이지헬프 원격지원 서비스

Security White Paper

Feb 2017

목차

이 문서는 이지헬프의 원격지원 제품에 대한 보안 관련 문서입니다. 컴퓨터를 원격으로 조작하는 것은 보안성이 매우 중요합니다. 이에 당사의 제품에 대한 보안 설계와 구성에 대해 설명하고 어떻게 보안성을 완벽하게 구현하는지에 대해 고객에게 투명하게 공개합니다.

대상

이 문서는 기술 문서로써 관련 네트워크 관리자 분들을 위해 작성되었습니다. 이 문서에 설명되어 있는 정보는 매우 기술적이고 상세합니다. 이 문서는 이지헬프 서비스를 도입하기 전에 필요한 보안 우려를 확인하는데 참고할 수 있습니다.

1. 보안에 대한 관점

사물 인터넷 기술이 발달함에 따라 원격으로 제품의 기술을 지원하거나, 문제점을 분석하는 원격 지원의 시장이 계속 진화하고 있습니다. 많은 기업들은 원격 지원을 도입하는 것을 생각하고 있으며 그에 따른 보안에 대해 관심이 높아지고 있습니다. 최근 온라인 상태의 제품과 온라인 서비스 등이 증가하고 있기 때문에 보안과 인터넷은 더욱 밀접한 관계에 있을 수 밖에 없습니다. 하지만 대부분의 사용자들은 온라인 서비스나 제품의 보안에 둔감합니다.

항상 문제시 되고 있는 온라인 보안 사고를 보면 간단한 비밀번호 설정이나 적절한 보안 패치 등을 하지 않아 발생되는 문제 또는 알 수 없는 파일을 아무렇지 않게 다운로드하여 설치해서 발생되는 문제 등이 있습니다. 이렇듯 사용자들은 온라인에서 보안에 대해 상당히 취약하기 때문에 불법 사이버 공격은 줄어들고 있지 않습니다.

사이버 공격은 기술적 진화로 점점 빠르고 쉽게 변화하고 있으며, 사이버 공격의 자동화가 이루어지면서 인터넷 보안은 언제, 어디서나 위협받고 있습니다. 전문적인 네트워크 기술자도 실수로 잘못된 파일을 다운로드하거나 보안 패치를 무심코 지나쳤다면 그로 인해 기업 전체의 네트워크가 사이버 공격에 노출될 수도 있습니다.

이지헬프는 기업이 인터넷에 연결되어 있는 고객의 컴퓨터에 원격으로 접속하여 지원을 하는 원격 지원 서비스입니다. 고객들은 사회적으로 공인된 기업이라도 상담원이 컴퓨터를 자유자재로 할 수 있기 때문에 보안에 더 걱정하는 것은 사실입니다. 그러나 원격 지원을 통해 고객 스스로 해결할 수 없는 문제를 상담원이 해결해주기를 원합니다. 또한 원격 지원 서비스의 보안은 정해진 보안 플로우에 따라 시행되기 때문에 안전하다고 할 수 있습니다.

그러므로 원격지원을 할 때는 이지헬프와 같이 보안적으로 신뢰할 수 있는 원격 소프트웨어를 사용해야합니다. 이지헬프 원격 지원 서비스는 항상 네트워크를 감시하여 외부의 위협으로 안전하게 보호하고 있으며, 취약한 보안 문제에 대해 아무 걱정없이 고객 지원을 할 수 있습니다.

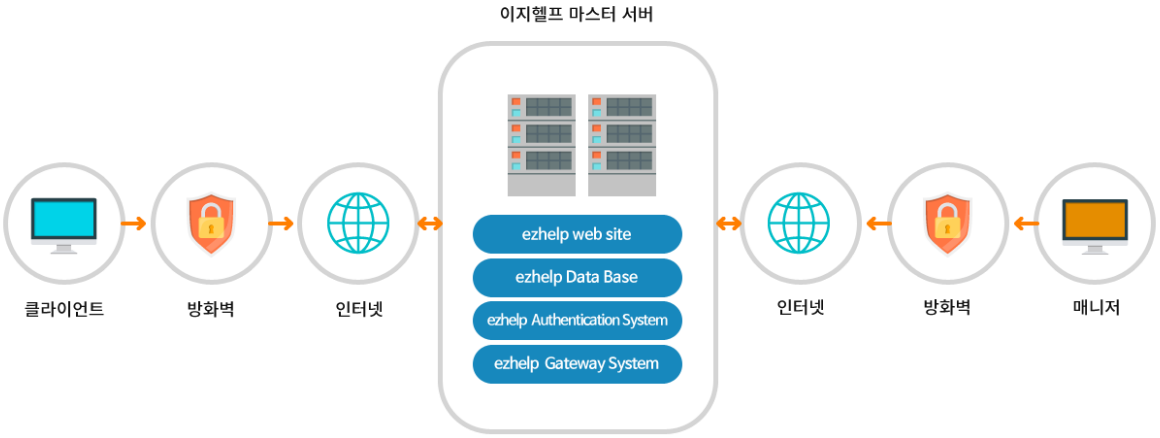
이지헬프는 원격 지원에 있어 안전한 보안성과 쉽고 빠른 편리성, 안정적으로 동작하는 우수성을 갖추고 있으며, 또한 원격지원 서비스의 품질을 높이기 위한 기술과 인프라를 갖추고 있습니다. 서비스의 모든 단계에서 보안성을 고려하여 설계되어 있으며, 기술적, 물리적 보안 대책을 철저하게 하고 있습니다.

이지헬프의 도입으로 업무의 효율성과 생산성을 향상시킬 수 있으며, 고객 지원으로 인한 비용 절감도 할 수 있습니다.

2. 이지헬프의 이해

1) 아키텍처

이지헬프가 설계한 보안 메커니즘을 설명하기 전에, 이지헬프 서비스의 아키텍처를 먼저 설명합니다.



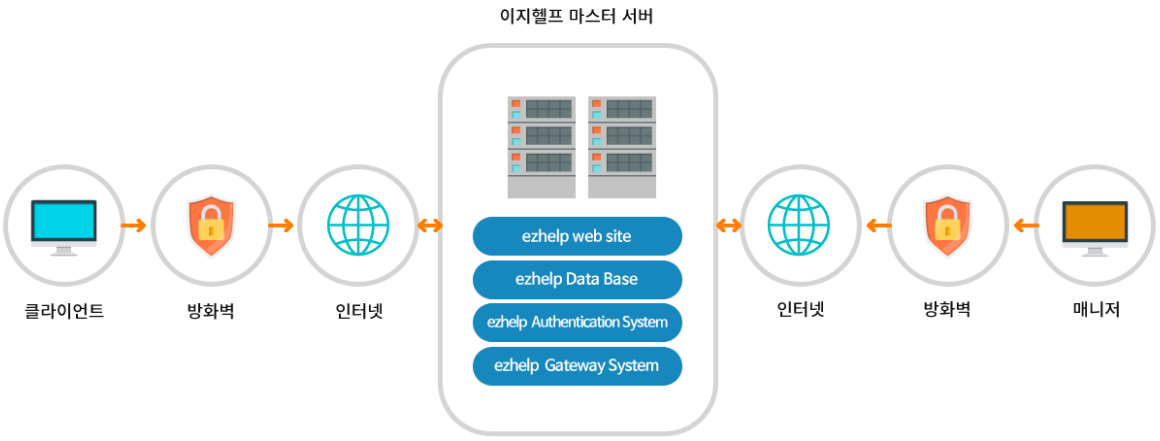
<그림 1. 이지헬프 아키텍처>

이지헬프 아키텍처는 원격 접속의 세션에 관련된 엔티티(ENTITY)가 3개 있습니다. 클라이언트 또는 클라이언트PC는 원격지원 받는 사람 또는 컴퓨터 입니다. 이지헬프 매니저는 접속하는 컴퓨터 또는 해당 컴퓨터의 이지헬프 호스트 소프트웨어 입니다. 이지헬프 마스터서버는 클라이언트PC 와 이지헬프 매니저 사이의 인증 및 트래픽을 중개하는 이지헬프 서비스 입니다.

2) 설계 원리

이지헬프는 중요한 리소스에 대해 원격접속을 신뢰할 수 없는 네트워크를 경유해도 안전하게 실행할 수 있게 설계되어 있습니다. 개발 중 유저 편의성보다 보안성에 더욱 중점적으로 고려하였습니다.

3) 서비스 흐름



<그림 1.1. 이지헬프 아키텍처>

① 이지헬프 매니저는 이지헬프 인증 시스템에 사용자 인증을 통해 로그인 하며, 접속코드 6 자리를 부여 받습니다.

② 접속코드 6 자리를 클라이언트 PC 에게 전달하여 해당 접속코드를 통해 이지헬프 매니저와 원격접속 연결을 진행합니다.

③ 클라이언트 PC 는 이지헬프 인증 시스템을 통해 이지헬프 매니저와의 접속유형을 판별하게 됩니다.

④ 직접 연결이 가능한 경우에는 클라이언트 PC 와 이지헬프 매니저 상호간에 직접 연결을 수립하여 원격접속이 이루어지게 됩니다.

⑤ 만약, 직접 연결이 어려운 환경의 경우에는 이지헬프 게이트웨이 시스템을 중개자로 하여 원격접속이 이루어지게 됩니다.

3. 기술적 보안

1) 원격접속 및 연결 유형

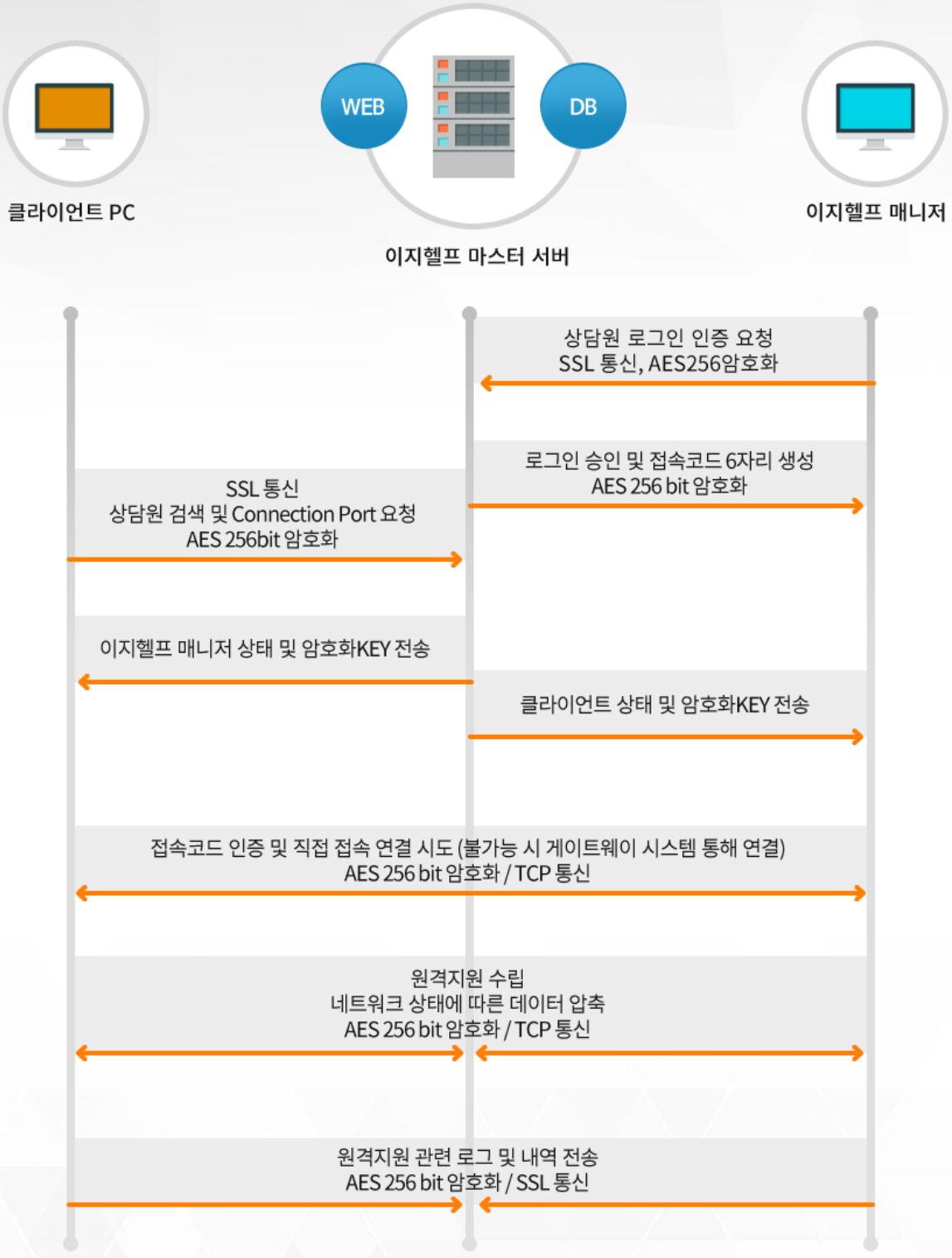
이지헬프의 원격접속 인증에 사용되는 접속코드는 랜덤 6자리 숫자로 제공되고, 생성된 접속코드는 이지헬프 매니저와의 원격접속을 위해 사용되며 제 3자의 임의 접근은 원천적으로 허용하지 않습니다. 또한, 이지헬프 매니저를 다시 시작하면 새로운 접속코드가 생성되기 때문에 접속코드를 안내 받은 클라이언트PC만 연결할 수 있습니다.

원격접속을 진행할 경우 이지헬프가 최적으로 연결 유형을 결정합니다. 모든 경우의 60~70%는 이지헬프 인증 시스템을 거친 뒤 TCP를 통해 바로 연결이 수립됩니다. 또한, 바로 연결이 어려운 경우에는 TCP 통신을 통해 이지헬프 게이트웨이 시스템을 거쳐 연결하게 됩니다.

2) 데이터 암호화

원격접속 정보를 암호화 처리없이 평문으로 전송하면 중간자 공격 (MITM: Man in the Middle)에 대한 위험에 고스란히 노출될 수 있습니다. 안전한 데이터 전송을 위해서는 클라이언트 PC에서 1차 암호화를 통하여 전송될 데이터에 대한 보안 처리를 거쳐야 합니다. 이지헬프는 모든 원격 접속에서 전달되는 데이터를 End-to-End 에서 256bit AES 세션 암호화를 통하여 전달하게 됩니다.

이지헬프 데이터 트래픽은 256bit AES 세션 암호화를 이용해 보호됩니다 이 기술은 https/SSL와 동일한 형식으로 이용되고 현재 기준으로 가장 안전한 방법입니다. 또한, 매번 생성되는 암호화키를 통해 완벽하게 보호되기 때문에, 악의적인 공격자의 스니핑(Sniffing)공격에도 해독이 불가능한 상태로 안전하게 데이터를 전송하여 보호됩니다.



<그림 2. 이지헬프 데이터 암호화 흐름도>

3) 네트워크 보안

이지헬프는 네트워크 사용자의 데이터를 보호하기 위해 강력한 산업 표준 기술을 사용합니다. SSL (Secure Socket Layer) 데이터 암호화는 이지헬프 시스템과 이지헬프 매니저 및 클라이언트 PC 사이의 보안 연결을 만듭니다. 원격접속 연결 시 강력한 2048-bit SSL 암호화 통신을 제공하여 클라이언트 PC와 이지헬프 시스템 사이에 전송되는 모든 데이터에 대해서는 암호화 통신을 제공함으로써, 악의적인 공격자의 스니핑(Sniffing)공격에도 해독이 불가능한 상태로 안전하게 데이터를 전송합니다.

이지헬프는 원격 서비스 사이트 접속 시 HTTPS 통신을 통한 안전한 웹 접근을 제공하며, 원격지원 웹 서버는 외부에서 액세스할 수 있는 페이지에 중요 데이터를 저장하지 않습니다. 이지헬프 시스템에 최신 보안 패치를 적용하며, 메시지/요청/응답 등의 세션에서 잘못된 재전송 공격을 방지하기 위한 방침을 수립하여 적용하고 있습니다.

4) 디지털 서명된 응용프로그램

이지헬프에서 배포하는 모든 소프트웨어는 가장 강력하고 안전한 디지털 서명(VeriSign Secured)이 되어 Private 키가 없이는 어떠한 개인도 변경하거나 업데이트할 수 없습니다. 나중에 소프트웨어가 변경되면 디지털 서명이 자동으로 유효하지 않게 되어 보안 위험으로 안전함을 보장합니다.

5) 데이터센터 보안

이지헬프는 각 국가의 데이터 센터를 기반으로 이지헬프 전용 네트워크 망을 구성하고 있어 이 망을 기반으로 서비스를 운영, 관리합니다. 또한, 시스템 구성을 이중화 하여, 천재지변으로 시스템 장애가 발생해도 다른 대체 시스템을 통해 안정적인 서비스 제공이 가능합니다.

또한, 개인 접근통제, CCTV 감시, 지문인식 출입통제 등 365일 24시간 모니터링 및 현장 보안요원을 통해 인증된 사람에게만 데이터센터 출입을 허용하고 있습니다.

4. 응용 프로그램 보안

6자리 접속코드 사용

이지헬프는 원격접속의 안전을 보장하기 위해 접속 시 접속코드를 사용할 수 있습니다. 이지헬프 매니저가 원격접속을 위해 6 자리 접속코드를 알려주면 클라이언트 PC 는 이지헬프 매니저로부터 전달받은 접속코드 이외의 코드로는 원격접속을 허용할 수 없습니다. 6 자리의 접속코드는 이지헬프 매니저의 고유 코드이며, 이지헬프 매니저가 새로 로그인할 때마다 접속코드는 변경됩니다.

은폐모드 불가

이지헬프는 원격접속 중 클라이언트에게 반드시 원격지원이라는 표시를 클라이언트 PC 에 표시하도록 되어 있습니다. 이는 현재 이지헬프 매니저가 정상적으로 원격접속 중을 알리는 것입니다. 그러므로 이지헬프 매니저가 클라이언트 PC 에 은밀하게 접속하여 감시하거나 부적절한 프로그램을 설치할 수 없게 되어 있습니다.

원격 권한 회수

이지헬프 원격지원은 이지헬프 매니저가 원격으로 클라이언트 PC 를 제어하고 있지만, 만약 이지헬프 매니저가 클라이언트 PC 의 민감한 정보를 사전 동의 없이 수정/삭제하거나 악의적인 프로그램을 설치하려고 할 때 클라이언트는 이지헬프 매니저로부터 원격제어 권한을 바로 회수하여 불필요한 원격접속을 차단할 수 있습니다.

지정된 IP 로그인

이지헬프 서비스를 이용하는 관리자 ID 는 상담원이 지정된 컴퓨터 이외에 다른 컴퓨터에서 고객 컴퓨터를 원격 지원하는 것을 불가능하게 합니다. 관리자는 상담원의 IP 를 리스트로 관리하여 추가/삭제를 할 수 있습니다.

접속로그

이지헬프는 상담원이 이지헬프 매니저에 로그인을 한 기록과 클라이언트 PC 에 원격접속을 수행한 기록을 모두 로그에 저장하기 때문에 상담원이 언제, 어떤 고객에게 원격접속을 했는지, 문제는 없었는지 등을 체크할 수 있습니다. 또한 원격접속의 로그는 그래프 통계로 제공합니다.

5. 총평

이지헬프 원격지원 서비스는 최고의 전문 네트워크 보안팀에 의해 설계되었으며, 최첨단 암호 기술과 인증 기술을 도입하였습니다. 이러한 보안 설계를 기반으로 최적의 원격지원 서비스를 하고 있으며, 네트워크 보안 시스템이 실시간으로 항상 데이터를 보호 감시하고 있습니다. 또한 이지헬프는 자체적인 보안 규약을 포함한 국제 보안 규약을 따르고 있으며, 이를 철저하게 준수하고 있습니다. 제품의 보안은 지속적인 투자와 지원, 그리고 글로벌 수준의 환경이 갖춰져야 완전한 보안이 가능합니다. 이지헬프는 고객의 안전을 위해 항상 만반의 준비를 하고 있습니다.

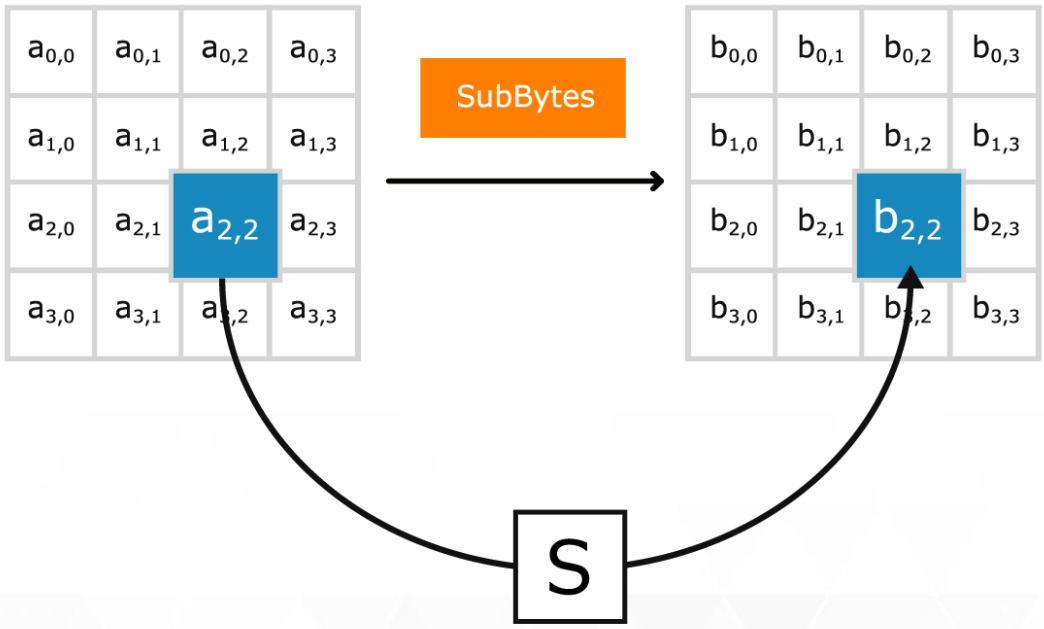
이지헬프 원격지원 서비스는 신뢰할 수 있습니다.

6. APPENDIX

용어 설명

AES (Advanced Encryption Standard)

고급 암호화 표준(AES)은 2001년 미국 표준 기술 연구소(NIST)에 의해 제정된 암호화 방식입니다. AES는 미국 정보가 채택한 이후 전 세계적으로 널리 사용되고 있습니다. 1977년 공표된 DES를 대체한 AES는, 암호화와 복호화 과정에서 동일한 키를 사용하는 대칭 키 알고리즘입니다. AES는 ISO/IEC 18033-3 표준에 포함되어 있으며 여러 암호화 패키지에서 사용되고 있습니다. AES는 또한 미 국가안보국에 의해 1급 비밀(TOP Secret)에 사용할 수 있도록 승인된 알고리즘 중 최초로 공개되어 있는 알고리즘입니다.



SSL (Secure Socket Layer)

SSL은 네트워크 내에서 메시지 전송의 안전을 관리하기 위해 넷스케이프에 의해 만들어진 프로그램 계층(Layer)입니다.

넷스케이프의 생각은 비밀이 보장 되어야하는 메시지를 맡은 프로그램은 웹 브라우저 또는 HTTP와 같은 응용프로그램과 인터넷의 TCP/IP 계층 사이에 들어가야 한다는 것입니다.

여기서 "소켓"이라는 용어는 데이터를 네트워크상의 클라이언트와 서버 프로그램 사이 또는 같은 컴퓨터의 프로그램 계층끼리 주고받는 소켓 방식을 줄여서 말한 것입니다.

SSL은 클라이언트와 서버 간의 정보를 암호화하여 만약 해킹을 통해 정보가 유출되도 정보 내용을 보호할 수 있습니다. SSL은 웹 제품 뿐 아니라 파일 전송 규약(FTP)등 다른 TCP/IP 애플리케이션에 적용할 수 있으며, 인증 암호화 기능과 데이터의 암호화 등으로 인터넷 상의 위협으로 보호할 수 있습니다.

SHA-2 기반의 SHA-256 해시 알고리즘

SHA는 안전한 해시 알고리즘(Secure Hash Algorithm)은 미국 국립 표준 기술 연구소인 NIST가 표준으로 채택한 것으로 서로 관련된 암호학적 해시 함수들의 모음입니다. 그중 SHA-2 기반의 SHA-256은 32비트 워드를 사용하는 해시 함수이며, SHA-1 또는 SHA-0 보다 공격에 더 안전하다고 알려져 있습니다.

MITM (man in the middle attack, 중간자공격)

중간자 공격은 네트워크 통신을 조작하여 통신 내용을 도청하거나 조작하는 공격 기법입니다. 중간자 공격은 통신을 연결하는 두 사람 사이에 중간자가 침입하여, 두 사람은 상대방에게 연결했다고 생각하지만 실제로는 두 사람은 중간자에게 연결되어 있으며 중간자가 한쪽에서 전달된 정보를 도청 및 조작한 후 다른 쪽으로 전달하는 방식입니다.