Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.3, Jun. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.3.725

제어시스템 보안인증 도입 방안 연구*

최 호 열,† 김 대 영, 신 형 준, 한 창 희, 허 준 범‡
고려대학교 컴퓨터학과

A Study on Introducing Security Certification for Control Systems*

Hoyeol Choi,† Daeyeong Kim, Hyungjune Shin, Changhee Hahn, Junbeom Hur‡
Department of Computer Science and Engineering, Korea University

요 약

SCADA 시스템은 국내 산업분야 전반에서 원격 감시 제어를 위해 이용되고 있는 만큼 제어시스템의 보안인증을 올바르게 확립해야 할 필요가 점차 커지고 있다. ISASecure에서 진행하는 EDSA-CRT 테스트는 장치가 정상적인 환경과 비정상적인 네트워크 프로토콜 트래픽 환경에서 핵심 서비스를 적절하게 제공할 수 있는지에 초점이 맞춰져 있기는 하지만 IP, ARP, TCP등 IP 기반 프로토콜을 대상으로 진행하고 있고, 제어 프로토콜에 적용한 테스트 연구는 전무하다. 따라서 본 논문에서는 제어 프로토콜 중 가장 널리 사용되는 DNP3 프로토콜에 대해 EDSA-CRT를 적용하여 테스트 요구사항을 도출하고자 한다. 이에 우리는 DNP3 프로토콜에 대한 33개의 테스트 케이스를 제시한다.

ABSTRACT

SCADA(Supervisory Control and Data Acquisition) system is widely used for remote monitoring and control throughout the domestic industry. Due to a recent breach of security on SCADA systems, such as Stuxnet, the need of correctly established secure certification of a control system is growing. Currently, EDSA-CRT (Embedded Device Security Assurance-Communication Robustness Test), which tests the ability to provide core services properly in a normal/abnormal network protocol, is only focused on the testing of IP-based protocols such as IP, ARP, TCP, etc. Thus, in this paper, we propose test requirements for DNP3 protocol based on EDSA-CRT. Our analysis show that the specific test cases provide plentiful evidences that DNP3 should follow based on its functional requirements. As a result, we propose 33 specific test case for DNP3 protocol.

Keywords: SCADA, DNP3, EDSA-CRT, Certification, Robustness Testing, Load Stress Testing

I. 서 론

국내 국가핵심기반기설을 관리하기 위해 사용하는 제어 시스템 중 가장 널리 사용되는 SCADA 시스템은 통신, 전기, 가스, 수도, 교통 등 국가 주요기간시설과 제조업 및 국내 산업분야 전반에서 원격 감시제어를 위해 이용되고 있다. 최근, 제어시스템 보안사고의 급증으로 인해 보안의 문제가 안전, 나아가 국가안보의 문제로 대두되고 있다. 이에 제어시스템의 보안인증을 올바르게 확립해야 할 필요가 점차 커지고 있다. 특히 2014년 말 국내에 발생한 한국수력원자력 원전자료 유출 사건으로 폐쇄망인 제어시스템의 보안위험이 심각하다는 것이 확인되었고 이를 해결하기 위해 제어시스템에 대한 견고한 보안인증 시스템을 구축해야 한다는 인식이 확대되었다. 또한 2010년 이란의 원자력발전소에 대한 해킹사고인 Stuxnet 사건으로 인해 폐쇄망으로 운영되는 시설 또한 사이버공격에 안전하지 않다는 것이 확인되었

Received(01. 08. 2016), Modified(05. 19. 2016), Accepted(05. 22. 2016)
* 이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2013R1A2A2A01005559).
† 주저자, cho4103@korea.ac.kr
‡ 교신저자, jbhur@korea.ac.kr(Corresponding authour)

고, 이는 국가 재난 예방을 위해서 국가 기간 시설을 아우르는 제어시스템에 대한 철저한 보안인증이 시급하다는 것을 보여주었다.

국내 및 해외에서 약 88% 이상 이용되는 사실상 표준(De Facto Standard)인 SCADA 시스템 외에 MODBUS 등 제어시스템에 사용되는 다양한 프로토콜에는 여러 형태의 보안취약점이 존재하며 이를 악용한 여러 가지 유형의 공격이 발생하고 있다. 다양한 형태의 공격들은 향후 국가 기간 시설의 운영을 마비시켜서 재난사태까지 초래할 수 있다는 측면에서 국내 제어시스템의 안전성을 면밀하게 평가할 수 있는 시스템 마련이 시급하다. 더욱이 제어시스템을 구성하는 각 분야를 대상으로 한 보안사고가 꾸준히 발생하고 있으며, 이에 대비하기 위한 보안인증 시스템의 확립이 필요하다.

현재 ISCI(ISA Security Compliance Institute, 국제 자동화학회 보안준수 연구소)는 SCADA 시스템의 보안을 향상시키기 위해 ISASecure 인증 프로그램을 만드는 등 국제적 차원에서 보안인증 시스템 확립을 위한 연구가 진행 중이다. 특히 ISASecure에서 진행하는 EDSA (Embedded Device Security Assurance)는 임베디드(Embedded) 장치의 보안과 장치 별 특성 및 장치공급자 개발 과정상의 보안 이슈에 초점을 맞추고 있다. EDSA를 이루는 인증 분야 중 CRT (Communication Robustness Test)는 테스트 장치가 정상적인 환경과 비정상적인 네트워크 프로토콜 트래픽 환경에서 핵심 서비스를 적절하게 제공할 수 있는 기능 테스트에 초점을 맞추고 있다. 하지만 EDSA-CRT 테스트는 IP, ART, TCP 등 IP 기반 프로토콜을 대상으로 진행되고 있으며 제어 프로토콜에 적용한 테스트 연구는 전무하다. 따라서 본 연구에서는 제어 프로토콜 중 가장 널리 사용되는 DNP3(Distributed Network Protocol) 프로토콜에 대해 EDSA-CRT를 적용하여 테스트 요구사항을 도출하고자 한다.

II. 관련 연구

2.1 제어 시스템

최근 첨단 정보통신기술의 발달로 인한 철도, 발전소, 전력 등 국가단위 기간기설들의 제어 시스템도 진화하고 있다. 이러한 제어 시스템은 물리적 기능 및 섬세한 프로세스를 제어 및 감시하기 위하여 핵심 기간 시설 및 산업에서 채택하고 있는 시스템이다. 일반적으로 제어 시스템은 필드에서 생성된 데이터와 필드 내 센서의 측정 데이터를 수집하고 중앙에서 원격까지 장비를 순차적으로 제어하는 명령을 수행한다. 특히 대규모 플랜트 네트워크와 같은 제어 시스템 기반 환경은 국가 단위에서 관리하며 주요 핵심 기반시설로 분류되고 있다 [1].

제어 시스템 내에서 장치들은 상호 또는 외부 기기와 연결되며, 각 장치에 대한 원격 제어 및 접근이 가능하다. 또한 단방향 명령 전달 및 조작에서 벗어나 양방향 통신 서비스 환경이 구축되고 있다. 이 중 SCADA 시스템은 원방감시 제어 시스템, DCS (Distributed Control System) 시스템은 분산 제어 시스템, 그리고 ICS(Industrial Control System) 시스템은 산업 제어 시스템으로 각각 분류되고 있다.

SCADA 시스템은 1960년 무렵 원격 시스템을 효과적으로 제어 및 조작하기 위해 사용되기 시작하였다. 당시 제어 시스템의 대다수는 특정 업체에 의해 독점적으로 개별 제작되었으나, 이후 네트워크 기술 표준화에 따라 1990년 이후 점차 시스템의 운영 및 관리, 그리고 상이한 시스템 간 연계와 상호운영 요구가 증대됨에 따라 점차 개방형 시스템으로 변화하게 되었다. 이에 따라 시스템의 많은 부분에 걸쳐 표준화가 현재까지 추진되고 있다. 이는 폐쇄적인 네트워크인 SCADA 시스템의 네트워크 구성이 공중망에 걸치게 되었고, 인터넷을 통해 외부로 노출되는 등 새로운 보안 이슈가 발생하게 되었다.

기존의 SCADA 시스템과 같은 대규모 제어 시스템 시설들은 대부분 물리적 보안 요구사항을 충족하는데 주력했지만, 점차 제어 시스템의 개방화 추세에 따라 해킹, 바이러스 등 여러 가지 악성 소프트웨어를 이용한 공격으로부터 제어 시스템을 안전하게 보호하기 위한 요구가 증대되고 있다 [2, 6, 7].

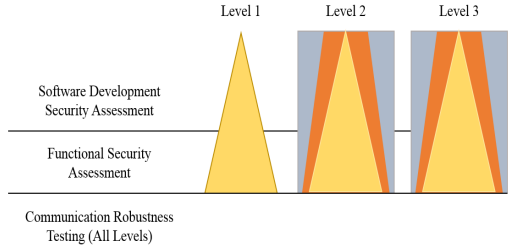


Fig. 1. ISASecure EDSA Certification Structure

2.2 EDSA-CRT

2.2.1 EDSA

ISASecure 프로그램이 산업 간 컨소시엄, 즉 ISCI에서 발족하여 산업 전반에 걸쳐 IACS (Industrial Automation and Control Systems)에 대한 사이버 보안에 대한 개선을 목적으로 시작되었다. 이는 해당 시스템에 산업 표준의 장치와 장치 보안을 준수하는 프로세스 요구사항을 제공함으로써 보안 기능을 제공한다. 특히 시스템 관리자와 장치 보안인증에 대한 조달 과정을 단순화함으로써 효율성을 증대시키고 있다.

ISASecure 검증(Certification)은 앞서 기술한 장치들 중 특히 임베디드 장치의 보안 이슈 및 해당 장치의 특성과 장치 공급자 개발 과정 검증을 위해 사용된다. 이러한 검증을 ISASecure EDSA라 부르며, 임베디드 장치가 해당 ISASecure 검증 요구사항을 만족하게 되면 ISASecure EDSA 인증을 받게 된다.

임베디드 장치는 내부에 임베디드 소프트웨어를 구동하는 동시에 직접적으로 감시, 조작 및 산업 프로세스를 가동하는데 목적을 두고 있다. 이러한 임베디드 장치 중에는 PLC(Programmable Logic Controllers), DCS, 그리고 RTU(Remote Terminal Unit)이 포함된다. ISASecure EDSA 인증은 세 단계의 검증으로 이루어지며 이를 통해 장치의 단계적 보안인증을 제공된다. 각 단계는 각각 ISASecure Level 1, ISASecure Level 2, ISASecure Level 3로 각각 나뉜다. 인증의 모든 단계는 SDSA(Software Development Security Assessment), FSA(Functional Security Assessment), 그리고 CRT를 포함한다. Fig.1.에서와 같이 SDSA와 FSA 요구사항은 단계가 올라감에 따라 증가하게 되며, CRT의 경우에는 인증 단계에 관계없이 일정하게 유지된다 [12].

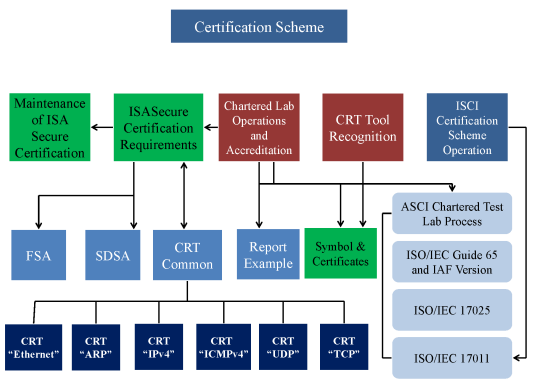


Fig. 2. Detailed Formal Specifications of EDSA

ISASecure EDSA 인증을 받기 위해서는 SDSA, FSA, CRT 세 가지 보안 평가 테스트를 받아야 한다. SDSA는 장치가 어떠한 환경에서 개발되었는지를 검사한다. FSA는 장치의 보안 기능을 검사하며, 어떤 경우에는 장치의 보안 기능이 시스템 환경 전반에 걸쳐 할당되어 있는지를 파악한다. CRT는 장치가 정상적이거나 혹은 오작동하는 네트워크 프로토콜 트래픽 하에서 주요 기능들을 적절하게 수행할 수 있는지를 검사한다. 이상의 테스트들은 일반적으로 잘 알려진 네트워크 공격에 대한 민감성 테스트 항목들을 포함한다.

2.2.2 CRT

통신의 견고성(Robustness)은 임베디드 장치에 대한 네트워크 프로토콜 구현이 비정상적인 공격이나 악의적인 트래픽 등 네트워크로부터 발생하는 여러 가지 통신에 대하여 얼마나 안정적으로 동작하는지에 대한 척도를 가리킨다. 특히 유효하지 않은 메시지 혹은 일치하지 않은 메시지 시퀀스가 생성되어 다양한 트래픽 경로를 통해서 장치로 유입되는 상황 등을 의미한다. 또한 일반적으로 잘 알려진 네트워크 공격으로부터 각 프로토콜이 어느 정도로 민감한지를 테스트 하는 부분이 검증의 일부로 포함되어 있다 [8].

적절하지 않은 메시지 응답이나 장치가 적절하게 주요 서비스를 유지하지 못한다면 이는 장치 내의 잠재적인 보안 취약점으로 간주된다. 여기서 CRT는 구현의 정확성이나 프로토콜 표준의 의무적인 확장에의 순응과 같은 요소를 검사하는 기능을 제공하지 않는다. ISASecure CRT의 핵심 정의는 '적절하게 주요 서비스를 제공'할 수 있는가를 말한다. 여기서 주요 서비스란 일반적으로 프로세스 조작, 프로세스 뷰, 커맨드, 그리고 프로세스 알람 등을 말한다. ISCI에서는 각 그룹 별 프로토콜에 대한 CRT 상세 작업을 진행하고 있다. 여기서 프로토콜 별 그룹은 우선순위를 기준으로 분류되며, 그룹 1이 가장 높은 우선순위를 가진다.

CRT 테스트는 다음의 세 단계로 이루어진다.

● 기본 동작(Baseline Operation): 기본 동작 단계에서는 적은 양의 부하에서 테스트 사례가 적절하게 동작하는지 판별한다.

● 기본 견고성 테스트(Basic Robustness Testing): 기본 견고성 테스트는 임의의 오류가 포함된 프레임이나, 단일 혹은 조합된 오류성 신호 하에서 오류를 범하지 않는지에 대한 구현을 조사한다.

● 부하 스트레스 테스트(Load stress testing): 부하 스트레스 테스트는 유효한 프로토콜 데이터 유닛으로 이루어진 높은 트래픽 환경에서의 응답 및 구현 상태를 조사한다.

또한 CRT가 ISASecure EDSA에서 담당하는 공식적인 사양은 Fig.2.와 같다 [2]. 기술적인 사양은 장치가 인증될 것인지를 결정하는데 적용하는 내용을 포함한다. 이에 대한 승인(Accreditation)은 테스트 조직이 어떻게 CRT 도구 인정 허가를 얻은 공식적으로 발급받을 수 있는지를 설명한다.

III. DNP3 프로토콜 테스트 요구사항

3.1 DNP3

DNP3는 자동화 처리 시스템에서 구성 요소들 간의 통신에 사용되는 통신 프로토콜이다. 이 프로토콜은 전기나 수도 등 국가 주요 기간 시설에 사용되고 있다. DNP3는 SCADA 시스템에서 주 처리 국(Master)과 지국(Outstation) 사이의 통신을 관장하는 중요한 역할을 하고 있다 [3] , [4] , [5] .

3.2 범위

이 논문은 DNP3 프로토콜이 작동하는 임베디드 장치 실행의 견고성 테스트의 요구사항을 제공하는데 목적을 두고 있다. 요구사항은 다음의 상황에서 프로토콜이 보여야 하는 자기 방어 능력으로 정의 한다.

● 정상적으로 형성된 메시지와 메시지 순번

● 부정확한 메시지

● 부적절한 순번의 메시지

이러한 상황에서 장치가 자동화 시스템 제어와 오류 보고 기능을 지속적으로 제공해주지 못한다면 그 장치 내부에 잠재적인 보안상의 취약점이 있다는 것이 증명된다. 이 연구에서는 제어 표준이 정확히 구현되었는지에 대한 여부나 필수 항목들이 일치하는지 테스트하는 방법을 제시하는 연구는 아니다. 이러한 정확성 테스트는 단순히 외부 자극에 의한 장치의 응답을 관찰하는 것만으로는 확인 할 수 없다.

3.3 테스트 프로토콜 요소

본 장에서는 DNP3의 대한 견고성 테스트를 명시한다. 이 테스트는 구현된 프로토콜이 응용계층(Application Layer), 전송 함수(Transport Function), 데이터 링크 계층(Data Link Layer)에서 무작위로 선정된 오류를 포함한 프레임을 수신할 때 정상적으로 작동하는지 조사한다. Fig.3.은 계층화 스택(Layering Stack)에서 각 계층이 어느 위치에 위치하는지 보여준다 [5].

3.3.1 응용계층

응용 계층은 EPA 와 OSI 모델에서 가장 상위에 있는 계층이며 하위 계층과 DNP3 사용자의 소프트웨어 사이의 인터페이스이다. 응용계층은 표준화된 기능들(Standardized Functions), 데이터 포맷(Data Formats), 데이터 취득 값(Acquisition Values)과 제어 명령 속성(Control Commands)의 절차를 제공한다. DNP3 사용자의 소프트웨어는 고유 장치가 주 처리 국, IED, 데이터 집중기

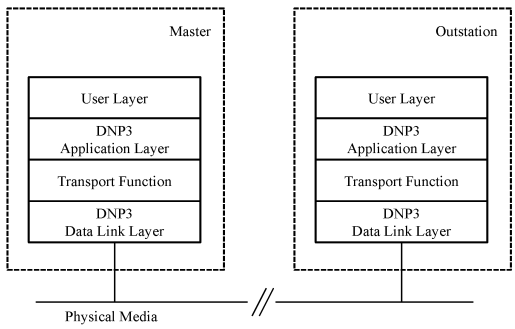


Fig. 3. 3-Layering Stack for DNP3

(Data Concentrator)를 구분하는 역할을 하는 응용 프로그램이다. 또한 DNP3 사용자의 소프트웨어는 다른 DNP3 장치에서 메시지를 보내고 받을 수 있는 응용 계층의 서비스를 사용한다.

3.3.2 전송함수

전송 함수는 응용 계층과 데이터 링크 계층 사이에 존재하고 있다. 전송 함수는 데이터를 전송 할 때 응용 계층 프래그먼트(Fragment)를 데이터 링크 계층 사이즈의 데이터 유닛(Data Unit)으로 분해하고, 데이터를 수신할 때에는 트랜스포트 세그먼트(Transport Segment)들을 원래의 응용 프래그먼트로 재조립 하는 역할을 한다.

3.3.3 데이터 링크 계층

데이터 링크 계층은 응용 계층의 전송 함수를 담당하는 부 계층과 물리 전송 계층 사이의 인터페이스를 제공한다. 데이터 링크 계층은 인접하는 시스템 간의 데이터 전송 제어 및 회선 상을 유통하는 전송 데이터의 오류를 검출하는 역할을 한다. 데이터가 통신 채널을 통하여 전송될 때 해당 계층에서는 가장 최근의 8 비트짜리 DNP3 특유의 오버헤드 데이터를 추가한다. 이 프로토콜은 통신 채널을 통할 때 옥텟(Octet) 방식 모드에서 사용하기 위해 설계되었고, 여기에 TCP/IP와 UDP/IP를 사용하는 패킷 방식의 네트워크를 통할 때에도 사용할 수 있게 설계되었다. DNP3 데이터 링크 계층은 연결방식에 상관없이 어느 시스템에서도 적합하다. 연결방식은 통화(Dialing), 로그인(Loging in), 또는 목적 장치로의 데이터 전송이 발생하기 전에 통신 채널을 설정하는 것을 요구하는 물리 네트워크를 뜻한다. 본 문서에서는 연결 서비스 요구 조건에 대해서는 기술하지 않는다. 이는 시스템에 종속적이고, DNP3 프로토콜의 필드를 벗어나기 때문이다.

3.4 견고성 테스트

테스트 요구사항을 도출해내는 목적은 구현된 프로토콜 상에서 임베디드 제어 장치의 견고성에 접근하고 공격이 지속되는 과정에서 장치의 제어 기능과 보고 능력을 테스트 하는 것이다. 이때, DUT(Device Under Test)는 테스트가 진행되는 동안 지속적으로 정확히 동작한다는 것을 증명하기 위해 〔EDSA-310〕의 요구사항을 만족해야 한다〔8〕. 견고성 테스트는 세 가지의 개념적인 단계와 테스트 환경 전제조건 단계로 진행된다. 이 세 가지 단계는 내용이 서로 겹칠 수 있다.

첫 번째 개념적 단계는 기준 작동 단계이다. 이 단계에서는 테스트에 사용하기 위해 선택된 DUT 프로토콜 모음(Protocol Suite)이 프로토콜 퍼징(Fuzzing)이나 스트레스 테스트(Stress Test)가 진행되기 전에 적은 하중의 간단한 테스트 케이스에서 적절하게 작동한다는 것을 증명하기 위한 테스트를 수행한다.

두 번째 개념적 단계는 기본 견고성 테스트 단계이다. 이 단계에서는 무작위로 선정된 오류를 포함한 프레임이나, 세그먼트, ASDU(Application Service Data Unit)을 수신하더라도 해로운 영향이 발생하지 않도록 하는 능력을 검토하기 위해 실행한다. 상태 프로토콜(Stateful Protocol)의 경우, 구현된 프로토콜이 상태에 의존적인 메시지에 대해서, 그 메시지가 정확한 순번이나 잘못된 순번으로 도착 하였을 때 어떻게 반응하는지에 대해서도 테스트 하게 된다.

세 번째 개념적 단계는 부하 스트레스 테스트 단계이다. 이 단계에서는 유효한 메시지를 포함한 높은 트래픽 속도에 대한 실행 응답에 대해 검토한다. 상태 프로토콜의 경우, 위와 마찬가지로 구현된 프로토콜이 상태에 의존적인 메시지에 대해서, 그 메시지가 정확한 순번이나 잘못된 순번으로 도착 하였을 때 어떻게 반응하는지에 대해서 테스트 하게 된다.

이러한 테스트는 단일 요소 테스트에서부터 복잡한 부하 스트레스 테스트까지 개별적으로 논리적 단계에 의해 진행되는 것으로 개념화 되어있기는 하지만, 반드시 이러한 순서대로 진행되어야 하는 것은 아니다. 임의의 순서대로 테스트를 진행한다 하더라도 견고성에 대한 정확한 결과를 도출 해 낼 수 있다.

3.4.1 기준 작동 테스트

TD(Test Device)가 견고성 테스트를 시작하기 전에, DUT는 필수적인 서비스들을 유지하는 것을 포함하여 테스트 환경에서 기대된 만큼 작동 할 수 있다는 능력을 입증해야 한다.

3.4.2 기본 견고성 테스트

제어 프로토콜 표준을 분석해서 특정 견고성 테스트의 구역을 구분한다. 이것은 모든 필드 값 범위들과 근본적인 메시지 표현의 결합 값을 식별하는 것을 포함한다. (예를 들면, 하나의 바이트 영역내의 10에서 100까지의 영역에 대해서, 그것의 근본적으로 표현된 결합 값들은 0에서 255이다.) 기본 견고성 테스트는 각각의 결합 값들이 잘 받아들여지는지 또 이와 같은 근접한 값들이 메시지 인코딩 내에 표현되었을 때, 이 결합 값에 대한 인접한 값들이 승인되거나 거절되는지를 테스트 한다. 또한 부호를 지니거나 그렇지 않은 값들을 전달하기 위해 명시된 필드들이 적절하게 구별되고 처리되는지를 테스트한다. 다음은 각 계층 별 메시지 필드 민감성 테스트를 설명한 것이다.

● 응용 계층: 잘못된 메시지들 또는 메시지 시퀀스들에 대한 기본적인 견고성 테스트를 위해서, TD로부터 DUT에게 임의의 헤더 값과 옵션 값으로 유효한 필드와 유효하지 않은 필드를 생성해 테스트를 수행한다. 유효하지 않은 필드로는 응용 계층 객체 헤더(Object Header)의 객체 그룹(Object Group), 객체 변화(Object Variation) 필드 설정 변경 시 연관성 있는 한정자(Qualifier), 범위(Range)값 변경들을 예로 들 수 있다. 이러한 변경들은 반드시 해당 변경이 DUT에게 영향을 줄 수 있는 각 응용 계층 프래그먼트의 필드에 적용되어야 한다.

● 전송 함수 계층: TD는 DUT에게 정확한 형태나 부정확한 형태로 DNP3 메시지를 전송한다. 이 때 DUT의 예상되는 응답의 결과가 DNP3 견고성 테스트의 기본을 형성한다. 잘못된 메시지나 메시지 순번에 대한 기본 견고성 테스트를 위해서, TD에서 DUT로 전송되는 유효한 DNP3 메시지 또는 메시지 순번을 DNP3 메시지의 한 구성요소가 잘못된 값을 가지도록 의도적으로 변경시킨다. 이러한 변경 사항은 DNP3 메시지의 각 필드에 적용되어야 한다. 각각의 DNP3 메시지의 변경된 사항들은 DUT에 영향을 줄 수도 있다.

● 데이터 링크 계층: 정확하거나 그렇지 않은 형태의 데이터 링크 프레임이 TD로부터 DUT에게 보내지고, DUT로부터 예상되는 응답들을 얻는 행위가 DNP3 데이터 링크 계층의 견고성 테스트에 대한 기준을 형성한다. 잘못된 메시지 또는 메시지 시퀀스들에 대한 기본 견고성 테스트를 위해서, TD에서 DUT로 전송되는 데이터 링크 프레임 중에서 변칙적인 프레임에 대한 반응을 테스트하기 위해 임의로 구성이 잘못된 프레임이나 오류를 포함 할 수 있도록 변경을 주어 테스트한다. 이

Table 1. Example-Specific Test Cases (Transport Function Layer)

Test ID	DNP3.Test
Test name	Start of transport segment-series with no FIR bit set
Test description	When no transport segment-series is in progress, a Transport Function of a DUT receives transport segment-series of which the first segment does not have FIR bit set from a Data Link Layer.
Test type	Basic robustness: violation of sequence for segments
Test status	Mandatory
Expected DUT behavior	The DUT checks every bit of FIR field of each segment.
Test object	To probe how a DUT process the transport segments which do not start with FIR bit set.
Test configuration	A TD is connected to the DUT by an underlying the DNP3 Protocol. The TD may monitor for any response from the DUT
Test procedure	A Transport Function of the TD sends transport segment-series of which the first segment does not have FIR bit set to a data link layer.
Expected DUT response	When no transport segment-series is in progress, any transport segment received without the FIR bit set shall be discarded.
Results	Pass or fail

러한 변경들은 반드시 해당 변경이 DUT에게 영향을 줄 수 있는 각 데이터 링크 계층의 프레임의 필드에 적용되어야 한다.

3.4.3 부하 스트레스 테스트

부하 스트레스 테스트는 유효한 메시지 트래픽 전송에 대한 테스트로, 두 가지 단계로 구성된다.

1단계 - 유효한 메시지 트래픽은 DUT 벤더가 지정한 포화(Saturation) 속도 임계치보다 낮은 선에서 높은 속도로 전송한다. 즉 기기의 속도 제한을 이용해 부하 실험을 한다.

2단계 - 유효한 메시지 트래픽은 자동으로 조정된 링크 속도 까지(Full Auto-negotiated Link Rate)전송한다. (예를 들어 어떤 종류의 오작동 또는 공격을 시뮬레이션 했을 때) 즉 네트워크 최대속도를 이용해 부하실험을 한다.

프로토콜 구현에 대한 공격은 다음과 같다.

● 변종 메시지를 이용한 반복적 탐사 메시지 전송을 이용한 공격

● 공격자가 제어 할 수 있는 도착 시퀀스 그리고 관련된 시간을 포함된 정확한 메시지를 이용한 공격

● 앞의 두 공격을 결합한 공격 (특정 프로토콜 구현상에서의 간과점이나 오류를 이용하는 목적의 공격을 의미)

● 구현 측면에서 고려되지 않는 멀티 계층 간 결합 특성을 활성화시키는 공격

오류(Error) 또는 간과점을 이용한 공격의 일반적인 예로 고의적인 버퍼 오버플로(Overflow)를 들 수 있다. 구현자(Implementer)가 반복을 고려하지 않았을 때, 구현자는 과도한 메시지 또는 필드 크기를 감지하는 것을 무시할 수 있다. 하나의 프로토콜 계층의 구현에 의해 초기 자원할당이 조정 단계로 구동될 때 다중 계층의 프로토콜 스택 내에서 구현 상호작용(Implementation Interactions)이 일어날 수 있다.

기기(Device)는 부하 스트레스 테스트에 영향을 끼치는 높은 트래픽 속도에 대하여 보호 가능하며 장치 벤더에 의해 다음과 같은 요구사항에 따라 문서화되어 있다.

3.4.4 구체적인 테스트 케이스

다음 Table 1.은 DNP3의 각 계층별 구체적인 테스트 케이스의 예시를 보여준다. 구체적인 테스트 케이스는 이 연구의 핵심으로 DNP3에 특화된 요구사항이며 지면상의 문제로 인해 본 논문상에 모두 기입할 수 없으므로 나머지 테스트 케이스에 대해서는 다음의 링크 [9]의 full-paper를 통하여 확인할 수 있다.

IV. 비교 분석

Table 2.는 기존 보안 인증 평가 방법인 Achilles Communication Certification [10]과 ISASecure Certification CRT [8] 와 본 논문에서 제시하는 보안 평가 인증 방법에 대해서 간략한 비교를 보여준다.

Achilles Communication Certification은 중요한 기반구조에서 발견되는 어플리케이션, 장치, 시스템 의 안전한 개발을 위해 주도산업 기준점을 제공한다. 이는 인증 산업 장치의 네트워크 견고성에 접근하여 여러 조건 아래에서 제시된 요구사항을 만족하는지 확인하는 과정으로 설계되었다.

Achilles Communication Certification에서

Table 2. Comparison with the Existing Method

	Achilles Certification	ISASecure Certification CRT	Proposed
Target protocol	Modbus/TCP, DNP3 over IP, ICCP, IEC 6185	Ethernet, ARP, IPv4, ICMPv4, TCP, UDP	DNP3
Specific test cases for DNP3	X	X	O
Requirements	O	O	O

DNP3 프로토콜은 테스트 항목에 존재하지만 구체적인 세부사항에 대한 언급이 부족하다. 평가 및 인증에 대한 요구사항은 존재하지만 테스트 항목의 목록만 간단히 작성되어 있기 때문에 보안성 평가 방법에 대한 제시가 구체적이지 않다 [11].

ISASecure Certification CRT [8]는 Ethernet, ARP, IPv4, ICMPv4, TCP, UDP를 지원하지만 DNP3 같은 전용 프로토콜에 대한 내용이 없으므로 DNP3 만이 가지고 있는 요구사항 및 네트워크 공격을 테스트하기가 어렵다. 이러한 이유로 기존 평가 인증 방법들은 현재 국내 DNP3 프로토콜에 대한 보안 적합성 검증을 수행할 방법론이 전무한 실정이다.

본 논문에서 제안한 보안성 평가 방법은 CRT를 기준으로 각 계층 별 필수 요구사항에 따라 테스트 요구사항을 도출함으로서 국내 DNP3 프로토콜의 견고성 테스트를 하는데 활용이 가능하다.

V. 결 론

본 논문에서는 제어시스템의 개요 및 제어 프로토콜과 보안인증 적용을 위한 제어 프로토콜 세부 사양을 조사하였다. ISASecure에서 제공하는 EDSA-CRT는 Ethernet, ARP, IPv4, UDP, TCP 등 IP 기반의 프로토콜에 대해서만 제한적으로 테스트가 이루어지고 있으며, 제어 프로토콜에 대한 CRT 테스트 전례를 거의 찾아볼 수 없다. 이에 본 논문에서는 여러 제어 프로토콜 중 가장 널리 사용되는 DNP3 프로토콜을 중심으로 CRT 적용을 통해 테스트 요구사항 도출을 목표로 조사를 진행하였다. CRT 테스트 요구사항 도출을 위해서 본 논문에서는 우선적으로 DNP3 프로토콜의 세부 사양 조사를 선행하였다. 그 후 EDSA-CRT 기준에 맞춘 테스트 항목 도출을 실시하였으며, 특히 DNP3의 각 계층 별 헤더 및 필수 요구사항에 따라 테스트 요구사항을 도출하였다.

본 연구에서 도출한 제어시스템의 테스트 요구사항 분석 및 도출 결과는 국내 제어 시스템을 활용하는 기간산업에서 통신 견고성 테스트를 하는데 활용할 수 있을 것이다. 또한, 기간산업 외에 다양한 산업 제어 시스템의 통신 부문 보안성 평가를 위한 기반 자료를 제공할 수 있을 것으로 기대한다. 향후, 이를 기반으로 국내 제어 시스템의 보안성 평가를 통해 보다 안전하고 신뢰성 있는 서비스 제공이 가능할 것으로 기대한다.

References

[1] Seonmun Kwon and Taesik Son, "The vulnerabilities and security present condition of DNP3 protocol in control systems," Conference of the Korea Institute of Information Security and Cryptology, 24(1), pp. 53-58, 2014

[2] Dongsoo Lee and Kwangjo Kim, "Building Small-Scale Testbed for DNP3 Protocol in SCADA system," Journal of The Korea Institute of Information Security and Cryptology, pp. 66-71, 2013

[3] Moonsu Jang, Gunhee Lee, SinKyu Kim, Byung-gil Min, Woo-nyon Kim, and Jungtaek Seo, "Testing Vulnerabilities of DNP3," Journal of Security Engineering, 7(1), pp. 15-28, 2010

[4] Tae-Gyeong Kim, "An Application level security design for DNP3," Journal of the Korea Institute of Electrical Engineers, pp. 362-363, July. 2010

[5] IEEE Power & Energy Society, "IEEE Standard for Electric Power System Communications - Distributed Network Protocol (DNP3)," IEEE, pp. 1-821, 2012

[6] Clarke, Gordon R, Deon Reynders, Edwin Wright, "Practical modern SCADA protocols: DNP3, 60870.5 and related systems," Newnes, 2004

[7] Jeong-Han Yun, Sung-Ho Jeon, Kyoung-Ho Kim, Woo-Nyon Kin, "A Burst-based Whitelist Model for DNP3 Communication in the SCADA System," International Journal of Control and Automation, 21, pp. 56-59, 2013

[8] EDSA-310, Embedded Device Security Assurance - Common requirements for communication robustness testing of IP-based protocol implementations, ISA Security Compliance Institute, 2010

[9] Hoyeol Choi, Daeyeong Kim, Hyungjune

Shin, Changgee Hahn, and Junbeom Hur, "A Study on Introducing Security Certification for Control Systems," https://goo.gl/Zx4Uit

[10] The Achilles Certification Program, https://www.wurldtech.com/certifications/achilles-communications-certification

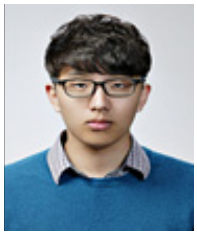
[11] Kim, Jongwan, and Taeshik Shon. "A Study of Security Certification and Accreditation for DNP3 linkage section in EMS/SCADA," Journal of The Korea Institute of Information Security & Cryptology, 25(3), pp. 703-713, 2015

[12] EDSA Certification, http://www.isasecure.org/en-US/Certification/IEC-62443-4-2-EDSA-Certification

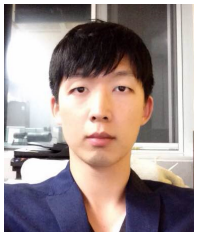
〈저자소개〉

최 호 열 (Hoyeol Choi) 학생회원
2015년 2월: 중앙대학교 컴퓨터공학과 학사 졸업
2015년 2월~현재: 고려대학교 컴퓨터학과 석사과정
〈관심분야〉 정보보호

김 대 영 (Daeyeong Kim) 학생회원
2014년 2월: 대전대학교 컴퓨터공학과 학사 졸업
2014년 3월~현재: 고려대학교 컴퓨터학과 석사과정
〈관심분야〉 클라우드 보안



신 형 준 (Hyungjune Shin) 학생회원
2015년 2월: 중앙대학교 컴퓨터공학부 졸업
2015월 2월~현재: 고려대학교 컴퓨터학과 석사과정
〈관심분야〉 시스템 보안, 클라우드 보안, 빅데이터 보안,



한 창 희 (Changhee Hahn) 학생회원
2014년 2월: 중앙대학교 컴퓨터공학부 학사 졸업
2016년 2월: 중앙대학교 컴퓨터공학과 석사 졸업
2016년 3월~현재: 고려대학교 컴퓨터공학과 박사 과정
〈관심분야〉 클라우드 보안, 응용 암호

허 준 범 (Junbeom Hur) 종신회원
2001년 2월: 고려대학교 컴퓨터공학 졸업
2005년 8월: 한국과학기술원 전산학 석사
2009년 8월: 한국과학기술원 전산학 박사
2009년 9월~2011년 8월: University of Illinois at Urbana-Champaign 박사후 연구원.
2011년 9월~2015년 2월: 중앙대학교 컴퓨터공학부 조교수
2015년 3월~현재: 고려대학교 컴퓨터학과 조교수
〈관심분야〉 클라우드 보안, 빅데이터 보안, 네트워크 보안, 응용 암호학