KR Maritime Cyber Security

News from KOREAN REGISTER

Jan 2019

Vol. 009

한국선급 활동

- 4차 산업 관련 기술 육성을 위한 조직개편 단행
- 싱가포르 선사 사이버보안 기술 세미나 실시

마이크로소프트 2019년 첫 패치 시행

선박 및 해양 사이버보안 이슈 및 대응방안

사이버 위협의 이해(OWASP Top 10)

데이터 보안 정책 수립 가이드

용어 설명

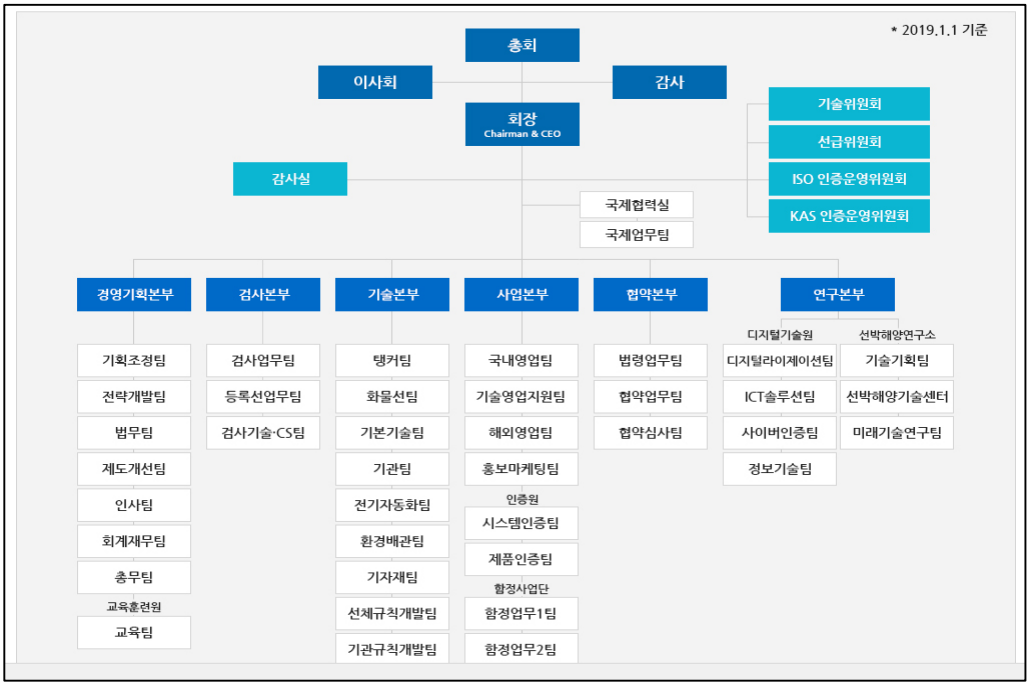
한국선급 활동

● 4차 산업 관련 기술 육성을 위한 조직개편 단행

한국선급(KR, 회장 이정기)은 디지털 선급 전환과 조직의 능동적인 대응 체계 확립을 위해 조직개편을 단행한다고 밝혔다. 이번 조직 개편의 핵심은 신속한 디지털 선급으로 전환을 위해 관련 조직을 통합하고 컨트롤타워를 두어 업무 효율성을 높이는데 있다. 구체적으로 디지털라이제이션팀, ICT솔루션팀, 사이버인증팀, 정보기술팀으로 구성된 전담조직인 '디지털기술원'을 신설하였다.

또한, 기획 및 경영시스템의 유기적인 운영을 위해 전략기획본부 및 경영본부를 '경영기획본부'로 통합하였으며, 다양하고 방대한 기술 분야의 체계적인 관리가 필요해 별도 연구본부를 신설하여 기술본부 산하 연구소를 연구본부 산하 '선박해양연구소'로 이동하고 디지털 기술원을 추가 편제하였다.

한국선급은 지난 2016년부터 사이버보안 대응 TFT를 구성하여 선박 사이버보안 핵심기술 연구를 수행해왔으며, 2018년 해상 사이버보안 시스템 인증 체계를 구축하여 사이버보안 기술 서비스 및 인증 서비스를 선사에 제공하고 있다. 신설된 사이버인증팀은 현재 선박·회사 사이버보안 인증, 기자재 사이버보안 형식승인 등의 업무를 담당하고 있으며, 선박 운영기술(OT) 시스템에 적용할 수 있는 침투테스트 진단 도구를 개발하고 있다. 자세한 사항은 홈페이지에서 확인 할 수 있다.



● 싱가포르 선사 사이버보안 기술 세미나 실시

2018년 12월, 사이버인증팀에서는 싱가포르의 주요 선사를 방문하여 사이버보안 최근 동향에 관한 기술 세미나를 실시하였다. IMO에서는 2021년 동 사항이 강제화될 예정이나, 해사업계에서는 2018년부터 OCMIF TMSA 및 SIRE, RIGHTSHIP등 탱커선 및 벌크선에 대한 화주검사에서 사이버보안 관리사항을 점검항목에 포함하고 있다.

현재 해운업계의 관심이 높은 상황에 열린 세미나였기에 선사로부터 많은 호응이 있었으며, 향후 기술 서비스 및 인증을 통해 가이드라인을 제공 할 것으로 예상된다.

한국선급 사이버인증팀은 작년 3월부터 선사 TMSA/SIRE 수검을 위한 사전점검, 개선 가이드라인, 임직원 교육, PC 보안 취약점 진단 프로그램 활용 등의 사이버보안 기술 서비스를 제공하여 선사 사이버보안 체계 구축을 성공적으로 지원한바가 있다.





마이크로소프트 2019년 첫 패치 시행

● 마이크로소프트, 2019년 1월 50개의 취약점 패치

마이크로소프트는 2019년 첫 보안패치 시행을 통해 9개 제품(Windows OS, Internet Explorer, Microsoft Edge, ChakraCore, .NET Framework, ASP.NET, Microsoft Visual Studio, Microsoft Exchange Server, Microsoft Office)에 대한 50개의 취약점을 패치하였다.

특히 이번 패치에서는 17 개의 버그가 공격자가 Microsoft 제품 또는 Windows 구성 요소 내에서 코드를 실행할 수 있는 "원격 코드 실행(RCE)“ 취약점으로 나타났다.

패치 전에 공개된 취약점은 CVE-2019-0579이며, 2번째로 높은 등급인 '중요(important)'를 받았다. 이 취약점은 윈도우 젯(Windows Jet) 데이터베이스 엔진에서 발견된 것이며, 성공적으로 익스플로잇 될 경우 원격에서 코드 실행을 가능하게 해준다. 공격 성립을 위해서는 특수하게 조작된 파일을 사용자가 열도록 해야 한다.

또 다른 치명적인 취약점은 CVE-2019-0547로 Windows DHCP 클라이언트 기계에서 공격자가 임의의 코드를 실행할 수 있게 해준다. 특수하게 조작된 DHCP 응답들을 필요로 한다. Windows DHCP 클라이언트는 모든 Windows 운영 체제에서 사용 가능하며 취약점은 원격으로 악용 될 수 있으므로 사용자는 이번 달의 업데이트를 놓치지 않아야한다.

CVE	Title	Severity	Public	Exploit	XI - Latest	XI - Older	Type
CVE-2019-0579	Jet Database Engine Remote Code Execution Vulnerability	Important	Yes	No	3	3	RCE
CVE-2019-0539	Chakra Scripting Engine Memory Corruption Vulnerability	Critical	No	No	1	N/A	RCE
CVE-2019-0568	Chakra Scripting Engine Memory Corruption Vulnerability	Critical	No	No	1	N/A	RCE
CVE-2019-0567	Chakra Scripting Engine Memory Corruption Vulnerability	Critical	No	No	1	N/A	RCE
CVE-2019-0565	Microsoft Edge Memory Corruption Vulnerability	Critical	No	No	1	N/A	RCE
CVE-2019-0547	Windows DHCP Client Remote Code Execution Vulnerability	Critical	No	No	1	N/A	RCE
CVE-2019-0550	Windows Hyper-V Remote Code Execution Vulnerability	Critical	No	No	2	2	RCE
CVE-2019-0551	Windows Hyper-V Remote Code Execution Vulnerability	Critical	No	No	2	2	RCE

Ref. : Microsoft January 2019 Patch Tuesday fixes 50 vulnerabilities

선박 및 해양 사이버보안 이슈 및 대응방안

● 선박 및 해양 사이버보안 이슈

국제 해운업계가 발표한 최근 문서 'Guidelines on Cyber Security onboard Ships(Rev.3)'에 따르면 선박은 다른 IT 시스템과 동일한 유형의 사이버 보안 문제를 겪고 있다. 이 문서에는 선박 IT/OT 시스템 보안을 위한 규칙 및 지침이 포함되어 있으며, 올바른 절차를 따르지 않을 때 어떤 일이 발생하는지에 대한 예를 소개한다. 이 사례는 과거 배와 항만에서 발생한 사이버보안 사고이며 공개적으로 드러나지 않은 사례이다.

<사례 1> ECDIS (Electronic Chart Display and Information System) 바이러스 감염

건화물 선박의 ECDIS가 바이러스에 감염되어 며칠 동안 항해 중 정박된 사례이며 이 선박은 종이해도를 탑재하지 않았다. 서비스 공급자가 탑승하여 많은 시간을 소요한 후 두 ECDIS가 바이러스에 감염된 것을 발견했다. 감염원 및 감염 경로는 알려지지 않았으며 항해 지연 및 수리 비용은 수십만 달러에 달했다.

<사례 2> 선박의 랜섬웨어 감염 사례

해상에서 항해중인 선박의 백엔드 시스템과 서버가 랜섬웨어에 감염되었다. 랜섬웨어 감염 경로는 선박 대리인 이었으며, 회사의 비즈니스 네트워크가 이메일 첨부 파일을 통해 랜섬웨어에 감염되었다. 감염이 비즈니스 네트워크에만 국한되어 항해 및 선박 운영에는 영향을 미치지 않았다. 또 다른 관련 예로는 선주가 랜섬웨어에 값을 지불했던 경우도 있다.

<사례 3> 적절한 (RDP) 암호를 설정하지 않음으로 인한 사고 발생

주요 응용 프로그램 서버에 대한 랜섬웨어 감염으로 인해 IT 인프라가 완전히 중단되었다. 랜섬웨어는 서버의 모든 중요한 파일을 암호화하여 중요한 데이터가 손실되고 선박 관리 작업에 필요한 응용 프로그램을 사용할 수 없었으며, 응용 프로그램 서버를 완전히 복구한 후에도 문제가 다시 발생했다. 감염의 근본 원인은 공격자가 원격 관리 서비스를 수행할 수 있게 해주는 잘못된 암호 정책이었으며, 회사의 IT 부서는 문서화되지 않은 사용자를 비활성화하고 사고를 수정하기 위해 선박 시스템에 강력한 암호 정책을 시행했다.

Ref. : Ships infected with ransomware, USB malware, worms

이 보고서에는 USB 드라이브가 사이버 보안 사고, 지연 및 재정적 피해를 초래 한 두 가지 사건에 대한 세부 정보가 포함되어 있다.

<사례 1>

건화물 선박은 막 벙커 작업을 마쳐 벙커 조사원은 완료 서명을 위해 문서를 인쇄하기 위한 엔진 제어실의 컴퓨터에 액세스 할 수있는 권한을 요청했다. 조사원은 컴퓨터에 USB를 삽입하여 선박의 관리 네트워크에 악성 코드를 감염시켰다. 악성 코드는 나중에 사이버 평가가 실시 될 때까지 탐지되지 않았으며 선원은 비즈니스 네트워크에 영향을 미치는 "컴퓨터 문제를 보고했다. 이는 방문객 소유의 USB 장치를 포함하여 선박 내 USB 장치의 사용을 방지하거나 제한하는 절차의 필요성을 강조한다.

<사례 2>

선박에 소프트웨어 업데이트 및 패치, 원격 진단, 데이터 수집 및 원격 작동을 위해 인터넷에 연결할 수있는 전력 관리 시스템이 장착되었다. 회사의 IT 부서는 선박을 방문하여 취약성 검색을 수행하여 인터넷에 연결되면 활성화 될 수있는 휴면 웜을 발견했다. 이 웜은 USB 장치를 통해 실행중인 프로세스로 확산되어 프로그램을 메모리로 실행하며 프로그램은 명령 및 제어 서버와 통신하여 다음 명령 세트를 수신하도록 설계되었다. 분석 결과에 따르면 서비스 제공 업체가 출처였으며 소프트웨어 설치 중에 USB 를 통해 악성코드를 시스템에 감염시켰다.

선박 및 해양 쪽 산업 시설에 대한 지속적인 사이버 공격 증가로 인해 많은 관련 기업들이 이와 같은 위협에 대응하기 위해 다양한 방법들을 모색하고 있다. USB로 소프트웨어 패치, ECIDS 업데이트, 시스템 간의 문서 이동 등 많은 용도로 사용되지만 동시에 USB를 통해 랜섬웨어와 같은 악성코드에 감염되기도 하고, 이를 통해 실제 운영되는 시스템을 공격하기도 한다. 심지어 USB 보안을 위해 인증 받은 USB만 연결이 가능하는 등의 보안 솔루션을 도입하더라도 우회하는 많은 공격 기법들이 있다.

대응방안으로 USB로 어느정도 침투가 가능한지 침투 테스트 컨설팅을 진행하기도 하며, 사이버 범죄자들이 USB를 통해 악성코드 유포나 공격을 어떻게 하는지 그리고 타겟이 어느 시설, 기업이 되는지에 대해 사전에 첩보를 입수해 대응하는 CTI (Cyber Threat Intelligence Service) 를 도입하기도 한다. 이와 동시에 내부 직원들에 대해 얼마나 쉽게 공격이 되고 감염이 되며, 영향 및 피해가 얼마나 큰지에 대한 사이버보안 교육이 반드시 필요하다. 아무리 침투테스트를 진행하고 보안 솔루션을 도입해도 내부 직원이 감염된 USB로 연결을 시도한다면 모든 보안이 무용지물이 되기 때문이다.

사이버 위협의 이해(OWASP Top 10)

● 사이버 위협 이해하기

사이버 위협이란, 조직 운영, 조직 자산, 개인, 기타 조직 또는 국가에 대해 사이버 시스템을 통한 무단 액세스, 파괴, 공개, 정보 수정 또는 서비스 거부와 같은 잠재적으로 악영향을 미칠 수 있는 상황이나 사건을 의미한다. (출처 : NIST SP : 800-128)

사이버위협은 ICT 기술이 발전함에 따라 자산에 미치는 영향이 변화하므로 자산의 취약점을 파악하기 위해 주기적으로 목록화 할 필요가 있다.

● 한국선급 해상 사이버보안 시스템 인증 검사항목(CS1)

204.1 위험관리 : 내부 정보기술 및 운영기술 환경에 의한 영향을 미치는 외부 환경 요인을 위협으로 식별하고 목록화하여야 한다.

● OWASP Top 10

OWASP(Open Web Application Security Project)는 오픈소스 웹 어플리케이션 보안 프로젝트이다. 주로 웹에 관한 정보노출, 악성 파일 및 스크립트, 보안 취약점 등을 연구하며 웹 어플리케이션 취약점 중에서 빈도가 많이 발생하고, 보안상 영향을 크게 줄 수 있는 10대 항목(OWASP Top 10)을 2004년, 2007년, 2010년, 2013년, 2017년 기준으로 발표하였다. 본 뉴스레터에서는 OWASP 10대 항목에 대해서 분석하고자 한다.

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – 인젝션	→	A1:2017 – 인젝션
A2 – 취약한 인증과 세션 관리	→	A2:2017 – 취약한 인증
A3 – 크로스 사이트 스크립팅 (XSS)	↘	A3:2017 – 민감한 데이터 노출
A4 – 안전하지 않은 직접 객체 참조 [A7 항목과 병합됨]	∪	A4:2017 – XML 외부 개체 (XXE) [신규]
A5 – 잘못된 보안 구성	↘	A5:2017 – 취약한 접근 통제 [합침]
A6 – 민감한 데이터 노출	↗	A6:2017 – 잘못된 보안 구성
A7 – 기능 수준의 접근 통제 누락 [A4 항목과 병합됨]	∪	A7:2017 – 크로스 사이트 스크립팅 (XSS)
A8 – 크로스 사이트 요청 변조 (CSRF)	☒	A8:2017 – 안전하지 않은 역직렬화 [신규, 커뮤니티]
A9 – 알려진 취약점이 있는 구성요소 사용	→	A9:2017 – 알려진 취약점이 있는 구성요소 사용
A10 – 검증되지 않은 리다이렉트 및 포워드	☒	A10:2017 – 불충분한 로깅 및 모니터링 [신규, 커뮤니티]

Ref. : OWASP Top 10 Project

● **OWASP Top 10 -2017**

OWASP Top 10 프로젝트는 개발자와 관리자의 보안 인식을 높이는 것이 목표였으나 현재는 애플리케이션 보안 업계표준이 되고 있다. Top 10 이외에도 웹 애플리케이션 보안에는 많은 위협이 있으며, Top 10 위협은 끊임없이 변화하고 있다. 2013년 대비, 'A4:2017-XML 외부개체(XXE)', 'A8:2017-안전하지 않은 역직렬화', 'A10:2017-불충분한 로깅과 모니터링' 항목이 추가되었고, A4:2013, A7:2013 항목은 'A5:2017-취약한 접근 통제' 항목으로 병합되었다.

OWASP Top 10	상세 내용
A1 : 인젝션	SQL, OS, XXE, LDAP 인젝션으로 신뢰할 수 없는 데이터가 명령어나 쿼리문의 일부분으로 전달되어 예상지 못한 명령을 실행하거나 적절한 권한 없이 데이터에 접근하게 되는 취약점
A2 : 취약한 인증	인증 및 세션 관리와 관련된 애플리케이션 기능이 잘못 구현되어 공격자가 패스워드, 키 또는 세션 토큰을 해킹하거나 다른 구현 취약점을 공격하는 취약점
A3 : 민감한 데이터 노출	대부분의 웹 애플리케이션과 API는 금융정보, 건강정보, 개인식별정보와 같은 민감정보를 제대로 보호하지 않는 취약점
A4 : XML 외부 개체(XXE)	XML문서 내에서 외부 개체 참조를 평가하는 취약점 - 외부개체는 파일 URI 처리기, 내부 파일 공유, 내부 포트 스캔, 원격 코드 실행과 서비스 거부 공격을 사용하여 내부파일을 공개할 수 있음.
A5 : 취약한 접근 통제	인증된 사용자가 수행 할 수 있는 작업에 대한 제한이 제대로 적용되지 않는 취약점 - 다른 사용자의 계정에 접근하거나, 데이터를 수정함
A6 : 잘못된 보안 구성	기본으로 제공되는 값이 잘못 정의되었거나 소프트웨어가 최신 업데이트 되지 않아 발생하는 취약점
A7 : 크로스 사이트 스크립팅(XSS)	애플리케이션이 신뢰할 수 없는 데이터를 가져와 적절한 검증이나 제한 없이 웹 브라우저로 보내져 사용자 세션 탈취, 웹 사이트 변조, 악의적인 사이트 이동등이 발생되는 취약점
A8 : 안전하지 않은 역직렬화	안전하지 않는 역직렬화로 인해 원격코드가 실행되어 권한 상승 공격, 주입공격과 재생공격 등이 수행될 수 있는 취약점
A9 : 알려진 취약점이 있는 구성요소 사용	알려진 취약점이 있는 라이브러리, 프레임워크 및 다른 소프트웨어 모듈 같은 컴포넌트로 인해 데이터 손실이나 서버가 장악되는 취약점
A10 : 불충분한 로깅 및 모니터링	불충분한 로깅과 모니터링으로 인해 데이터 변조, 추출, 변조되는 취약점

데이터 보안 정책 수립 가이드

● 데이터 보안 정책 수립 필요성

사이버 공격에 의해 회사의 기밀 정보가 유출 혹은 손상된다면 재정적 손실뿐만 아니라 평판 훼손, 생산성 저하 등의 비즈니스 연속성을 저해할 수 있으므로 데이터 보안 정책 수립이 필요하다. 회사는 시스템 장애, 데이터 파손 등으로 인한 피해를 최소화하고, 조속한 복구를 위하여 시스템 가동 및 복구에 필요한 데이터 백업계획을 수립하여 운영하여야 하며 각 시스템 관리자는 백업계획에 따라 정기 또는 필요시에 백업을 실시하여야 한다. 또한 회사는 지정한 보안등급에 따라 기밀 이상의 보안등급을 갖는 데이터는 암호화하여 저장·관리하여야 한다.

● 한국선급 해상 사이버보안 인증 검사항목(CS1)

데이터 백업(210.1) : 중요 데이터는 별도의 공간에 백업하여 안전하게 보관하여야 한다.

데이터 접근통제(210.2) : 데이터는 중요도에 따라 사용자 접근을 제한하고 물리적, 논리적 접근통제를 실시하여야 한다.

암호화 통신(216.1) : 데이터 전송 시 암호화된 방식으로 통신할 수 있는 환경을 구축하여야 한다.

데이터 암호화(216.3) : 중요 등급으로 분류된 데이터는 암호화하여 저장하여야 한다.

● 백업정책 주요 항목 (예시)

서버	백업요구사항								
	대상구분	형식	방식	용량	주기	보관주기	복구목표시간	매체	구분
DB 서버01*	OS 및 주요 파일	파일시스템	온라인	12GB	월간, 수시	3일	1시간	DAT	수동
	DBMS	파일시스템	온라인	30GB	월간, 수시	3일	2시간	DAT	자동
	DB데이터	RAW Device	온라인	120GB	일간	3일	2시간	DAT	자동
	DB로그데이터	파일시스템	온라인	12GB	일간	3일	1시간	DAT	자동
DB 서버02	OS 및 주요 파일	파일시스템	온라인	12GB	월간	3일	1시간	DAT	수동
	시스템 SW엔진	파일시스템	온라인	30GB	월간, 수시	4주	2시간	LTO	자동
	사용자 파일	파일시스템	온라인	30GB	일간	1주	1시간	LTO	자동

● 데이터 암호 유형(예시)

등급	데이터 구분	세부 내용	예시	암호화 적용
1	기밀자료	회사 내 허가된 일부 임직원에게만 제공되는 데이터	계약 현황 기밀 화물 적재 현황	O
2	대외비	회사 내 임직원은 열람할 수 있으며, 외부인에게는 제한되어 공개되지 않는 데이터	선박 운항 경로 적재 화물 현황	X
3	일반	회사 내외부 임직원, 고객, 위탁업체 직원 등 모든 사람에게 공개되는 자료	회사 소개자료 회사 공시 자료	X

● 영역별 암호화 적용 방안과 기준(예시)

적용대상	구분	예시	암호화 방법 예	권고 알고리즘* (암호 강도)
저장 시	암호화된 정보를 복호화할 수 없어야 하는 경우	비밀번호	해쉬 알고리즘	SHA-224/256/384/512
	암호화된 정보를 복호화할 수 있어야 하는 경우	기밀자료	대칭키 암호화 공개키 암호화	AES(AES-128/192/256), TEDA, ARIA, SEED
전송 시 (통신구간)	정보 전송 시 제3자에게 유출되는 것을 방지하기 위한 암호화	기밀자료, 비밀번호	통신구간 암호	SSL/TLS

● 애플리케이션 또는 매체별 암호화 적용 방안(예시)

대상	암호화 적용 방안
데이터베이스	데이터베이스 보안 전용 프로그램이나 관리시스템을 이용하여 기밀자료 등 데이터 암호화
개인용 PC	회사가 도입한 암호화 프로그램(ex : DRM 프로그램)을 이용하거나 운영체제, 오피스 프로그램, 압축프로그램이 제공하는 암호 기능 활용
이동식 저장매체	저장매체 자체에서 제공하는 암호화 기능을 이용하거나 보안기능이 없을 경우, 각 파일을 암호화한 저장
이메일	S/MIME(Security Services for Multipurpose) 등의 이메일 보안 프로토콜의 사용 또는 메일 암호화 프로그램 이용하고 해당 기능을 제공하지 않을 경우, 파일/디스크 암호 프로그램에서 제공하는 암호 활용
메신저	메신저 자체적으로 제공해 주는 대화 및 파일 전송 암호화를 적용하고, 해당 기능 미제공 시에는 사전에 암호화된 파일 제공

용어 설명

- **CVE(Common Vulnerabilities and Exposures) :** 공개적으로 알려진 소프트웨어 보안취약점을 체계적으로 관리하기 위해 취약점이 반견된 연도와 순번을 붙여 만들어진 취약점 데이터베이스로 미국의 마이터(MITRE. 비영리 연구기관)에서 운용, 관리하고 있다.

  (예) CVE-2018-0001 : 2018년 1번째로 식별된 취약점

- **SHA(Secure Hash Algorithm) :** 안전한 해시 알고리즘과 다음 버전인 SHA-1과 SHA-2는 미국 국립표준기술연구소(NIST)가 개발한 정부 표준 해시 함수이다. 해쉬란 임의의 데이터를 고정된 데이터 크기로 변환 시키는 것을 의미한다. 해쉬 알고리즘은 해쉬를 하는 방법에 대해 절차적으로 명세하며 SHA-256은 임의의 입력데이터를 256 비트의 출력데이터로 변환하는 해쉬 알고리즘이다. SHA-1은 TLS, SSL, SSH, IPSec 등 많은 보안프로토콜과 사용되었으나 최근 암호 해독 공격에 의해 SHA-1 알고리즘 약점이 노출되었다.

- **AES(Advanced Encryption Standard) :** 미국 국립표준기술연구소(NIST)는 2001년 AES를 미국 연방 정보 처리 표준(FIPS-197)로 공표하였다. 대표적인 대칭키 암호 알고리즘으로써 송·수신자가 암호화와 복호화에 같은 키를 사용한다. AES 알고리즘은 입력 평문의 길이는 128비트로 고정시키고, 사용하는 암호화 키의 길이는 128비트, 192비트, 256비트 중에서 선택할 수 있다. 지금까지 알려진 블록 암호 알고리즘에 대한 공격들에 대해 안전하게 설계되었다.

- **SSL(Secure Sockets Layer):** 넷스케이프에서 개발한 암호화 프로토콜로, 웹 서버와 웹 브라우저 간의 통신을 보호한다. SSL은 웹, 이메일, FTP뿐만 아니라 텔넷 트래픽까지도 보호하는 등 기밀성과 무결성을 보장하는 세션 지향 프로토콜이다.

- **TLS(Transport Layer Security):** SSLv3를 기반으로 만들어진 인터넷 표준 웹 보안 프로토콜이다. SSL과 같은 방식으로 작동하지만, 더 강력한 인증과 암호화 프로토콜을 사용한다.