제어망 보안을 위한 일방향자료전달시스템의 송수신 에이전트 개발

오영철*, 한미란**, 신용태***, 김종배****

*,**,***,****숭실대학교

E-mail : kjb123@ssu.ac.kr

요 약

최근 외부의 악의적인 공격으로부터 내부의 시스템을 보호하기 위하여 논리적, 물리적으로 망을 분리하고 있다. 하지만 사회공학적 해킹에는 물리적 망 분리도 취약할 수밖에 없다. 이러한 이유로 국가기반시설들을 담당하는 주요 기관들은 좀 더 안전한 네트워크 망을 구성할 필요가 있다. 따라서본 논문에서는 일방향자료전달 시스템을 제안한다. 본 논문에서 제시한 일방향자료전달시스템은 제어시스템으로부터 업무망으로 전달되어지는 정보를 수신하여 처리하고, 업무망의 제어 정보는 송신되지 않도록 구성한다. 이 방식을 통해 어떠한 경우에도 외부로부터 내부의 제어망을 통해 기간시스템에 접근하는 것이 불가능하기 때문에 국가기반시설을 안전하게 보호할 수 있다.

키워드

망분리, 망간자료전달, 망연계, 일방향자료전달 제어시스템, SCADA, 침입차단시스템

Ⅰ. 서 론

최근 폐쇄적으로 운영되는 제어망의 특정 계측정보와 감시정보 등의 데이터를 업무망으로 전송하여 운영관리와 장애 및 재난 등에 대비한 통합 모니터링이 필요하게 되었다. 이를 연계하기 위한 방식으로는 침입차단시스템의 일방향 설정을 통한 연동, 망간 자료전송 방식을 통한 연동 등을 방식을 사용하였으나, 제어시스템에 대한 해킹 위협이 증가하게 되었다. 이러한 보안 취약점에 따라 국가정보원에서는 해킹의 위협으로부터 안전한 제어망 네트워킹을 구성하기 위하여 제어시스템은 물리적 일방형 자료전달 장치 기술을 도입하고자 하고 있다.

본 논문은 기존 제어망 연계 아키테처를 분석하고, 취약점 개선을 위한 방안으로 일방향자료전달을 위한 송수신 에이전트 아키텍처를 설계하여, 보다 안전한 자료 연동 방안을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 현행 망연계 방식의 취약점에 대해 분석하고, 개선방안을 도출한다. 3장에서는 본 논문에서 제시하는 일방향 자료전달 시스템의 에이전트 개발 및 실증결과를 제안한다. 4장에서는 결론 및 향후 연구 과제에 대해 기술한다.

Ⅱ. 관련 연구

제어시스템이 사용하는 대상과 목적에 따라 구조가 다르지만 일반적으로 사용자에게 운용 인터페이스를 제공하는 인터페이스부, 통신 기능을 수행하는 통신부, 실제 데이터를 생성, 제어, 관리하는 단말장치부 등의 요소를 그림처럼 갖는다.[2] 일반적인 제어시스템의 물리적 보안 구성은 외부와 내부 환경으로 구분된다. 물리적으로 외부 환경은 자유롭게 이동가능한 장치를 사용할 수 있는 환경이다. 이에 반해 내부 환경은 이동 가능 장치는 반입이 금지 되어있다. 하지만 소형 메모리 디스크 및 USB 등이 반입되어 보안 상의 취약점이 존재 한다. 일반적인 제어시스템의 구성은 다음 그림[그림1]과 같다. 일반적인 제어망과 업무망의 네트워크는 양방향으로 자료를 전달하는 네트워크 시스템으로 구성되어 있다.

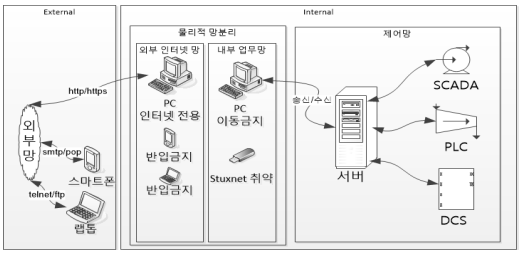

그림 1. 일반적인 제어 시스템 현황

III. 일방향자료전달시스템

일방향자료전달시스템은 망간 기술의 하나로 제어시스템과 업무망의 연계지점의 보안 위협을 제거하기 위하여 물리적 연결선 차단과 자료전송의 신뢰성을 보장하기 위한 연동기법이다. 일방향 자료전달시스템은 업무망에서 제어시스템으로 데이터를 보낼 수 있는 회선을 제거함으로써, 제어망에서 업무망으로 데이터 전송만 가능하고 업무망에서 제어망으로는 어떠한 데이터도 전달될 수 없게하여, 외부로부터의 침투 경로를 원천적으로 차단한다.

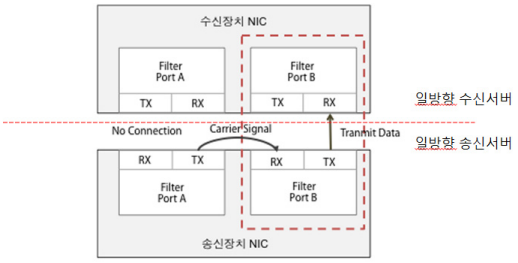

그림 2. 일방향자료전달시스템 광 케이블 개념도

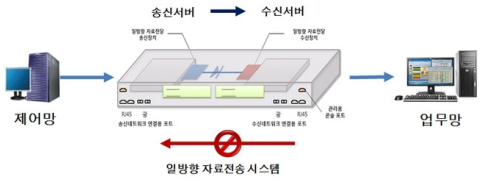

그림 3. 일방향 자료전달 시스템

일방향자료전달시스템은 네트워크 상에서 제어망과 업무망의 연계 부분에 위치하며, 물리적으로 제어망에서 업무망으로의 연결은 허용하나, 반대로 업무망에서 제어망으로의 연결되지 않는다는 보안요소를 지켜야 한다. 또한 전송데이터의 신뢰도를 유지하여야 하며, 기존 운영중인 제어시스템에서의 서비스 변경을 최소화하는 에이젼트 개발이 필요하다. 이러한 중요한 보안요소와 전송데이터의 신뢰성, 서비스의 연속성 보장을 위하여 일방향자료전달시스템은 제어망과 통신을 담당하는 송신서버와 업무망으로 데이터를 전송하는 수신서버의 일체형으로 구성되며, 관리도구와 해당 서비스에 적합한 에이젼트 개발이 필요하다. 송신서버와 수신서버의 일방향 구간은 하나의 광케이블로 구성되어 있다.

IV. 결 론

본 논문에서는 일반적인 제어시스템의 네트워크 구조를 알아보고 침입차단시스템을 사용한 제어시스템 네트워크 문제점을 파악하고 해킹의 위협으로부터 안전한 네트워킹을 구성하기 위하여 제어시스템은 물리적 일방형 자료전달 장치 기술을 설계하였다. 헤더 응답 기반 에이전트와 데이터 조작 응답기반의 에이전트 두 가지 방식의 개발 방안을 제시하고 이에 대한 실증을 통해 보다 보안이 강화된 제어시스템을 구현할 수 있는 방법을 제시하였다.

실제 운용되는 제어시스템 내에는 다양한 양방향 프로토콜에 기반되고 또한 비공개된 프로토콜에 의해 운영되는 서비스가 다수 존재한다.
물리적 일방향 시스템의 현장 적용을 위해서는 단순히 프로토콜이나 서비스의 내용만으로는 적용이 쉽지 않다. 다양한 상황과 환경 그리고 운영방식 등에 대한 고려가 필요하다. 향후에는 본 개발 및 테스트 결과를 바탕으로 데이터베이스 기반 통신 서비스와 같은 다양한 서비스를 수용하며, 10Gb 이상 대용량 자료 전달 서비스를 효율적으로 할 수 있는 시스템 개발 연구를 진행할 것이다.

참고문헌

[1] US.DepartmentofHomelandSecurity,ICS-CERT “Overview ofCyber Vulnerabilities “http://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities

[2] 최명균, 이동범, 곽진, “제어 시스템에 대한 보안정책 동향 및 보안 취약점 분석”, 정보보호학회지, ISSN:1598-3978, Vol21, Issue 5, 08.2011

[3] NIST SP800-82 Guide to Industrial Control Systems(ICS) Security

[4] 김경호, 장엽, 김희민, 윤정한, 김우년, “제어망 특성을 반영한 물리적 일방향 자료전달 시스템 설계 “, 정보과학회논문지:정보통신, Vol.40, No.2, 2013