정 보 보 호 학 회 지
제29권 제2호, 2019. 4

산업제어시스템에서의 SSL VPN 가용성 분석 연구

위 한 샘*, 이 재 훈*, 장 찬 국*, 이 옥 연*

요 약

산업제어시스템은 물리적인 현장장치의 상태를 기반으로 시스템과 시스템 내부의 프로세스들을 제어, 유지하는 CPS(Cyber Physica System)으로 볼 수 있다. 하지만 IT 시스템의 유입과 더불어 IT 시스템이 보유하고 있는 보안위협 또한 상속되었고 그에 따라 IT 시스템에서 사용하는 보안 대응책을 산업제어시스템에도 적용해야 한다. 본 논문에서는 산업제어시스템과 유사한 CPS인 교통신호제어시스템의 표준규격서에 통신보안으로 규격화 되어있는 SSL VPN을 산업제어시스템에 적용할 때 만족하는 보안요구사항을 살펴보고, 더불어 산업제어시스템에서의 보안 적용 시 반드시 고려해야 하는 가용성과 관련한 성능측정 결과를 보이고 결과분석을 수행한다.

Ⅰ. 서 론

산업제어시스템은 폐쇄적인 구조로 설계 및 운영되어왔으며, 그에 따라 사용하는 통신의 종류 역시 시리얼 통신을 주로 사용하여 현장장치 계층, 제어 계층, 운영 계층이 통신했다. 하지만 산업제어시스템의 규모와 현장장치의 수가 늘어나면서 더욱 효율적인 제어, 감시를 위해 기존 IT 시스템의 장비들이 유입되었고 IP를 기반으로 한 통신을 사용하게 되었다. 이에 따라 기존의 IT 시스템이 보유하고 있던 보안위협 또한 산업제어시스템에 상속되었다.

시리얼 통신에서 IP를 기반으로 한 통신을 사용하는 구조로 변화하면서 데이터에 대한 보안을 보장하지 않는 공중망에 현장장치를 제어, 감시하는 데이터가 노출되기 때문에 이에 대하여 데이터 기밀성, 무결성, 상호인증과정이 포함되어 있는 보안 장치와 침입 탐지를 위한 보안 장치의 사용은 필수적이다.

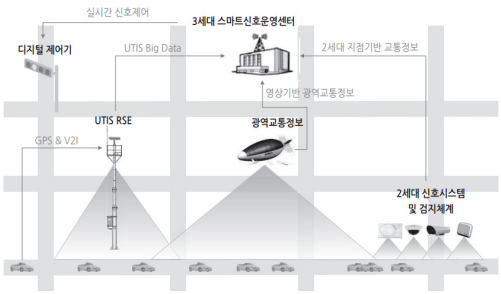
데이터 기밀성, 무결성, 상호 간 인증 기능이 가능한 대표적인 보안장치로는 VPN(Virtual Private Network)이 있다. VPN을 사용해 산업제어시스템의 운영 계층부터 제어 계층 또는 현장장치 계층까지 데이터 보안을 제공하는 가상사설망을 구성할 경우, 사용하는 망과는 독립적으로 허가되지 않은 사용자 또는 장비가 산업제어시스템 내의 현장장치와 관련된 제어, 감시 데이터를 분석, 분석을 통한 위/변조하는 등의 데이터 보안위협으로부터 제어, 감시 데이터에 대한 기밀성, 무결성 그리고 상호인증 기능을 제공받을 수 있다.

교통신호제어시스템의 경우 IP 기반의 유 무선통신의 도입에 따라 경찰청 교통신호제어기 표준규격서에 SSL VPN을 통한 교통신호제어기와 중앙관제시스템 사이의 제어, 모니터링 데이터에 대한 보안을 규격화 하였으며, 교통신호제어시스템에서 사용하는 SSL VPN의 경우 SSL VPN에서 사용하는 데이터 보안을 위해 사용하는 암호알고리즘은 KCMVP(Korea Cryptographic Module Validation Program) 검증필암호모듈을 적용해야 하고, 이를 바탕으로 CC(Common Criteria) 인증을 받은 SSL VPN을 사용해야 함을 명시하고 있다.[1]

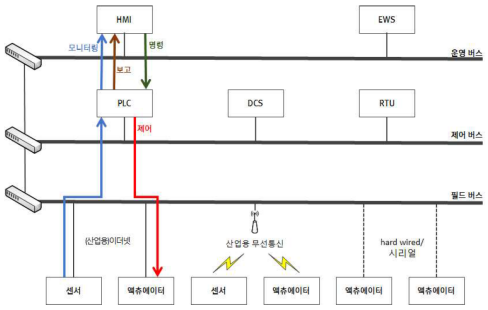
교통신호제어시스템과 산업제어시스템은 서로 다른 시스템이며 시스템 운영 방식, 설계 등에서 차이를 보이지만 현장의 물리적인 장치의 제어결과, 상태를 기반으로 신호체계 또는 작업공정을 유지 또는 변경하는 시스템과 시스템 내에서 동작하고 있는 여러 소프트웨어를 제어한다는 관점에서 생각했을 때 유사한 구조의 CPS로 생각할 수 있다.

교통신호제어시스템에서 중앙관제시스템과 산업제어시스템의 운영 계층 그리고 교통신호제어기와 산업제어시스템의 현장 계층은 특정 현장의 장치들을 제어하기 위한 명령을 전달하고, 그를 수행한 결과를 보고한다는 관점에서 유사하다. 더불어 데이터 보안을 적용해야

* 국민대학교 금융정보보안학과 (whssktk@kookmin.ac.kr, guderian88@kookmin.ac.kr, jangchankuk@kookmin.ac.kr, oyyi@kookmin.ac.kr)



〔그림 1〕 스마트 교통신호제어시스템 구조〔2〕



〔그림 2〕 산업제어시스템 네트워크 구성〔3〕

하는 대상이 현장장치들의 제어 데이터와 상태 데이터라는 점은 교통신호제어시스템에서 통신보안 규격으로 선택한 SSL VPN이 산업제어시스템에서도 사용될 수 있음을 의미하며 산업제어시스템에 적용 시 참고할 수 있는 성능 치를 마련을 통한 가용성 분석이 필요하다. 본 논문에서는 산업제어시스템에서의 IP 기반 통신보안의 방안으로 교통신호제어시스템의 통신보안 규격으로 명시된 방법으로 구현된 SSL VPN을 적용했을 때의 성능을 측정하고 성능에 대한 원인을 분석한다.

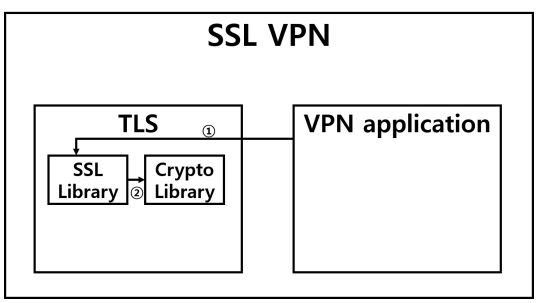
Ⅱ. 본 론

2.1. 검증필암호모듈 SSL VPN 구조

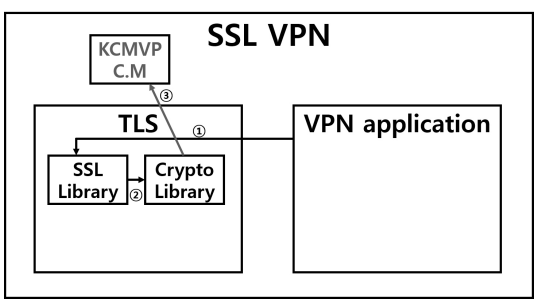
SSL VPN은 TLS가 구현된 라이브러리를 이용해 가상사설망을 구성하고 망 내에서 송/수신되는 데이터에 대한 보안을 제공하는 애플리케이션 또는 애플리케이션이 동작하는 하드웨어를 말한다. TLS 표준을 구현한 OpenSSL, MbedTLS 등의 오픈소스는 보통 SSL 라이브러리, Crypto 라이브러리로 이루어져 있으며 SSL 라이브러리에서는 통신과 관련된 기능을 지원하고 Crypto 라이브러리에서는 인증과정과 데이터 보안에 사용되는 블록암호, 공개키암호, 해시함수,메세지 인증코드 생성 등의 기능을 지원한다.

검증필암호모듈의 암호알고리즘을 SSL VPN의 데이터 채널 암호화에 사용하기 위해서는 VPN 애플리케이션에 사용되는 SSL 라이브러리에서 호출되는 Crypto 라이브러리의 암호알고리즘 목록에 검증필암호모듈의 암호알고리즘들을 추가해야 하며 그에 따른 Cipher Suites 들도 추가하는 방식으로 연동시켜야 한다. 연동이 완료된 후 암호알고리즘 호출 구조는 [그림 3]에서 [그림 4]와 같이 된다.

[그림 4]처럼 SSL 라이브러리에서 사용하는 암호알고리즘을 검증필암호모듈의 암호알고리즘을 사용하도록 구성하면 KCMVP의 보호함수 목록에 존재하는 암호알고리즘을 사용해 데이터 보안을 적용할 수 있지만 검증필암호모듈의 암호알고리즘의 최상위 API를 호출하고 내부함수들을 다시 거쳐 암호알고리즘의 출력값이 반환되기 때문에 기존의 구조보다 더 많은 함수호출을 하게 되며, 가용성을 저하시키는 요인이 된다.



〔그림 3〕 SSL VPN의 암호알고리즘 호출 구조



〔그림 4〕 KCMVP 검증필암호모듈이 탑재된 SSL VPN 암호알고리즘 호출 구조

2.2. 산업제어시스템 데이터 보안 요구사항

본 소단원에서는 산업제어시스템에서의 데이터 보안 요구사항을 소개하고 이에 대해 SSL VPN이 데이터 보안요구사항을 만족할 수 있는지 살펴본다. 산업제어시스템에서는 SCADA 프로토콜을 사용하여 현장장치의 제어, 상태 감시를 수행한다. 이때 발생할 수 있는 보안 위협은 [표 1]과 같으며 그에 대응하는 보안 요구사항은 [표 2]와 같다.

〔표 1〕 산업제어시스템 데이터 보안위협〔3〕

보안위협 항목	설명
제어시스템 서비스방해 (무결성, 가용성)	인증되지 않은 공격자는 고의적으로 다량의 정상적인 패킷이 발생하게 할 수 있고 운영계층, 제어계층의 장치들이 처리하기 어려울 정도의 패킷이 발생되었을 시 시스템의 가용성에 큰 영향을 끼친다.
데이터 유출 및 분석 (기밀성)	데이터 기밀성에 대한 부재로 인하여 네트워크상의 공격자에게 제어, 감시 데이터의 평문이 유출될 수 있고 공격자는 이를 분석하여 2차적인 공격에 활용할 수 있다.
데이터 위/변조 (무결성, 가용성)	유출된 제어, 감시 데이터를 활용하여 공격자는 원하는 데이터를 위조 또는 변조하여 현장장치의 상태 값을 임의적으로 변경할 수 있다.
데이터 재사용 (무결성, 가용성)	공격자는 유출 후 저장된 제어, 감시데이터를 재사용하여 현장장치의 상태 값을 변경시킬 수 있다.

〔표 2〕 산업제어시스템 데이터 보안 요구사항〔3〕

보안요구사항	설명
장치 식별 및 인증	장치의 신원을 검증하기 위해 서비스 제공 이전에 식별 및 인증 기능을 제공해야 한다.
전송데이터 무결성	민감한 전송데이터에 대해 위/변조 여부와 재사용 공격에 대비한 최신성 여부를 확인할 수 있도록 무결성 보장 기능을 제공해야 한다.
전송데이터 기밀성	민감한 전송데이터에 대해 기밀성 보장 기능을 제공해야 한다.
통신 세션 자동 종료	일대일 통신에 있어 설정 시간을 초과한 세션, 설정 시간 동안 미사용중인 세션, 사용 목적을 달성한 세션에 대해서는 종료하는 기능을 제공해야 한다.
암호연산	암호연산을 사용하는 경우 안전한 암호알고리즘 및 암호키 길이를 사용하여 암호연산이 수행되어야 한다.
암호키 관리	암호연산을 위해 사용하는 암호키에 대해 안전한 키 생성/설정/저장/파기 방법을 사용해야 한다.

[표 2]에서 나타난 산업제어시스템에서 요구되는 데이터 보안요구사항을 만족시킬 수 있는 정보보안의 기능은 상호 간 인증, 데이터 암호화, 데이터 무결성, 암호키 관리, 세션 생성과 종료 총 4가지로 분류할 수 있다. [표 3]은 [표 2]에 나타난 보안요구사항 중 VPN이 만족할 수 있는 보안 기능 지원 여부를 나타내며 비교를 위해 데이터 보안을 위해 사용되는 기법 중 구간 암호화 기법의 보안 기능 지원 여부를 함께 나타냈다.

구간 암호화 기법은 통신을 수행하는 두 개체가 사전 공유 키 혹은 키 관리 시스템으로부터 발급받은 대칭

〔표 3〕 VPN과 구간 암호화 보안 기능 별 지원 여부

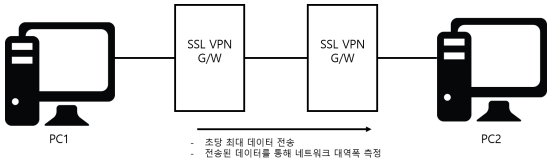
보안요구사항	SSL VPN	구간 암호화
장치 식별 및 인증	O	X
전송데이터 무결성	O	O
전송데이터 기밀성	O	O
통신 세션 자동 종료	O	X
암호연산	O	O
암호키 관리	O	X

키를 사용해 서로 간 송/수신되는 데이터를 암호화 하는 기법을 말한다.

구간 암호화 기법은 데이터 암호화에 초점이 맞춰져 있는 기법이기 때문에 장치 식별이나 인증을 진행하지 않는다. 더불어 별도의 키 관리 시스템을 사용하지 않는 경우 통신 세션 별 세션 키 발급 기능을 지원할 수 없다. 그에 반해 SSL VPN은 handshake 과정에서 공개키 인증서를 기반으로 한 상호 간 인증과 DH(Diffie-Hellman) 또는 ECDH와 같은 키교환 프로토콜을 사용하여 세션 키를 생성하고 그를 바탕으로 설정에 맞는 세션 동안 통신 후 세션을 종료하거나 재생성할 수 있는 특징이 있으며 이에 따라 [표 2]의 보안 요구사항을 모두 만족할 수 있다. 산업제어시스템의 정보보호 우선순위는 가용성, 무결성, 기밀성 순으로 중요하다.[3] 그러므로 SSL VPN이 산업제어시스템에 적용되기 위해서 가용성에 대한 검증이 필요하며 소단원 2.3에서는 2.1에서 설명한 구조로 구현된 SSL VPN을 설치하여 두 대의 PC 간 네트워크 대역폭을 측정한 결과를 나타내고 분석한다.

2.3. 성능 분석

본 소단원에서는 SSL VPN을 설치한 후 통신 성능 분석을 수행하며 성능측정 방법은 [그림 5]와 같다. SSL VPN을 설치하고 두 PC 간 네트워크 대역폭을 측정함으로써 PC1과 PC2를 직결했을 때와 비교해 얼마만큼의 성능 차이를 나타내는지 알아본다. 더불어 성능 저하에 영향을 미치는 요소들에 대해서도 분석한다. SSL VPN은 크게 상호 간 인증, 인증 후 생성된 세션 키를 사용한 데이터 암호화 과정으로 나눌 수 있다. 상호 간 인증 시 SSL VPN 서버 G/W와 클라이언트 G/W는 공통적으로 지원하는 Cipher Suite가 있어야만 인증을 진행할 수 있다. [표 5]는 경찰청 교통신호제어기 표준규격서에 명시된 Cipher Suites를 나타내며 본 소단원에서 수행한 성능측정 시 SSL 게이트웨이 간 보안 세션을 생성하기 위해서 [표 5]에 나타난 Cipher Suites를 사용했다. SSL VPN은 세션 키 생성을 위한 인증을 한 번 수행한 후 세션 생명주기 동안은 같은 세션 키로 보안통신을 수행하기 때문에 인증시간은 SSL VPN 성능 중 매우 적은 비중을 차지하므로 성능측정에서 제외했으며 세션 키를 사용한 암호화 통신 시의 네트워크



〔그림 5〕 네트워크 대역폭 측정 실험방법

대역폭을 측정했다. [그림 5]에 나타난 SSL VPN G/W는 PC1, PC2를 내부망에 구성하고 있음을 표시하기 위해 나타낸 것이며 성능에는 영향을 주지 않는다.

〔표 4〕 SSL VPN 장비 사양

하드웨어	설명
Processor	TI AM Processor (up to 800MHz)
RAM	Mobile DDR3 SDRAM 256MByte
Interface	Giga-bit Ethernet RJ45

〔표 5〕 경찰청 교통신호제어기 표준규격상에 명시된 SSL VPN Cipher Suites

Cipher Suite Name	Key exchange	Encryption
TLS_KCMVP_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256	ECDH	ARIA_128_GCM
TLS_KCMVP_ECDH_ECDSA_WITH_LEA_128_GCM_SHA256	ECDH	LEA_128_GCM
TLS_KCMVP_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256	ECDH	ARIA_128_CBC
TLS_KCMVP_ECDH_ECDSA_WITH_LEA_128_CBC_SHA256	ECDH	LEA_128_CBC
TLS_KCMVP_RSA_ECDSA_WITH_ARIA_128_GCM_SHA256	DH-2048	ARIA_128_GCM
TLS_KCMVP_RSA_ECDSA_WITH_LEA_128_GCM_SHA256	DH-2048	LEA_128_GCM
TLS_KCMVP_RSA_ECDSA_WITH_ARIA_128_CBC_SHA256	DH-2048	ARIA_128_CBC
TLS_KCMVP_RSA_ECDSA_WITH_LEA_128_CBC_SHA256	DH-2048	LEA_128_CBC

〔표 6〕 SSL VPN 데이터 전송 대역폭 측정결과

암호알고리즘	운영모드	대역폭
ARIA-128	CBC	30.6 Mbps
	GCM	38.9 Mbps
SEED-128	CBC	29.8 Mbps
	GCM	38.2 Mbps
LEA-128	CBC	32.5 Mbps
	GCM	43.1 Mbps

[표 6]는 PC 두 대 사이에 SSL VPN을 설치한 후 네트워크 대역폭 측정을 한 결과이며 10초동안 PC1에서 PC2로 데이터를 전송한 평균 대역폭을 측정하는 방법으로 실험하였다. 데이터 채널에 사용된 암호화는 검증필암호모듈의 보호함수인 국산 블록암호 ARIA, SEED, LEA를 사용했다. 운영모드는 현재 경찰청 교통신호제어기 표준규격서에 등재된 운영모드인 CBC와 GCM 운영모드를 사용하여 실험을 수행했다.

알고리즘별 대역폭 성능측정 결과의 특징으로는 ARIA, SEED, LEA 단일 알고리즘 간 성능 차이와 비교적으로 작은 차이를 보인다는 것이다. 이는 SSL VPN 전체 과정 중 암/복호화, 메시지 인증코드 생성/검증과정이 수행되는 시간은 일부이며 통신과 관련된 소스코드 수행시간과 암호알고리즘 수행시간이 더해져 네트워크 대역폭에 영향을 주기 때문에 단일 알고리즘별 성능 차이에 비례하는 네트워크 대역폭 성능 차이가 나타나지 않는 것으로 분석했다.

SSL VPN을 설치하지 않고 PC1, PC2를 직결하여 측정한 네트워크 대역폭은 351Mbps로 SSL VPN을 사용할 경우 최소 대역폭인 SEED-128 CBC 운영모드를 사용할 때의 대역폭인 29.8Mbps, LEA-128 GCM 운영모드를 사용할 때의 대역폭은 기존의 대역폭의 11%~12%를 나타냈다.

성능저하에 영향을 미치는 요소로 먼저 SSL VPN에서 보안을 적용하기 위해 데이터를 애플리케이션 계층까지 올림으로 인해 생기는 시간이다. VPN과 더불어 데이터 보안을 위해 사용하는 구간 암호화같은 경우 4계층의 헤더까지 캡슐화된 패킷을 받아들여 암호화, 메시지 인증코드 생성 등의 데이터 보안을 적용하지만 SSL VPN은 이와 같은 과정을 위해 애플리케이션 계층까지 데이터를 올려 보안을 적용하는 방식을 사용한다.

두 번째로 검증필암호모듈을 SSL Crypto 라이브러리에 연동함으로써 생기는 추가적인 함수호출이 성능저하에 영향을 미친다. 검증필암호모듈이 연동되지 않은 SSL VPN은 데이터 보안을 적용하기 위해 SSL Crypto 라이브러리의 암호알고리즘 함수 API만을 호출하는 방식을 사용하지만 검증필암호모듈이 연동된 SSL VPN의 경우 SSL Crypto 라이브러리에서 다시 검증필암호모듈의 암호알고리즘 API를 호출하고 검증필암호모듈의 최상위 API로부터 내부함수들을 여러번 호출하는 작업을 암호화하는 패킷마다 수행하기 때문이다.

Ⅲ. 결 론

본 논문에서는 CPS 보안 관점에서 교통신호제어시스템의 SSL VPN을 산업제어시스템에 적용할 때 SSL VPN이 산업제어시스템의 보안 요구사항을 만족할 수 있는 보안 기능들을 설명하고 산업제어시스템의 정보보호 요소 중 우선순위가 가장 높은 가용성과 관련하여 SSL VPN을 설치한 후 데이터 통신의 네트워크 대역폭을 측정했다. 이를 통해 산업제어시스템에 검증필암호모듈이 연동된 SSL VPN을 적용할 때 참고할 수 있는 네트워크 대역폭 성능 치와 SSL VPN으로 인해 발생하는 네트워크 대역폭 성능저하의 이유, 그리고 검증필암호모듈을 SSL VPN에 연동함으로써 생길 수 있는 네트워크 대역폭 성능저하의 이유에 대해서도 분석했다.

참 고 문 헌

[1] “교통신호제어기 표준규격서”, 경찰청, 2019
[2] 고광용, “스마트 신호제어시스템 개발 현황과 교차로의 미래”, TTA Journal Vol.160, pp. 44-50, 2015
[3] TTA, “산업제어시스템 보안요구사항”, TTAK.KO-12.0307
[4] NIST Special Publication 800-113, Guide to SSL VPNs
[5] 최승오, 김우년, “사이버 물리 시스템 테스트베드 기술 연구 동향”, 정보보호학회지 제 27 권 제2호, pp. 46-56, 2017
[6] 이재훈, “LTE 통신망을 이용한 교통신호제어시스템용 HW 기반 SSL VPN 성능 분석 연구”, 정보

보호학회지 제27권 제2호, pp. 22-28, 2017
[7] www.openssl.org
[8] tls.mbed.org

〈저 자 소 개〉

위 한 샘 (Hansaem Wi)
정회원
2016년 3월 : 국민대학교 수학과 졸업
2018년 9월 : 국민대학교 금융정보보안학과 석사 졸업
2018년 9월 ~ 현재 : 국민대학교 금융정보보안학과 박사과정
<관심분야> 전자공학, 통신공학, 정보보호

이 재 훈 (Jaehoon Lee)
정회원
2013년 3월 : 국민대학교 수학과 졸업
2019년 3월 : 국민대학교 금융정보보안학과 박사 졸업
<관심분야> 네트워크 보안, 정보보호

장 찬 국(Chankuk Jang)
정회원
2016년 3월 : 국민대학교 수학과 졸업
2018년 3월 : 국민대학교 금융정보보안학과 졸업
2018년 3월~현재 : 국민대학교 금융정보보안학과 박사과정
<관심분야> 네트워크 보안, 정보보호

이 옥 연 (Okyeon Yi)
정회원
1990년 2월 : 고려대학교 대수학 석사 졸업
1996년 8월 : University of Kentucky 대수학 박사 졸업
2001년 9월~현재 : 국민대학교 과학기술대학 금융정보보안학과 교수
<관심분야> 네트워크 보안, 정보보호