Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.23, NO.6, Dec. 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.6.1143

전력 제어시스템의 시리얼 기반 DNP통신 취약점에 관한 연구

장 지 웅,[1†] 김 휘 강[2‡]
[1]전력거래소, [2]고려대학교 정보보호대학원

A study on vulnerabilities of serial based DNP in power control fields

Ji Woong Jang,[1†] Huy Kang Kim[2‡]
[1]Korea Power Exchange, [2]Graduate School of Information Security, Korea University

요 약

SCADA(Supervisory Control And Data Acquisition, 원방감시제어시스템) 등 상당수의 전력 제어시스템은 RS232C 시리얼 통신 및 9.6kbps의 저속 아날로그 통신을 기반으로 하는 DNP3.0 프로토콜을 사용하여 전력 현장으로부터 데이터를 취득하고 있다. 이는 아날로그 통신구간에서의 공격불가, 시리얼 방식의 내재적 보안성, Master/Slave 중 Master만이 통신을 시작하는 프로토콜 특성 등으로 인해 안전하다고 알려져 왔다.

본 논문에서는 상용 제어시스템 시뮬레이터를 통해 DNP 통신을 구현한 후, 탭핑(Tapping)을 통해 기밀성, 무결성, 가용성 관점에서 보안실험을 진행하여 취약점을 확인할 수 있었다. 즉 기존에 안전하다고 여겨진 전력 현장으로부터의 데이터 취득에도 적절한 인증 및 암호화 방식을 도입하여야 함을 보일 수 있었다.

DNP User Group을 중심으로 DNP 인증과 암호화에 대한 논의가 시작된 지 7~8년이 경과하였지만 실제 전력계통망에 도입하여 사용하는 곳은 없는 것으로 확인되고 있다. 이러한 이유는 전력시스템의 특수성에 따른 부가적인 보안 요구사항에 기인하는데, 본 논문에서는 이러한 제약을 극복하고 실제 전력계통망에 인증과 암호화 도입을 위한 고려사항을 제시하였다.

ABSTRACT

Power control system like SCADA(Supervisory Control And Data Acquisition) is gathering information using RS232C and low-speed analog communication network. In general, these methods are known as secure because of the secure characteristics from the analog based communication network and serial communication.

In this study, first we build DNP communication environment using commercial power control simulator and find some vulnerabilities by testing from the viewpoint of confidentiality, integrity and availability. Consequently, we see the necessity of a valid method for authentication and data encryption when gathering information, even though that is known as secure so far.

Discussion of needs of DNP authentication and data encryption is started about several years ago, but there is still nowhere applied that on real environment because the current methods can not fully meet the security requirements of the real environment. This paper suggests a solution to the vulnerabilities, and propose some considerations for enhancing power control system's security level by applying DNP authentication and data encryption.

Keywords: DNP vulnerability, Power Control System, SCADA

접수일(2013년 6월 13일), 수정일(1차: 2013년 9월 2일, 2차: 2013년 11월 5일), 게재확정일(2013년 12월 2일)

† 주저자, creative@kpx.or.kr
‡ 교신저자, cenda@korea.ac.kr(Corresponding author)

I. 서 론

전력망은 폐쇄성으로 인해 상대적으로 해킹에 안전하다고 여겨져 왔었으나, 2010년 '스턱스넷' 에 이은 2012년 '플레이머' 출현 등 지속적인 APT (Advanced Persistent Threat)공격으로 전력 제어시스템 또한 실제 사이버 전의 대상이 될 수 있다는 것을 보여주었다.

전력제어시스템은 폐쇄적인 통신망, 전용 OS와 소프트웨어를 사용하는 환경에서 개방형 통신망 및 범용 OS와 소프트웨어를 사용하는 환경으로 변화하고 있다. 이러한 변화는 제어시스템의 편의성을 증대시키는 반면 보안상 취약점을 노출하는 양면적 특성을 가지고 있다. 대다수 전력제어시스템은 외부와의 인터페이스는 전용장비 체계를 유지하고 있지만 제어시스템 내부의 경우 범용 OS와 범용 프로토콜을 수용하여 사용하고 있다.

발·변전소에서 데이터를 취득하는 SCADA (Supervisory Control And Data Acquisition, 원방감시제어시스템), EMS (Energy Management System, 계통운영시스템) 등은 시리얼 기반 DNP 통신 및 9600bps 저속 아날로그 통신망을 활용하고 있다. 시리얼 통신방식의 내재적 보안성 및 Master만 통신을 재개하는 DNP 프로토콜의 특성으로 인해 해당 데이터 취득 구간은 안전성이 유지된다고 믿어왔으며 그에 따라 별도의 네트워크 보안장비가 설치되지 않고 운영되고 있다. 또한 보안장비를 설치하려 해도 DNP 통신구간에 적합하게 개발된 상용 보안장비도 없는 실정이다.

하지만, 최근 4-5년간 시리얼 기반 DNP 환경에서 중간자 공격이 가능함이 확인되었고, DNP 프로토콜 자체의 취약점을 활용한 공격 가능성도 보고되었다.

시리얼기반 DNP 프로토콜 구간의 안전성이 의심된다는 것은 전력 제어시스템의 보안관리에 대단히 큰 의미가 있다. 데이터취득 과정에서의 보안성이 인정된다면 특정 위치의 전력제어시스템 보안관리만 잘 하면 되지만, 보안성이 의심된다면 데이터를 제공하는 전국 각지의 발·변전소의 보안관리도 중앙의 전력제어시스템과 동일한 수준으로 수행해야 된다는 의미가 된다.

이에 따라 본 연구에서는 상용 시뮬레이터를 이용한 기밀성, 무결성, 가용성 측면에서 취약점이 존재함을 확인하는 보안실험을 진행하였다. 이는 실제 사용하는 제어시스템의 환경과는 다르지만 제어시스템에 내재되어 있을 수 있는 여러 위협의 가능성을 보인다는 데 큰 의미가 있다.

II. 선행연구

SCADA 보안과 관련한 선행 연구로는 김영진(2009) [3], 강동주(2013)[4]등이 있다.

김영진(2009)의 연구는 제어시스템에서 많이 사용하는 DNP(Distributed Network Protocol), ICCP(Inter-control Center Communication Protocol), Modbus 등의 프로토콜이 무결성이 보장되지 않으므로 일방향 통신기술 등을 적용하는 대책을 제시한 바 있다.

강동주(2013)[4]는 전력 SCADA 시스템의 사이버 위험을 평가하는 정량적 방법론을 제시하였다.

DNP 프로토콜의 취약점과 관련된 선행 연구는 Omar Faruk(2008) [16], 장문수(2010)[8], 김의형(2010)[6], 최문석(2013)[5] 이 있다.

Omar Frank(2008)는 Nessus 취약점 스캐너와 Retina 취약점 스캐너를 이용하여 TCP/IP 기반의 DNP 프로토콜의 취약점을 살펴보았다. 본 논문은 Omar Frank의 연구를 확장하여 시리얼 통신 구간의 취약점을 점검하였으며, 상용 취약점 공격 툴과 연구 목적으로 제작한 공격자 프로그램을 병행 사용하여 실제 전력 현장과 유사한 환경을 구성하였다.

장문수(2010)는 시리얼 기반 DNP 통신을 사용하는 일반적인 제어시스템 구성에서 DigitalBond社가 제시한 DNP3.0 프로토콜 명세서 상의 취약점을 분석하여 가로채기, 방해, 불법수정, 위조 4개의 공격 유형을 분류하고 12개 취약점을 이용한 공격 실험을 수행하였는데 그 중 5개 시나리오가 공격에 활용될 수 있음을 가능함을 보였다. 이는 시리얼 기반 DNP 통신을 사용하는 환경에서도 DNP3.0 프로토콜의 취약점을 활용하여 정보수집, 서비스 거부공격, 제어명령 변조가 일정부분을 가능함을 보인 국내 사례이다.

김의형(2010)은 RS232C 시리얼 기반 DNP 통신 구간에 탭핑 작업을 통해 중간자 공격 환경을 구성하였다. 제어시스템 역할을 하는 PC와 RTU (Remote Terminal Unit, 원격소장치) 역할의 PC 구축하고 RS-232C 시리얼 케이블 연결하여 DNP3.0을 구성하였다. 또한 DNP3.0 Packet Analyzer 및 Generator를 사용하였다. 실험을 통하여 두 통신장치 A, B 사이에서 공격자가 성공적으로 패킷을 도청하고 변조하는 것이 가능함을 보였으며, 해결방안으로는 데이터의 무결성 확보를 위해 메시지 인증과

HMAC을 사용하는 방식을 제안하였다.

최문석(2013)은 DNP 프로토콜의 데이터링크 계층에서의 보안기능을 수행하는 키 구조와 분배방식을 제공하면서 추가되는 데이터량을 최소화하는 보안 솔루션을 제시하였다.

또한 국내 전력IT 업계에서도 연구개발과제를 통해 DNP 암호화를 구현하려는 시도가 있다. 제어시스템과 현장 전력설비와의 통신과정에 데이터 암호화, 인증 및 키분배를 제공하는 프로토콜을 개발·적용하려는 노력이 진행되고 있다. 암호화 및 인증 장비의 성공적인 도입을 위해서 관련분야에서 표준으로 인정될 수 있는 암호모듈 설계의 적용, 기존 전력현장의 장비에 특별한 변경 없이 동작할 수 있는 호환성, 저속 아날로그 통신환경에서도 최소한의 시지연을 발생시키면서 암·복호화를 수행할 수 있어야 한다.

III. 전력제어시스템

3.1. 전력제어시스템의 종류와 계층제어체계

전력분야 제어시스템은 Fig.1.의 개념도로 이해할 수 있다. 전력의 공급과 수요의 균형을 맞추고 전력을 생산과 소비 및 융통을 해결하는 역할을 계통운영시스템(EMS)이 맡고 있다. 전력생산 부분인 발전기를 제어하는 역할은 발전제어시스템(DCS)이 수행한다. 전력융통, 즉 송전부문의 데이터 취득과 감시 및 제어는 원방감시제어시스템(SCADA)이 수행하고 있다. 또한 전력소비 부분인 전력수용가와 관련된 제어는 배전자동화시스템(DAS)이 그 역할을 수행하는 체계이다.

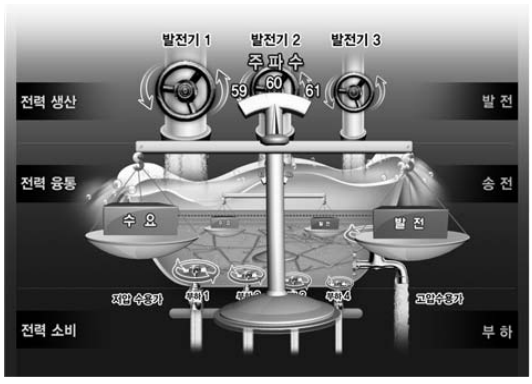

Fig.1. A conceptual diagram of a power control system [18]

3.2. 전력제어시스템의 신규 보안위협

3.2.1 PC형 원격소장치 도입

원격소장치란(RTU) 발·변전소 현장에 설치되어 발전량, 전압, 전류 등의 계측 값과 스위치 등의 닫힘/열림상태 등의 계통상태 자료를 수집하여 중앙의 제어시스템으로 보내주며, 반대로 제어시스템으로부터 제어값을 받아 발·변전소 현장으로 전달하는 장치이다.

일반적으로 RTU는 고유한 OS 및 하드와이어링에 의한 케이블링으로 구성된 전력설비였다. 그러나 최근에는 구성의 편의성 및 경제성으로 인하여 Windows OS를 사용하는 일반 PC를 활용한 PC형(서버형) RTU가 소규모 발전회사를 중심으로 도입되고 있다.

Windows OS는 바이러스, 웜, 트로이목마 등의 악성코드가 존재하고 인터넷 또는 USB 등을 통해 확산이 가능하다. Windows 기반의 PC형 RTU가 악성코드에 감염될 경우 시스템을 제어하지 못할 뿐만 아니라 전체 시스템에 악영향을 줄 수 있다.

Table 1. Conventional RTU vs PC Type RTU

RTU 형식	일 반 형	PC형
자료취득 방법	하드와이어에 의한 연결	범용 통신에 의한 연결
하드웨어	산업용 보드 채용	범용 PC 사용
OS	고유 OS	범용 OS
보안성	외부 접근이 곤란하여 보안성이 우수	외부 접근성이 용이하여 보안성이 취약

3.2.2 원격소장치와 업무망 등의 외부망 연계

폐쇄적인 통신망을 사용하는 전력분야 제어시스템이 인터넷과 같이 개방적인 통신망과 연계되는 형태로 변화하고 있다. 해외의 한 조사에 따르면 폐쇄망으로 운영한다고 주장하는 SCADA 시스템을 표본추출하여 조사한 결과 외부망과의 연계접점이 평균 6개소를 넘는다는 조사가 있었다.

제어망의 자료를 외부에 제공하고자 하는 수요는 항상 있어왔다. 발전분야 제어망의 경우, 자료를 외부에 제공하기 위해서는 발전제어시스템(DCS)이나 원격소장치(RTU)가 연계접점이 될 수 있다. DCS의 경우 주요정보통신기반시설로 지정되어 외부기관의 관리, 감독을 받는 시스템이므로 제어 담당자는 원격

소장치를 활용하여 서비스를 외부에 제공하고 싶은 유인을 가지게 된다.

하지만, 원격소장치와 외부망과의 연계는 그 자체로 보안위협을 증가시키는 행위이다. 다수 사용자가 있는 통신망에 출처가 불분명한 데이터를 유입시킬 가능성을 증가시키기 때문이다.

3.2.3 인터넷 기반 프로토콜 수용 시 보안 위협

신재생발전원의 확산 및 스마트그리드 보급 등 계통운영 환경변화에 따라 전력제어시스템은 현행 시리얼 기반의 전용회선이 아닌 인터넷 기반 통신환경에서 전력설비와의 데이터 연계를 수용할 가능성이 있다. 아날로그 저속 전용회선망을 기반으로 하는 방식은 비용이 많이 들어 데이터 취득개소가 2배, 3배로 증가한다면 감당하기 어려워지고 TCP/IP 기반의 통신방식의 수용 요구가 높아질 것이다. 해외 ISO 상당수가 인터넷 환경으로 발·변전소 데이터를 취득하고 있는 것도 이러한 이유이다.

물론 TCP/IP를 기반으로 한 인터넷의 경우, SSL/TLS 또는 IPSec 같은 보안 프로토콜과 같이 인증 및 암호화를 위해 널리 사용되는 프로토콜이 존재한다. TCP/IP 기반 DNP 통신도 이런 보안 프로토콜을 사용하여 구성할 수도 있고, 기존 보안 프로토콜을 활용한 방식을 일부 변형하여 제어시스템 통신 프로토콜과 잘 호환되도록 정의하여 사용하는 대책도 고려할 수 있다.

하지만, 여러 보안조치에도 불구하고 제어시스템과 인터넷 연결은 불특정 공격의 대상이 된다는 점에서 그 자체로 보안위협을 증가시킨다. 경제성 및 인터넷의 다양한 장점으로 인해 해당 통신방식을 수용할 경우, 인증 및 암호화 방안, 네트워크 및 보안장비 구성, 보안관제 및 기타 개선대책을 충실히 마련하고 다양한 위협의 대응을 위한 충분한 준비를 선행해야 한다.

Table 2. TCP / IP-based authentication and encryption protocols

구성	설명
SSL	SSL은 1993년 웹서버와 브라우저 간의 안전한 통신을 위해 Netscape 사에서 개발하였으며, 세션계층에서 적용되며 FTP, TELNET, HTTP등의 프로토콜의 안전성을 보장
TLS	TLS는 SSL 3.0을 기반으로 업그레이드 시킨 프로토콜로서 SSL3.0이 표준화 된 이후 TLS 프로토콜에 대한 표준화가 시작됨
IPSec	IPSec은 암호화 보안 서비스를 사용하여 IP네트워크를 통한 보안된 개인통신을 보장하는 개방형 표준 프레임 워크로 라우팅하는 컴퓨터에서는 IPSec을 지원할 필요가 없는 특징

프로토콜 측면의 준비로는 DNP protocol over TCP/IP 등 제어시스템 통신 프로토콜에 보안 요구사항을 추가한 프로토콜 개발 또는 SSL/TLS나 IPSec을 지원하는 DNP 프로토콜을 활용을 고려할 수 있다. 이때, 게이트웨이, RTU ARP 캐시 테이블 변조를 이용한 ARP 스푸핑(Spoofing) 공격 등 예상 가능한 취약점에 대한 분석이 이루어져야 한다.

네트워크/보안장비 구성 측면에서도 다양한 요소를 고려하여야 한다. 인터넷에서 유입되는 트래픽은 위험 요소를 가진다는 전제 하에 다계층 심층 보안 방식(Defense-In-Depth)을 구축하여야 한다. 이를 위해 SSL/TLS 및 IPSec을 통한 터널링 구성, 침입방지시스템 등이 활용될 수 있다. 또한 전력망에 대한 공격패턴은 알려지지 않은 기법들이 훨씬 많으므로, 기존에 시그너쳐 기반의 침입탐지시스템에 의존적인 트래픽 감시 체계를 개선하여 행위기반 또는 비정상 행위 학습을 통한 침입탐지시스템을 구축할 필요가 있다.

IV. 보안실험의 설계

4.1. 실험의 범위와 한계

전력제어시스템의 데이터 취득구간의 보안위협을 살펴보기 위해서는 DNP프로토콜 취약점 실험, 중간자공격 및 응답코드 조작 실험, 악성코드 전이 실험 등 다양한 시나리오를 가진 광범위한 보안실험이 필요하다.

하지만 전력제어시스템의 대부분이 주요정보통신기반시설로 지정되어 있어서 실제시스템과 동일한 실험환경을 구축할 수 없고, 취약점이 발견될 가능성이 있는 시나리오도 외부에 공개하기 어려운 제약이 있다.

따라서 본 논문에서는 일반적인 제어시스템의 테스트환경을 구축하고 APT유형의 공격이 아닌 상용 공격툴을 사용한 방법을 설정하여 대부분의 제어시스템에서 공통적으로 노출될 취약점을 보이는 것을 목적으로 실험을 진행하였다.

따라서 본 실험에서 발견된 취약점이 특정 제어시스템의 취약점 발굴 및 개선대책을 제시 용도로 사용은 어려우나 전력제어시스템이 가지는 전반적인 오류에 대한 시사점은 충분히 제공할 수 있다.

4.2. DNP 테스트 베드 구성

DNP3.0 프로토콜 통신 환경을 구현하기 위해서 Fig.2.와 같이 Master/Slave 간 시리얼 통신 환경을 구축하였다.

Fig.2. Configuration of Serial communication environment configuration

RS-232케이블을 두 장비에 연결하여 시리얼 통신 환경을 구축하였다. 연결된 두 장비는 각각 Master와 Slave로 역할로 나누어 동작한다. Master는 Slave로부터 데이터를 계측하고 Slave에 특정한 명령을 내리는 기능을 갖추고 있으며, Slave는 Master가 원하는 데이터를 전송하거나 전달받은 명령을 수행하고 결과를 보고하는 기능을 갖고 있다.

실험에서는 두 대의 PC에 각각 Master, Slave로 지정하였으며 최대한 실제 제어시스템에서 동작하는 계측 메커니즘과 유사하게 시뮬레이션을 하기 위하여 TriangleMicroWork社에서 제공하고 있는 DNP3.0 상용 시뮬레이터인 "Protocol Test Harness" 제품의 Trial 버전을 설치하여 시리얼 기반 DNP3.0 통신 환경을 구축하였다.

Master와 Slave 역할을 수행하는 PC의 하드웨어의 사양은 아래와 같다.

Table 3. H/W spec of master and slave PC

구분	Master	Slave
CPU	Intel core2 Quad CPU Q6600 (2.4GHZ)	Intel core i5 (2.4GHZ)
메모리	6 GB RAM	2 GB RAM
시리얼 통신속도	9,600 bps	9,600 bps
OS	Windows 7 x64	Windows 7 x64

4.3. 탭핑 환경 구성

시뮬레이션 환경에서 공격자의 PC 혹은 노트북이 정상적인 두 통신 주체 사이에 끼어들어 기밀성, 무결성, 가용성을 침해하는 상황을 Fig.3. 과 같이 구성하였다. 두 개의 장비 사이에서 시리얼 탭핑을 통해 공격자가 연결되었다.

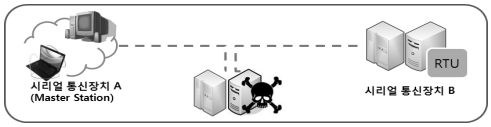

Fig.3. Configuration of Tapping

공격자가 연결된 상황에서는 두 통신 주체가 자신의 존재를 알아채지 못하도록 하기 위하여, 공격자 프로그램은 두 시리얼 통신 장치로부터 전송되는 모든 데이터가 정상적으로 전달되도록 하는 기능이 있어야 한다. 그리고 자신의 공격을 수행하기 위해 오가는 데이터를 파싱하고 이를 변조하는 기능도 필요하다.

본 논문에서 사용한 공격자 프로그램은 전력거래소와 한양대학교가 공동으로 추진 중인 DNP 보안 분야 연구개발과제를 목적으로 제작된 프로그램을 수정, 추가 개발하여 사용하였다.

V. 보안실험 내용 및 결과

5.1. 기밀성 측면의 보안실험

시리얼 기반 DNP 통신과정은 기밀성 측면의 취약점을 가지고 있음을 보이기 간단한 실험을 구성하였다. Triangle MicroWorks社의 Protocol Test harness와 소프트웨어로 Master와 Slave를 구성하고, Slave 측에 상용 스니핑 프로그램인 Wire-Shark을 설치하였다.

WireShark의 패킷 캡쳐기능을 이용하였으며, 실험에 사용된 Slave 에뮬레이터의 포트는 20000번 이므로 WireShark필터 기능을 이용하여 포트 20000으로 들어오는 패킷만 분석하였다.

(1단계) Master에서 DNP 명령어 전송

Master 측에서 "Read Specific DNP3.0 data Type"을 Slave에 전송한다.

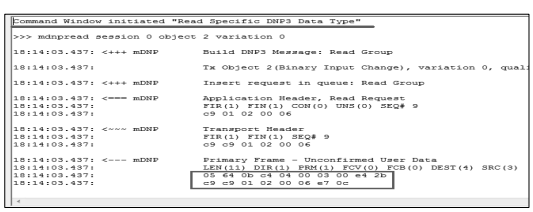

Fig.4. Transfer of DNP command

(2단계) WireShark 에서 DNP 패킷 스니핑

WireShark을 통해 Master에서 보낸 패킷이 스니핑된 것을 확인할 수 있다.

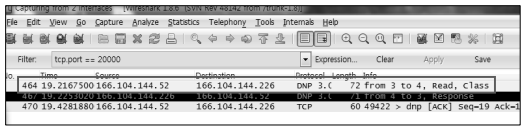

Fig.5. Sniffing result: consistent with the byte stream sent from master

(3단계) Slave에서 response 전송

Slave에서 Master로 응답 코드를 보내면 data link로 전송되는 응답 코드의 바이트 스트림을 확인할 수 있다

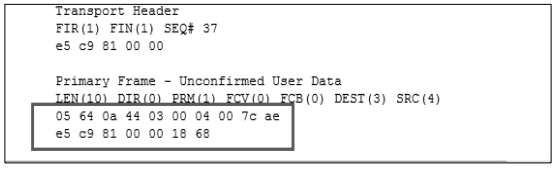

Fig.6. Verify that the command arrived at the Slave

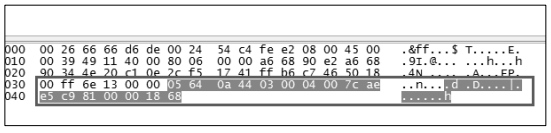

Fig.7. Sniffing snapshots from Wireshark

(4단계) Master에서 response 메시지 확인

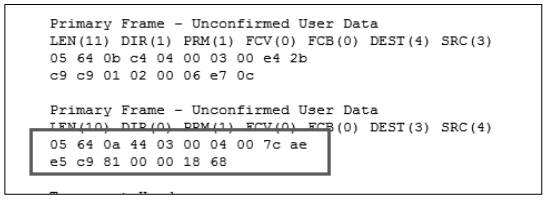

Fig.8. Master messages consistent with the packets sent from slave

위와 같은 간단한 실험을 통해서도 시리얼 기반 DNP 통신방식은 데이터의 기밀성을 쉽게 훼손할 수 있었다. 이는 DNP3.0 프로토콜이 통신구간에서 암호화 되지 않는 평문데이터를 전송하는 데서 기인한 취약점이다.

5.2. 무결성 측면의 보안실험

5.2.1 Master Request 변조 공격

5.2.1.1 변조된 명령 전달

본 실험은 Master가 내린 명령 Request를 중간에서 공격자가 가로채어 공격자가 원하는 명령 Request로 치환하고 전송하는 것이 가능함을 보이는 것이 목적이다.

Master가 보내는 Request는 목적에 따라 여러 종류의 명령을 Slave에게 전달할 수 있다. 공격자는 자신이 원하는 명령으로 Request로 변환하여 전송하여 Slave를 제어 할 수 있게 된다. 실험에서는 이런 공격의 일례로 Slave에 Unsolicited Message를 허용하도록 하는 명령을 전달 한 후, 이 Request를 허용하지 않도록 하는 명령으로 치환하는 공격을 수행한다.

(1단계) Master의 Enable Unsolicited Message 명령 패킷 전송

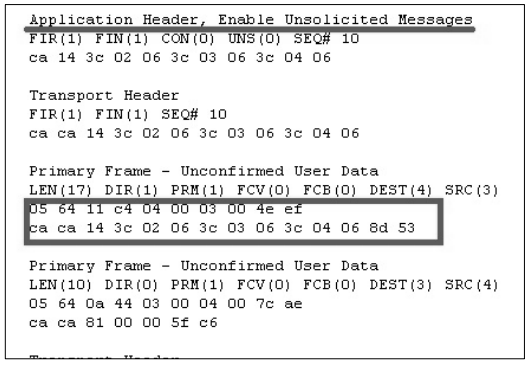

Fig.9. Enable Unsolicited Message

Fig.9.은 Master가 Enable Unsolicited Message 명령 패킷을 전송하는 모습을 보여준다. 해당 명령 패킷에 해당하는 바이트 스트림이 시리얼 케이블을 통해 전송된다. 붉은 밑줄은 Master에 의해 수행되는 명령을 의미하고 붉은 네모 상자안의 바이트 스트림을 해당 명령을 의미하는 패킷을 의미한다.

(2단계) 정상 명령 패킷의 변조와 전송

Fig.10.는 Master가 보낸 Enable Unsolicited Message 명령 패킷을 공격자가 중간에서 가로채어 Disable Unsolicited Message 명령 패킷

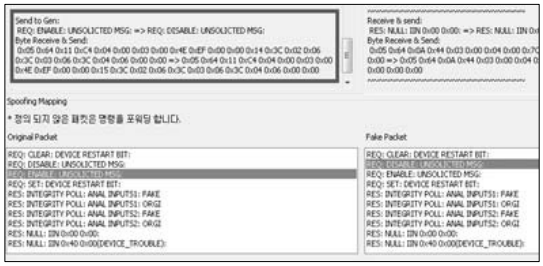

Fig.10. Man in the middle attack : Enable Unsolicited Message→ Disable Unsolicited Message

으로 변조하여 Slave에 전송하는 모습을 ㅇ타낸다. 공격자 프로그램은 미리 정상 패킷과 변조 패킷을 각각 정의하고 대응시켜 패킷을 변조한다.

(3단계) Slave의 변조된 명령 패킷 수신

```
Insert request in queue: Disable Unsolicited Response

Application Header, Response
FIR(1) FIN(1) CON(0) UNS(0) SEQ# 10
ca 81 00 00

Primary Frame - Unconfirmed User Data
LEN(10) DIR(0) PRM(1) FCV(0) FCB(0) DEST(3) SRC(4)
05 64 0a 44 03 00 04 00 7c ae
ca ca 81 00 00 5f c6

Primary Frame - Unconfirmed User Data
LEN(14) DIR(1) PRM(1) FCV(0) FCB(0) DEST(4) SRC(3)
05 64 0e c4 04 00 03 00 6d d3
cb cb 02 50 01 00 07 07 01 89 cf

Application Header, Write Request
FIR(1) FIN(1) CON(0) UNS(0) SEQ# 11
cb 02 50 01 00 07 07 01
```

Fig.11. Slave's acknowledgment of the modulated packet

Fig.11.은 Slave가 중간자 공격으로 인해 변조된 명령 패킷을 수신하는 모습을 나타낸다. Master가 전송한 Enable Unsolicited Message 명령 패킷을 공격자로 인해 Disable Unsolicited Message 명령 패킷으로 변조되었고 이를 Slave가 수신하게 되었다. 붉은 밑줄로 표시된 부분은 수신된 바이트 스트림을 해석하여 Slave가 Disable Unsolicited Message 명령이 전송되었다고 해석한 결과를 나타내며, 붉은 네모 모양 안의 값은 이에 대한 패킷의 바이트 스트림을 나타낸다.

5.2.1.2 잘못된 원격 설비 자료 전송 및 설정

본 실험은 Master가 Slave에게 특정 데이터를 전송하거나 Slave의 특정 설정을 변경할 시 전송 데이터나 설정 값 자체를 변조하여 Slave에 잘못된 값을 전달하여 예기치 못한 원격 설비의 에러가 발생할 가능성을 보이는 실험이다.

해당 공격 시나리오의 한 예로서 Restart IIN (Internal INdication) 값을 잘못된 값으로 변조하여 Slave의 Restart IIN 값을 공격자의 의도대로 임의 변경하는 공격을 실행한다. 참고로 IIN은 Response 메시지의 일부 필드이며 원격 설비의 상태나 에러를 나타낸다. Restart IIN의 경우, 원격 설비가 재시작 되었음을 나타내며 이를 수신한 Master는 수신을 알리며 동시에 원격 설비의 Restart 설정을 Clear하기 위해 Clear Restart IIN 명령을 내린다. Clear Restart IIN은 Slave의 Restart IIN 값은 0으로 설정하는 것을 의미하며 공격자는 0이 아닌 1로 전송 값을 변조하여 보내면 반대로 Restart IIN을 활성화시키는 것이 가능하다.

(1단계) Master의 Restart IIN 값 설정 패킷

```
Command Window initiated "Clear Restart IIN"

>>> mdnpclearrestart session 0

00:37:17.484: <+++ mDNP       Build DNP3 Message:

00:37:17.484:                 Tx Object 80(Internal Indications), variation 1, qu

00:37:17.484: <+++ mDNP       Insert request in queue: (null)

00:37:17.484: <=== mDNP       Application Header, Write Request
00:37:17.484:                 FIR(1) FIN(1) CON(0) UNS(0) SEQ# 11
00:37:17.484:                 cb 02 50 01 00 07 07 00

00:37:17.484: <--- mDNP       Primary Frame - Unconfirmed User Data
00:37:17.484:                 LEN(14) DIR(1) PRM(1) FCV(0) FCB(0) DEST(4) SRC(3)
00:37:17.484:                 05 64 0e c4 04 00 03 00 6d d3
00:37:17.484:                 cb cb 02 50 01 00 07 07 00 d7 f9
```

Fig.12. Master Command : Clear Restart IIN

Fig.12.은 Master가 Slave의 Restart IIN값을 바꾸기 위하여 바꾸기를 희망하는 Restart IIN 값을 패킷에 포함시켜 Clear Restart IIN 명령 패킷을 전송하는 모습이다. 해당 패킷에는 Restart IIN을 0으로 설정하도록 되어있다. 붉은 밑줄은 명령 종류를, 붉은 네모의 값들은 전송되는 패킷의 바이트 스트림을 의미한다.

(2단계) 패킷의 설정 값 변조와 전송

Fig.13. Man-in-the-middle attacker : Restart IIN values: 0x00 → 0x01

Fig.13.은 중간자 공격자가 Master로부터 전송된 패킷을 중간에서 가로채어 Restart IIN 값을 0x00에서 0x01로 변조하여 Slave에게 전송하는 것을 나타내고 있다.

(3단계) Slave의 변조 패킷 수신

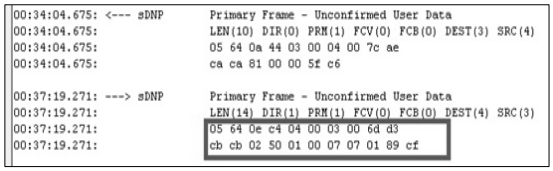

Fig.14. Slave receives the modulated Restart IIN

Fig.14.는 Master로부터 전송되고 중간자 공격자로부터 변조되어 전달된 패킷을 Slave가 수신하는 것을 나타낸다. 수신된 패킷은 붉은 네모 모양안의 바이트 스트림이며 Restart IIN 값이 0x01로 설정되어있음을 알 수 있다. 해당 값 그대로 Slave의 Restart IIN가 설정되어진다.

5.2.2 Slave Response 변조 공격

5.2.2.1 원격 설비의 계측 데이터의 변조 전송

본 실험은 Master의 Request에 의해 전송되는 Slave의 Response를 공격자가 중간에서 임의로 대체하여 전송하는 것이 가능함을 보여준다. Master가 Integrity Data Poll 명령 패킷을 전송하고 그에 따라 Slave가 자신의 계측데이터 값을 전달하는 도중에 중간자가 해당 데이터 값을 자신이 원하는 임의의 값으로 변조하여 Master에게 전달하도록 공격 실험을 진행하였다. 참고로, Integrity Data Poll 명령은 Class123의 모든 이벤트와 Class0의 Static 데이터를 원격 설비로 부터 읽어오는 역할을 한다.

(1단계) Master의 명령 패킷 전송

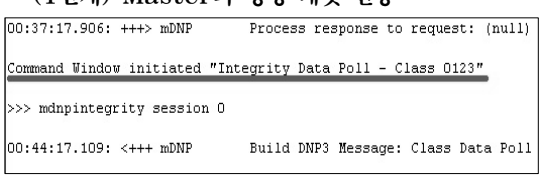

Fig.15. Master Command : Integrity Data Poll

Fig.15.은 Master가 Integrity Data Poll이라고 하는 명령을 Slave에게 전달하는 과정이다.

(2단계) Slave의 계측 데이터 포함 패킷 전송

Fig. 16.은 아날로그 Input 계측 값의 전송을 위해 만들어지고 전송되는 패킷의 바이트 스트림 값이다. 두 개의 붉은 네모안의 바이트 스트림이 Slave가 전송하는 데이터이다.

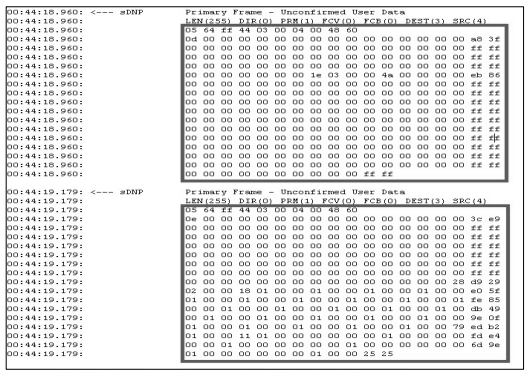

Fig.16. Slave Response : Analog Inputs

(3단계) Slave 패킷의 계측 데이터 조작

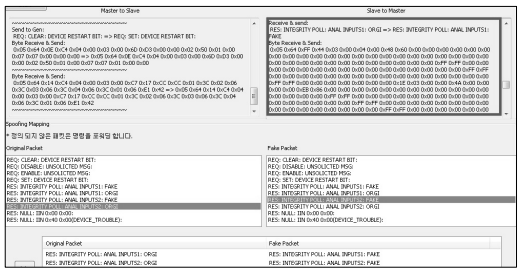

Fig.17. The first packet modulation transfer of Man-in-the-middle-attack tools

Fig.17.은 중간자 공격 프로그램이 Slave가 Master에게 전송하는 계측 데이터를 가로채어 자신이 원하는 값으로 변조한 후 해당 변조 패킷을 Master에게 전송해주는 것을 나타낸다. Slave로부터 전송되는 Analog Input 계측 데이터 패킷은 두 개의 패킷으로 나뉘어 전송되므로 해당 공격 프로그램은 이 두 패킷을 각각 자신이 원하는 패킷으로 변조하여 전송한다. Fig.17]은 첫 번째 패킷을 변조하는 과정이다.

(4단계) Master의 변조된 계측 데이터 수신

Fig.18.은 Master가 중간자 공격 프로그램에 의하여 변조된 Analog Input 데이터 값을 수신한 결과를 나타낸다. Slave가 전송한 Analog Input 데

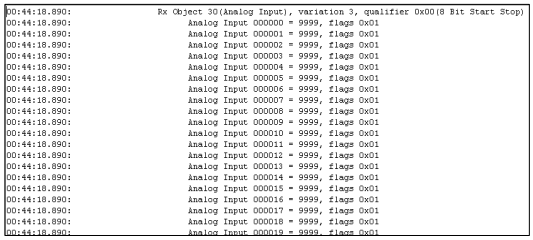

Fig.18. Successful reception of modulated data,

이터 값은 0이었으나 중간자 공격에 의해 9999로 변조되어 Master에 전달되었다. Fig. 18]은 변조된 패킷이 수신된 모습을 나타내고 있다.

수신된 데이터는 Fig.16.에서 보낸 데이터와 동일한 데이터가 Mater에서 수신되었음을 확인할 수 있다.

5.2.2.2 잘못된 원격 설비의 현재 상태 및 에러 발생 유무 정보 전송

본 실험은 Slave의 상태를 나타내는 Response의 IIN(Internal INdication) 플래그를 중간에서 공격자가 변조하여 원격 설비의 상태를 Master가 잘못 이해하도록 유도하는 것이 가능함을 보여준다.

IIN 플래그는 Internal Indication Bit의 약자이며 2바이트의 크기로, 기기 결함, Class 0/1/2/3 데이터의 사용 가능 여부, 시간의 동기화 필요 여부, 그리고 통신 상 발생한 에러들에 대한 내용을 나타내는 역할을 한다. 이 플래그는 Slave가 전송하는 모든 Response 패킷에 포함되어 있어 항상 Master가 IIN을 확인할 수 있도록 한다. 실험에서는 아무런 이상이 없는 상태를 의미하는 IIN 값을 중간자 공격 프로그램으로 기기 불량(DEVICE TROUBLE)을 의미하는 IIN 값으로 변조하여 Master가 Slave의 상태를 오인하도록 한다.

(1단계) Slave의 Response 패킷 전송

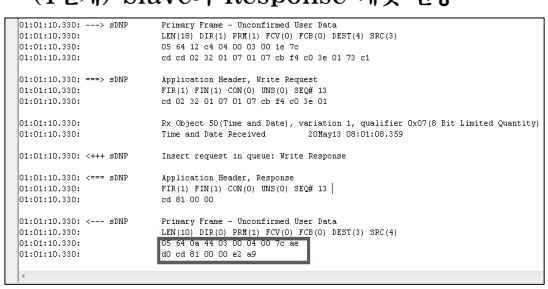

Fig.19. Slave Response : IIN = 0x00Response of Slave packet transmission, IIN = 0x00

Fig.19.은 Slave가 Master의 Time Synchronization 명령을 받고 이를 수행한 뒤 Response 패킷을 Master에게 전송하는 것을 나타낸다. 전송되는 패킷은 IIN 필드를 포함하며 값은 0x00으로 설정되어 정상적인 상태를 나타낸다.

(2단계) Slave의 Response 패킷 변조 및 전송

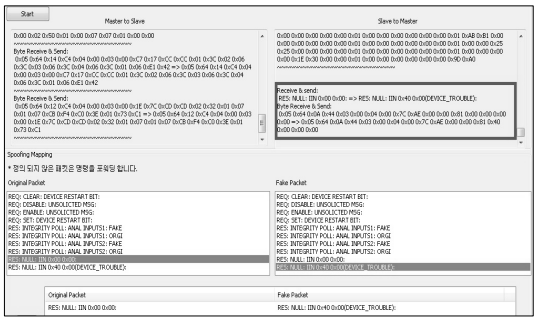

Fig.20. Modulation of IIN Response : 0x00|0x00 → 0x40|00

Fig.20. Slave로부터 전송된 Response 패킷을 중간자 공격프로그램이 수신하여 IIN 값을 변조하고 Master에게 해당 변조 패킷을 전송하는 것을 보여준다. Response의 IIN 필드 값이 정상임을 나타내는 0x00|0x00에서 기기 불량을 의미하는 0x40|0x00로 변경되어 전송된다.

(3단계) Master의 변조된 IIN 값 수신

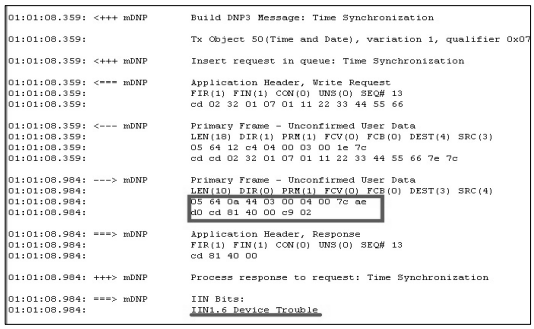

Fig.21. Master의 변조 Response 패킷 수신, IIN = 0x40|0x00

Fig. 21.는 Master가 Slave로부터 변조되어 전송된 Response 패킷을 수신하고 바뀐 IIN 값으로 인하여 Slave의 상태를 기기 불량(Device Trouble)으로 오인하는 모습을 나타내주고 있다. 붉은 네모 모양안의 바이트 스트림은 전송된 변조 패킷 값이

고 붉은 밑줄은 Master가 기기 상태를 불량으로 오인한 것을 보여준다.

5.3. 가용성 측면의 보안실험

Master 혹은 Slave가 입을 수 있는 가용성 측면의 취약점을 실험하였다. Master 장비에 대량의 패킷을 전송하는 DoS 공격을 수행하였다. 그 결과 Master에 해당하는 시뮬레이터에 패킷을 임시 저장하는 큐 버퍼의 용량을 오버플로우 시킬 수 있었으며 이를 통해 잠시 Master는 자신에게 전송되는 다른 DNP 패킷을 처리 하지 못하는 상황이 발생하였다.

(1단계) Slave의 패킷 전송

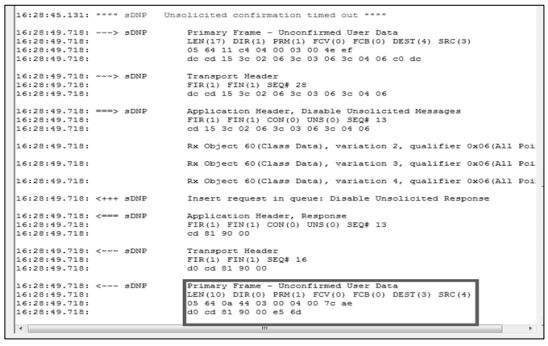

Fig.22. A large amount of meaningless converted to 0x00 packets by an attacker

Fig.22.는 Slave가 Disable Unsolicited Response 패킷을 Master에게 전송하는 모습을 나타낸다. 본 실험에서는 Slave가 전송하는 패킷의 종류나 내용은 의미가 없다. 해당 패킷은 Master에게 전송되기 전에 다량의 패킷으로 변환되어 전송된다.

(2단계) 다량의 패킷을 Master로 전송

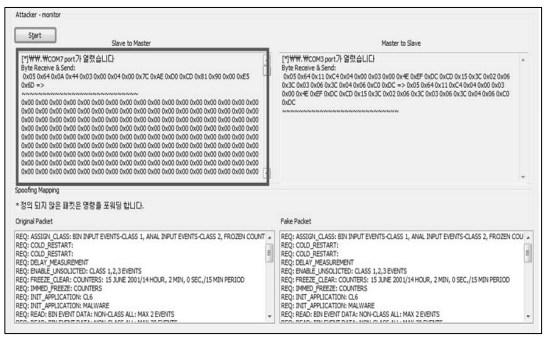

Fig.23. The attacker's 0x00 packet transmission

Fig.23.은 공격자가 Slave로부터 전송되는 패킷을 0x00…0x00의 의미 없는 다수의 패킷으로 변환하여 전송하는 모습을 나타낸다. 공격자는 Master가 자신에게 들어오는 바이트 스트림을 임시 저장하는 큐 버퍼를 모두 채우는 것을 목표로 한다.

(3단계) Master 시뮬레이터 에러 발생

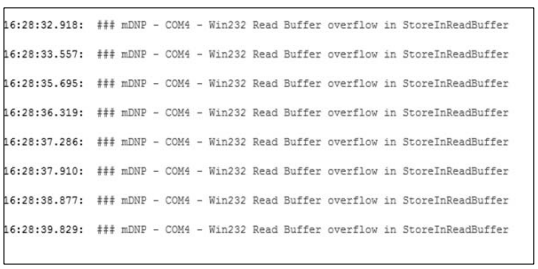

Fig.24. The queue buffer overflow of master

Fig. 24.는 공격자가 Master에 전송한 다수의 0x00…0x00 패킷들로 인하여 Master의 큐 버퍼가 오버플로우 되는 현상을 보여준다. 통신을 담당하는 모든 프로그램들은 내부적으로 큐 버퍼를 이용하여 패킷을 전송받고 처리하는데 이때 패킷들에 대한 유효성 검사를 통해 의미 없는 패킷을 드랍하거나 길이나 값을 검사하는 일이 수행되어야 한다. 만일 이에 대한 처리가 제대로 되지 않게 되면 본 실험의 결과와 같이 예기치 못한 에러가 발생하여 시스템의 가용성을 해칠 수 있다.

전송속도에 따른 DNP 통신 시뮬레이터의 가용성 침해 가능성을 살펴보았다. Fig.25]는 트래픽 전송속도 별 버퍼오버플로우 발생 시간을 나타낸다. 공격 PC에서 시뮬레이터로 전송하는 트래픽의 속도를 조절하여 버퍼에서의 데이터 처리 속도를 알 수 있었다.

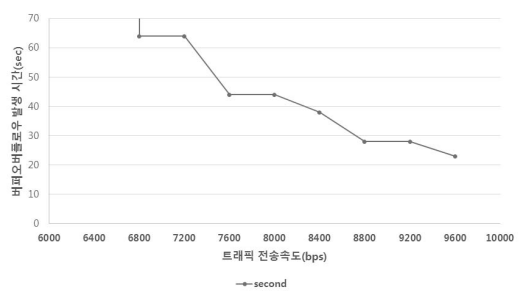

Fig.25. The availability of infringement accrding to transmission rate

시뮬레이터는 대략 6400bps 정도의 데이터 처리속도를 갖고 있어, 만일 시뮬레이터로 6400bps 이상의 트래픽이 전송 되면 내부에 지정된 큐 버퍼에 처리되지 않은 데이터가 쌓이게 되고 이러한 현상이 지속될 시 버퍼오버플로우가 발생할 수 있다. 일반적인 통신 상황이 아니라 악의적 목적의 공격자가 대량의 트래픽을 빠르게 전송할 경우, 이를 대응하기 위해서는 데이터를 처리하는 속도나 고정된 버퍼의 크기를 향상시켜야하며, 별도로 트래픽 검사 모듈을 두어 비정상적인 통신을 사전에 차단할 수 있도록 하는 것이 필요하다.

VI. 실험결과 분석 및 개선대책

6.1. 기밀성 측면의 보안 실험

6.1.1 실험결과 분석

DNP 통신을 수행하는 과정에서 Master 및 Slave가 암호화 과정을 거치지 않아 기밀성 측면의 취약점이 발생하였다. 공격자가 Master-Slave 통신의 전송 패킷을 중간에서 가로챌 수 있을 경우, 패킷에 대한 별도의 복호화 과정이나 무작위공격(Brute Force Attack) 없이도 패킷의 내용을 알 수 있게 된다.

6.1.2 개선대책

DNP 통신 과정에 암·복호화 과정을 추가하는 것이 근본적인 해결책이라 할 수 있다. 암호화구현에는 크게 BITW(Bump-In-The-Wire)와 BITS(Bump-In-The-Wire)방식이 존재한다. BITW는 Master나 Slave 사이에 암호 및 복호화 모듈을 별도로 설치하여 패킷 감청이 불가능하도록 막는 것이다. 이미 오래전에 설계되어 전체 시스템을 재설계하고 구현하는 것이 힘든 경우에 별도의 기기를 추가하여 보안을 적용하는 것을 의미한다. BITS는 프로토콜 스택에 보안 알고리즘을 추가하는 것을 말한다. 이의 경우, 앞서 설명한 BITW와 달리 전체적인 시스템을 다시 구현하여야 한다. 상황에 따라 유용한 보안 메커니즘의 구현 방식을 채택하는 것이 필요하다. 세션 키 교환과 키를 이용한 메시지 암호화가 적용된다면 공격자가 전송되는 패킷을 획득하더라도 패킷을 복호화하지 못하기 때문에 통신의 안전성을 보장할 수 있다.

6.2. 무결성 측면의 보안 실험

6.2.1 실험결과 분석

DNP 통신을 수행하는 과정에서 Master 및 Slave의 인증과정이 없어 무결성 측면의 취약점을 확인할 수 있다. Master와 Slave는 패킷의 변조 여부, 전송자를 식별할 수 없기 때문에 패킷이 공격자로 인해 변조되더라도 이를 알아낼 수 없다. 그리고 공격자는 패킷의 CRC 값과 시퀀스 넘버를 제외하고는 별도의 패킷 조작이 요구되지 않기 때문에 쉽게 Master/Slave 스푸핑을 수행할 수 있었다.

6.2.2 개선대책

DNP 통신 과정에 인증과정을 도입하는 것이 근본적인 해결책이라 할 수 있다. 인증은 Master에서 Slave로의 제어 방향과 Slave에서 Master로의 감시 방향 모두 적용되어야 한다. Challenge Response 인증 방법이나 Aggressive mode를 사용한 인증 방법이 존재한다. Aggressive mode는 Challenge-Response 인증보다 다소 낮은 보안성을 보장하지만 대역폭 사용량을 줄일 수 있는 장점이 있는 인증 메커니즘이다. 두 인증 방법은IEEE 1815-2012 표준에서 권고하고 있는 DNP 보안 메커니즘이다. 이를 활용하여 본 실험과 같은 유형의 공격에 대비할 필요가 있다.

6.3. 가용성 측면의 보안 실험

6.3.1 실험결과 분석

DNP 통신과정에 트래픽 유효성 검사를 수행하지 않아 가용성 측면의 보안실험이 성공할 수 있었다. DNP 통신을 담당하는 어플리케이션에서 시리얼 포트로 전송되는 패킷에 대한 유효성 검사가 이루어지지 않기 때문에 의미 없는 0x00 … 0x00 의 패킷이 일시적으로 임시 버퍼에 저장되고 이로 인해서 버퍼오버플로우가 발생한다. DNP 패킷 이외의 패킷은 전송되지 않도록 하는 유효성 검사가 필요하다.

6.3.2 개선대책

DNP 통신을 위한 어플리케이션은 시리얼 포트로 전송되는 트래픽을 검사하는 절차가 요구된다. 우선

전송된 패킷이 DNP 패킷의 구성과 일치하는지 확인하고, 예외적인 값이 포함되어 있거나 규정된 길이를 초과하는 지 확인하는 유효성 검사가 수행되어야 한다. 그 다음으로 DNP 통신 담당 어플리케이션의 가용성을 침해할 정도의 양과 속도로 전송되는 패킷을 필터링하는 기능이 적용되어야 한다.

VII. 결론 및 향후연구

보안요소를 고려하지 않고 개발된 DNP3.0 프로토콜은 기밀성, 무결성, 가용성 측면에서 취약점이 있음을 확인할 수 있었다. 보안실험에서 발굴된 취약점 해결을 위해서는 무엇보다도 시리얼 기반 DNP 통신구간에 적합한 암호화와 인증방식을 도입하는 것이 중요하다.

DNP 구간에 암호화와 인증 도입에 대한 노력으로는 DNPSec, IEEE1711, DNP Secure Authentication 등이 있다. DNPSec은 기밀성과 무결성 및 인증을 위해 고안되었으며, 기존 DNP3.0의 최소한의 변형만을 가하기 위해 CRC를 사용하였고, 기밀성 보장을 위해 각 Frame별 암호화를 하고 데이터링크 계층에서 동작하도록 고안되었다.

또한 IEEE 1711은 변전소 시리얼 통신의 무결성과 기밀성 보장을 위한 암호 프로토콜로 IEEE 1689와 AGA 12-2 표준을 기반으로 만들어졌다. 특히 이 프로토콜의 암호알고리즘의 선택적 사용이나 요구에 따른 오버헤드 변경 기능은 시스템 구성 시에 유연성을 제공할 수 있다.

DNP 인증을 위한 노력으로 DNP Secure Authentication이 있다. 이는 응용계층에서 동작하며, HMAC을 사용한다.

이렇듯 DNP 인증과 암호화와 관련한 논의의 역사가 7~8년이 되었음에도 실제 전력계통망의 DNP 통신구간에 인증 및 암호화가 도입된 곳은 한 곳도 없는 것으로 파악되고 있다. 이는 전력 제어시스템의 특수성과 추가적인 보안 고려사항 때문이다.

우선 전력시스템은 침해시도가 있는 상황에서도 항상 신뢰성 있게 운영해야 하는 가용성 제약이 있다. 또한 전력시스템은 거대시스템으로 (legacy system) 으로 모든 시스템을 동시에 교체할 수 없는 제약이 있다. 가령, 원격소장치를 장비 수명주기에 맞추어 교체한다면 인증과 암호화 도입에 15년 가량이 소요될 수 있다. 따라서 암호화 및 인증 방식 마련 시 설비의 전체교체가 어려우므로 기존 장비와 호환되면서 일부의 모듈 변경 정도로 도입 가능한 방식을 마련하여야 한다. 이것이 전력계통망에 암호화와 인증도입 시 제약으로 작용하는 특수성이다.

또한 96,000bps 저속 전용 회선망을 사용하여 2초 단위 감시 및 제어신호를 실시간 전송하는 전력계통망의 경우 인증과 암호화 과정이 2초 제어주기 안에서 지연 없이 처리해야 한다. 따라서 암호화·복호화 속도, 키 분배 구조 및 관리 오버헤드 등도 추가 고려사항이다.

DNP 보안을 전력현장에 적용하는데 있어서 다행스러운 점은 전력 제어시스템의 핵심적인 역할을 하는 계통운영시스템이 국내기술에 의해 제작되어 2014년 말부터 사용할 수 있게 준비되고 있다는 점이다. 계통운영시스템 국내 연구진에 의해 개발되어 보안 요구사항 수용하기 위한 변경 및 추가개발이 용이한 상황이다.

따라서 향후 연구에서는 전력계통망의 특수성과 추가적인 보안 고려사항을 반영할 수 있는 인증 및 암호화 체계를 개발하고 실 계통에 적용하는 노력을 지속적으로 하여야 할 것이다.

References

[1] Korea Power Exchange, "A study on information security policy of Smart Grid," SEP. 2012

[2] National Cyber Security Center, "Security Guidelines for Electronic Control System," APR. 2010

[3] Young-Jin Kim, Jung-Hyun Lee and Jong-In Lim, "A Study on the Secure Plan of Security in SCADA Systems," Jonornal of The Korea Institute of information Security & Cryptology, 19(6) pp. 145-153, Dec. 2009

[4] Dong-joo Kang, Jong-joo Lee, Young Lee, Im-sop Lee and Huy-kang Kim, "Quantitative Methodology to Assess Cyber Security Risks of SCADA system in Electric Power Industry," Jonornal of The Korea Institute of information Security & Cryptology 23(3) pp.445-457, JUN. 2013

[5] Moon-suk Choi, Chung-hyo Kim,

You-seok Lim, Seong-ho Ju, Yong-hun Lim and Kyung-seok, Jeon, "Development of Low Latency Secure Communication Device for Legacy SCADA," Jonornal of The Korea Institute of information Security & Cryptology 23(2), pp.339-346, APR. 2013

〔6〕 Ui-Hyong Kim, Kyong-Shik Kim, Kwang-Hyuk Lim and Eul-Gyu Im, "Study on Possibility of Man-in-the-Middle Attacks in RS-232C Serial Communication of the SCADA Systems for Power Systems" , Journal of Security Engineering, 7(4), pp 295-310, AUG. 2010

〔7〕 Yun Ho Shin, Gwang Hyuk Lim and Eul Gyu Im, "A Research on the Possibility of ARP Spoofing Attack in SCADA System Based on TCP/IP Environment," Jouranl of Information and Security, 9(3), SEP.2009

〔8〕 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), Feb. 2010

〔9〕 Tasik Shon, "EMS-SCADA targeted attacks and countermeasures," Presentation for Smartgrid Security Workshop 2013, May. 2013

〔10〕 U.S. Department of Energy, "21 Steps to improve Cyber Security of SCADA Networks," JAN. 2007

〔11〕 IEEE Power & Energy Society, "IEEE Standard for Electric Power Systems Communications - Distributed Network Protocol (DNP3)," OCT.2012

〔12〕 Tracy Amaio, Tien Van, "IEEE 1711-2010 Security For Legacy SCADA Protocols" SEQUI.inc, 2011

〔13〕 Grant Gilchrist, "Secure Authentication for DNP3," IEEE 2008

〔14〕 Shapiro, Bratus, Rogers and Smith, "Critical Infrastructure Protection 3 Chap1 Do it yourself scada vulnerability testing with lzfuzz," 2012

〔15〕 Triangle MicroWorks,Inc, "DNP3 Overview," 2002

〔16〕 Omar Faruk "Testing & Exploring Vulnerabilities of the Applications Implementing DNP3 Protocol" Master Thesis, Stockholm, Sweden, 2008

〔17〕 Jeong-Han Yun, Sung-Ho Jeon, Kyoung-Ho Kim, and Woo-Nyon Kim, "A Burst-based Whitelist Model for DNP3 Communication in the SCADA System", Proceedings, The 7th International Conference on Information Security and Assurance, 2013

〔18〕 Korea Power Exchange, "Development of K-EMS," 2009

〈저자소개〉

장 지 웅 (Ji Woong JANG) 정회원
2003년 2월: 한양대학교 전자전기공학부 졸업
2007년 2월: 한양대학교 경제금융대학 석사
2009년 2월: 한양대학교 경제금융대학 박사수료
2013년 8월: 고려대학교 정보보호대학원 석사
2003년 8월~현재: 전력거래소 정보보호팀 차장
〈관심분야〉 제어시스템 보안, 보안경제학

김 휘 강 (Huy Kang Kim) 종신회원
1998년 2월: KAIST 산업경영학 학사
2000년 2월: KAIST 산업공학과 석사
2009년 2월: KAIST 산업및시스템공학과 박사
2004년 5월~2010년 2월: NC소프트 정보보안실장, Technical Director
2010년 3월~현재: 고려대학교 정보보대학원 조교수
〈관심분야〉 온라인게임 보안, 네트워크 보안, 네트워크 포렌직, 침입탐지시스템, 봇넷탐지