 공개키로 암호화해서 보내는 것이다. 이때 A는 자신만이 가지고 있는 개인키를 통해 복호화하여 문서 확인이 가능하다. A에게 문서를 보내고 싶은 누구나 A의 공개키를 통해 암호화해서 A에게 보낼 수 있고, 이렇게 암호화된 문서는 A 이외에는 아무도 그 문서를 복호화할 수 없다. A의 개인키는 A만이 가지고 있기 때문이다. 그래서 이런 방식을 전자봉투라고 해서 특정인에게 내용을 안전하게 보내고 싶을 때 주로 사용하는 방식이다. 앞에서 설명한 대칭키를 온라인으로 안전하게 보낼 때 바로 이 방식을 사용한다. 이 방식이 사용되는 이유는 만약에 누군가가 중간에서 암호화된 대칭키를 가로챘다고 하더라도 A의 개인키가 없어서 대칭키를 복호화할 수 없는 특징이 있기 때문이다.

그림 6. 비대칭키를 이용한 전자봉투(데이터암호화)

마지막으로 해쉬함수에 대해 알아보자. 앞에서 설명한 대칭, 비대칭키 방식은 암호화도 할 수 있고, 복호화도 할 수 있는 양방향 암호방식이라면, 해쉬방식은 암호화는 할 수 있지만 복호화가 되지 않는 단방향 암호방식이다. [그림 7]과 같이 'Hello!'라는 단어를 해쉬함수의 하나인 SHA256를 이용하여 암호화하게 되면 334~로 시작하는 특정하게 고정된 길이의 문자열이 생성된다. 이 문자열은 내용이 동일한 파일이면 언제든지 동일한 값이 생성된다. 그런데 여기에서 느낌표를 제거하고 'Hello'라고 변경한 이후에 SHA256으로 암호화하게 되면 185~로 시작하는 완전히 다른 문자열이 생성된다. 즉 문서에서 한 글자라도 변경되면 결과값이 완전히 바뀌기 때문에 문서의 내용이 조작, 변경된 경우나 프로그램의 원본 파일에 악성코드나 백도어 등이 숨겨져 있는지 검증이 가능하다.

이런 기능을 이용하여 데이터를 보낼 때 미리 보내는 파일을 해쉬함수로 돌려서 결과값을 같이 동봉하여 보내면, 받는 쪽에서 같은 해쉬함수를 이용하여 결과값을 생성하여, 동봉한 결과값과 같으면 원본 파일에 문제가 없는 것이고, 같은 값이 아니면 데이터가 전송 중에 조작, 변경되었다는 것을 확인할 수 있다. 해쉬함수로 생성한 결과값을 이용하여 역으로 단어를 복원할 수 없다. 대상파일의 크기에 관계없이 동일한 크기로 결과값이 생성되기 때문에, 한쪽 방향으로만 암호화할 수 있지, 반대 방향으로 복호화가 불가능해서 단방향 암호방식이라고 불린다.

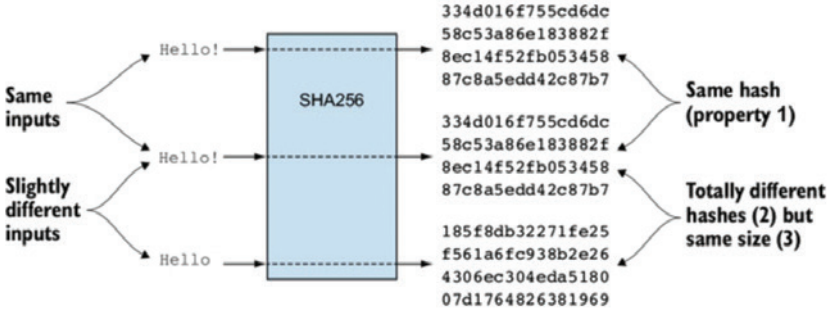

그림 7. 해쉬(Hash) 알고리즘의 동작 원리

앞에서 설명한 대칭키, 비대칭키, 해쉬함수를 이용하여 VPN이 어떻게 작동하는지 알아보자. [그림 8]과 같이 서울방송국과 부산방송국의 VPN 장비 간 트래픽을 전송하기 전에 터널을 생성하여야 한다. 크게 두 단계를 거쳐서 전송 준비단계가 완료된다. 1단계(Phase 1)에서는 비대칭키 방식과 디피-헬먼 키교환(Diffie-Hellman key exchange) 방식을 이용하여 양쪽 장비에 안전하게 대칭키를 생성시킨다. 2단계(Phase 2)에서는 1단계에서 생성한 대칭키를 이용하여 최종적으로 트래픽을 암복호화할 때 사용할 대칭키(IPSec Key)를 한 번 더 생성하여 데이터를 안전하게 전송할 준비를 마치게 된다.

VPN 장비 간에 터널을 생성한다는 말은 결국 암복호화에 사용할 대칭키를 양쪽 장비 간에 안전하게 공유하고 수신한 데이터를 검증하기 위해 어떤 해쉬함수를 사용할지, 대칭키가 유효한 기간을 어떤 단위로 결정할지 등을 합의한다는 것을 의미하며, 터널 생성에 대략 3~5초 정도가 소요된다. 이렇게 생성한 대칭키를 계속 사용하게 되면 보안성이 떨어지기 때문에 트래픽양이나 사용한 시간에 따라 갱신하게 되어 있다. 예를 들면, 양쪽 장비에서 주고받은 데이터 양이 10GB 단위로 혹은 사용한 시간이 1시간 단위로 새로운 대칭키를 생성하여 사용하기 때문에 키값이 유출되더라도 안전한 통신을 유지할 수 있는 장점이 있다.

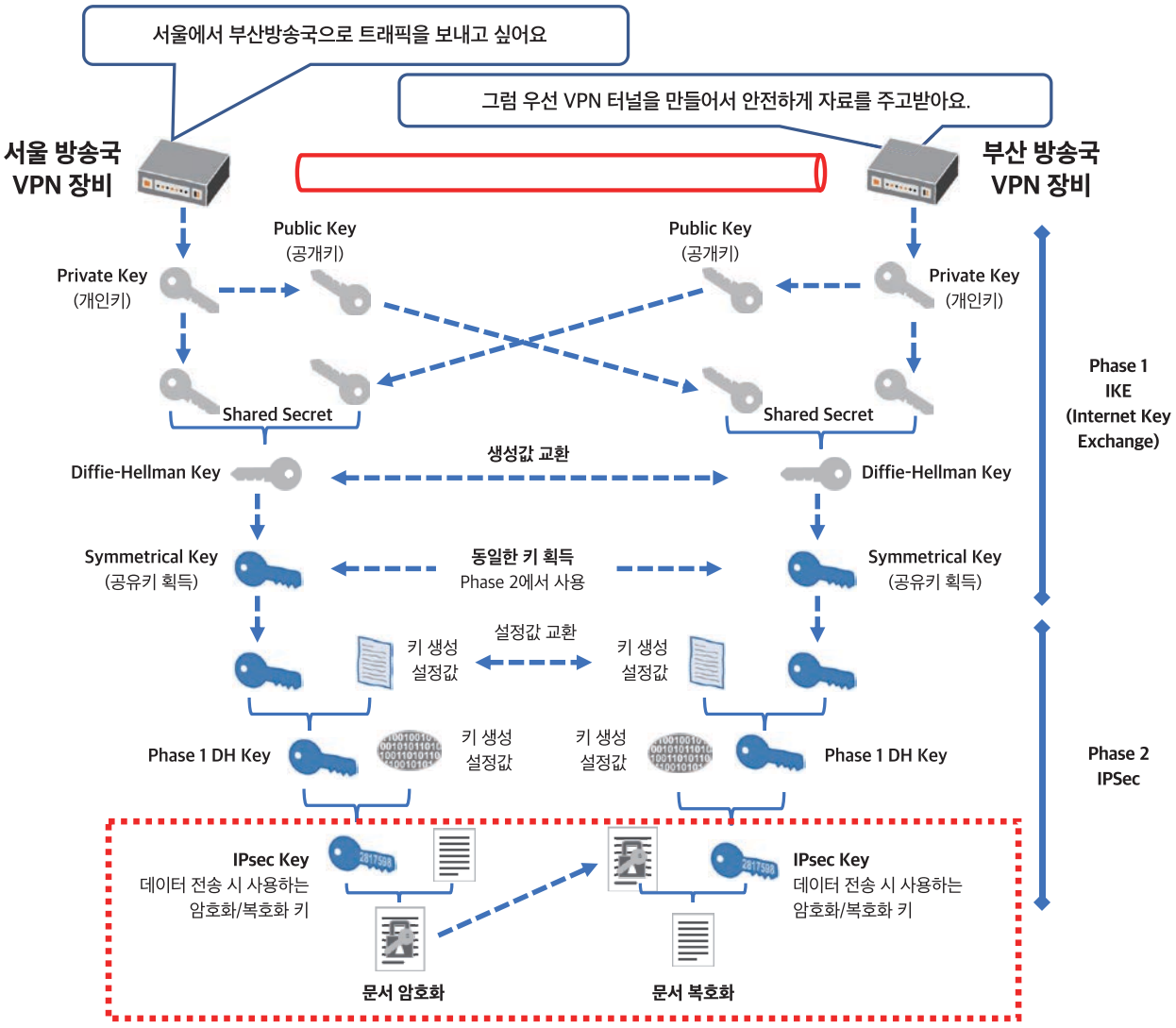

그림 8. IPSec VPN의 터널 생성 프로세스 순서 / 참조 : 체크포인트

최초로 출시된 VPN 장비는 VPN 기능만 작동하는 장비였다. 그런데 VPN의 위치가 외부 네트워크와 연결되는 게이트웨이 위치에 설치되다 보니, 방화벽 장비와 같은 위치에 설치되는 경우가 많았다. 이러다 보니, 방화벽과 VPN 장비를 통합해서 나오는 추세가 많아져서, 현재 공급되는 방화벽은 기본적으로 VPN 기능이 같이 포함된 제품이 대부분이다. VPN의 기능이 대칭키를 이용하여 트래픽을 암복호화하는 것이기 때문에, 장비의 CPU 성능에 따라 트래픽 처리 성능이 다양한 여러 가지 모델로 공급되고 있다. 통상 서울에 있는 전산센터를 중심으로 해서 여러 곳의 지방방송국과 VPN을 연결하기 때문에 서울전산센터에 있는 VPN 장비는 처리 성능이 높은 모델을 배치하고, 지방방송국은 규모에 따라 중소형장비를 설치하게 된다.

최근 코로나 19 사태로 재택근무를 하는 사례가 늘어나고 있다. 재택근무를 하게 되면 자택에서 회사 내의 전산 자원에 접속해서 다양한 업무 데이터나 문서를 주고받아야 하기에 보안적인 대비책이 준비되어 있어야 한다. 재택근무를 하기 위해서는 기본적인 준비가 필요하지만 최우선으로 필요한 사항이 자택에서 회사 서버와 안전하게 업무를 볼 수 있는 통로를 마련하는 것이다. 데이터를 안전하게 관리하기 위해서는 사내 네트워크에 접근할 때 허가된 회사 임직원이라는 것을 증명하는 것과 접속 후 자택의 단말과 사내 서버 간 데이터가 안전하게 전송되는 것이 필요하다. 이러한 요구사항에 대응할 수 있는 장비가 바로 SSL VPN 장비이다. 앞에서 설명한 VPN은 IPSec 기반의 장비로 주로 지역방송국과 같이 고정된 사용자를 위해서 사용된다. IPSec VPN 장비가 설치된 사무실이라면, 사용자가 별도의 접속을 할 필요 없이 접속을 원하는 전산실의 서버 IP 주소로 접근할 수 있다. VPN 장비 간에 자동으로 터널을 생성하고 있다가 접속을 원하는 IP 주소가 터널을 이용해야 하는 것으로 확인되면 자동으로 터널을 통해 전산실 서버와 데이터를 주고받을 수 있게 동작한다.

그에 비해 SSL VPN 장비는 지역방송국과 같이 특정한 위치에 고정된 사용자가 아니라 출장이나 현장기자 혹은 재택근무자와 같이 위치가 유동적인 사용자의 VPN 연결을 지원하는데 사용한다. 우선 사용자는 단말의 인터넷접속이 가능한 상태에서 웹브라우저를 통해 자사의 SSL VPN 장비에 접속 후, 아이디, 패스워드를 입력하여 접속이 허가된 사용자임을 인증받고 단말과 SSL VPN 장비 간에 암호화 방식과 대칭키, 사용할 해쉬함수 등을 합의하여 터널을 생성하게 된다. 즉 IPSec 방식은 장비와 장비 간에 터널이 생성되는 것이고, SSL 방식은 단말과 장비 간에 터널이 생성된다고 할 수 있다.

그림 9. HTTP + SSL = HTTPS

SSL 방식은 VPN 장비와의 연결뿐만 아니라 웹 서버와 암호화 통신이 필요할 때도 이용되고 있다. 최근 대부분의 웹서비스는 HTTP에서 HTTPS 방식으로 많이 넘어가고 있다. 바로 여기에 SSL 방식이 사용되고 있다. [그림 9]와 같이 기존의 HTTP 방식에서 암호화 통신을 위해 SSL 기반의 암호화 기술을 이용하면 HTTPS 방식으로 변경되는 것이다.

SSL 방식에서 터널을 만드는 절차도 기존 IPSec 방식과 대체로 비슷하다. [그림 10]과 같이 클라이언트가 서버의 인증서를 받아서 검증기관을 통해 믿을 수 있는 서버인지 확인하고, 앞으로 사용할 암호화 종류를 협상해서 결정한다. 그런 다음 서버의 인증서에 있는 공개키를 통해 클라이언트가 생성한 대칭키를 암호화해서 보내면, 서버는 자신의 개인키를 통해 복호화해서 클라이언트와 동일한 대칭키를 안전하게 획득하여 안전한 통로를 생성하게 된다. 이후에 데이터 전송은 이렇게 획득한 대칭키를 이용하여 암호화하고 복호화하며 인터넷상에서 안전하게 데이터를 주고받을 수 있게 된다.

현재 인터넷상의 대부분의 상거래나 안전이 필요한 통신에는 이런 SSL 기반의 암호화 통신이 주로 이용되고 있는데, 일상생활에서 많이 사용하는 인터넷뱅킹도 이 기술이 적용되어 있다. 실생활에서는 주민등록증, 운전면허증, 여권 등으로 자신의 신분을 증명할 수 있듯이, 인터넷상에서 자신의 신분을 증명하기 위해 사용하는 수단이 공인인증서이다. [그림 11]과 같이 우리가 발급받는 공인인증서에는 발급기관 정보와 개인의 공개키 정보 등이 포함되어 있다. 개인 PC에 공인인증서와 암호화된 개인키를 같이 보관하고 있다가, 인터넷뱅킹을 할 때, 자신의 인증서를 인터넷뱅킹 서버에 제출하면, 받은 인증서가 정상적인지 인증서검증기관을 통해 검증을 받게 된다. 인증서가 정상적이라고 판단되면, 인증서에 있는 고객이름(법인이면 법인명)과 고유번호를 이용하여 신원을 파악하고 해당 고객의 계좌정보를 검색하여 서비스가 가능하게 된다. 여기까지가 고객에 대한 신원을 확인하는 절차이고, 다음은 안전한 통신을 위한 대칭키 획득 절차이다.

인증서에 문제가 없다면 서버는 인증서에서 A의 공개키를 추출하여 서버가 자체적으로 생성한 대칭키를 암호화해 A에게 전달한다. A 사용자는 가지고 있는 암호화된 개인키를 풀기 위해서 패스워드를 입력하게 되는데, 이 패스워드는 우리가 공인인증서를 발급받을 때 입력했던 패스워드가

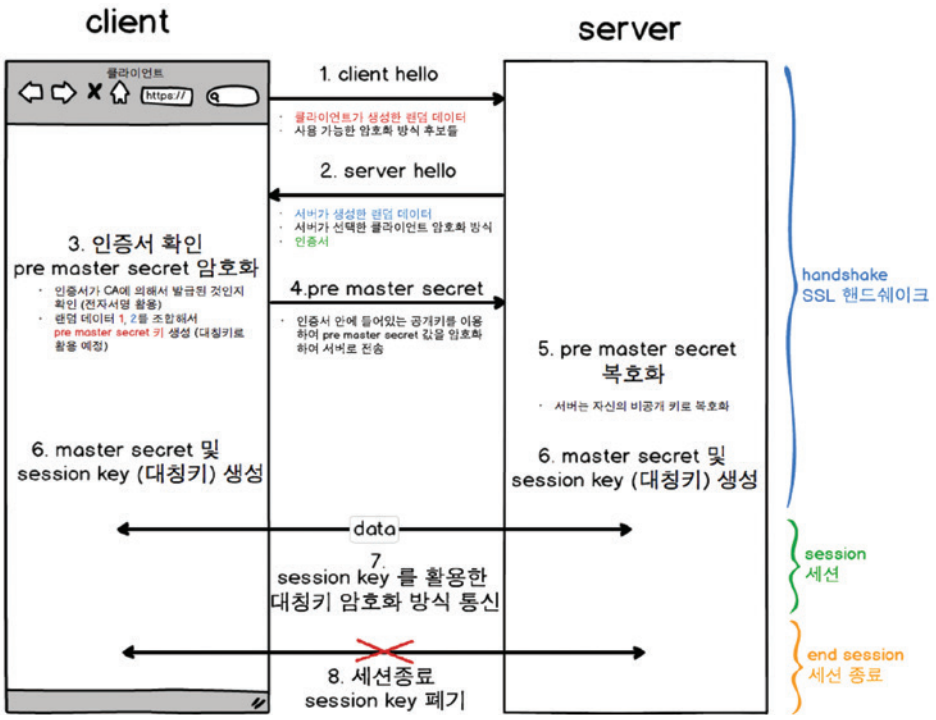

그림 10. SSL 터널 생성 프로세스 / 자료출처 : 초보 몽키의 개발공부로그

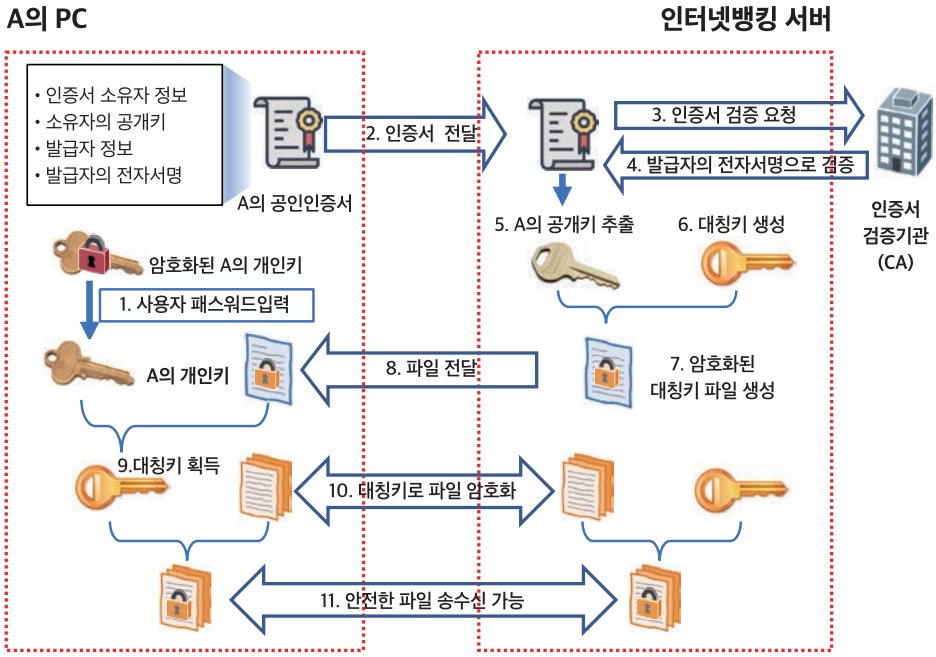

그림 11. 인터넷뱅킹 시 고객 인증과 암호화 통신 절차

이용된다. A는 자신의 개인키를 이용하여 자신의 공개키로 암호화된 대칭키를 복호화해 안전하게 대칭키를 획득하게 된다. 이렇게 획득된 대칭키를 이용하여 데이터를 암호화해 보내고, 받는 쪽에서는 복호화해 안전하게 통신이 이루어지게 된다.

인터넷뱅킹 로그인 완료 후 금액을 이체하거나 개인정보를 변경할 때 추가로 해야 하는 인증 절차가 있다. 초기에는 보안 카드라고 해서 30~40개의 숫자가 적혀있는 카드에서 특정 숫자의 번호를 입력하게 해서 보안성을 강화하는 수단으로 사용하였다. 이런 보안카드를 휴대폰으로 찍거나, 내용을 컴퓨터 내에 저장하면서 통째로 유출되는 사고가 빈번하게 발생해, 최근에는 보안을 더 강화하기 위해 OTP(One Time Password, 일회용 비밀번호)를 많이 이용하고 있다. 말 그대로 한 번만 사용 가능한 패스워드이기 때문에 중간에 해커가 가로챈다고 하더라도 문제가 없는 암호체계이다.

[그림 12]는 OTP의 동작 원리에 대해 설명하였다. 왼쪽의 접속자가 휴대하고 있는 OTP 생성기에는 시계가 내장되어 있다. 그래서 전원을 켜게 되면, 현재 시각을 입력값으로 해서 생성기마다 고유의 번호 생성함수가 작동하여 6자리의 번호를 생성하여 표시한다. 인터넷뱅킹의 인증서버에서도 표준시간을 이용하여 접속자마다 고유 생성함수를 준비하고 있다가 해당 접속자 생성기와 동일한 번호 생성함수를 작동시켜 동일한 6자리 숫자를 생성한다. 여기서 사용하는 기반 기술로 앞에서 설명한 해쉬함수가 사용된다. 동일한 값을 넣으면 언제나 동일한 결과값이 출력되는 원리를 이용하는 것이다. 여기서 동일한 값은 시간값을 활용하고 동일한 결과값이 6자리 숫자로 출력되는 원리를 이용하여, 서로의 6자리 숫자값이 동일하면 인증된 사용자로 판단하여 금액을 이체하거나, 고객정보수정을 승인하게 된다.
이때 보통 생성된 숫자의 유효기간은 1분이고, 혹시 OTP 생성기의 내장 시계가 느리거나 빠르게 가더라도, 인증 서버의 참조 시계도 접속자별로 시간을 보정하는 기능도 내장하고 있어서 OTP 생성기가 오래되어 내장된 시계가 정확하지 않더라도 문제없이 동작하는 기능을 포함하고 있다. 시간을 보정하는 원리는 인증서버에서 1분 과거시간, 현재시간, 1분 미래시간별로 각각 3개의 값을 생성하여, 접속 사용자가 어떤 값으로 응답하는지 확인해서 3개의 값 중에 응답값과 동일한 시간대 값을 확인하면 접속자의 OTP 시간에 맞추어 접속자의 시간값을 보정하는 방식으로 동작한다.

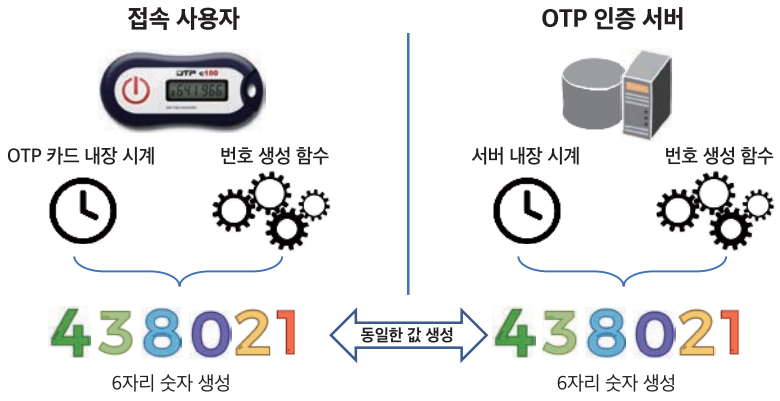

그림 12. OTP(One Time Password)의 동작 원리

지금까지 VPN을 설명하기 위해 온라인상에서 신원 확인 방법과 안전한 통신을 위한 암·복호화 방법에 대해 설명해 드렸다. 최근에 공인인증서 폐지와 관련된 뉴스를 접하게 된다. 필자가 보기에는 공인인증서를 폐지하려는 이유가 인증서 기술 자체의 문제보다도 이를 사용하기 위한 여러 복잡한 절차들, 예를 들면 1년 단위 갱신의 번거로움, 많은 보안 프로그램 강제 설치 등 기술 외적인 문제가 더 큰 원인이었지 않나 생각된다. 사용이 편리하고 안전한 지문, 홍채 등의 생체정보, 블록체인 등을 활용한 안전하고 신속한 인증 기술이 널리 사용되기를 기대한다.

다음 호에서는 DDoS(서비스 거부) 공격의 방식과 유형, DDoS 방어 장비에 대해 알아보도록 하겠다.