정 보 보 호 학 회 지
제27권 제2호, 2017. 4

OTP(One-Time Password)를 활용한 산업제어시스템 제어명령 무결성 보호방안

이 찬 영*, 정 만 현**, 민 병 길***

요 약

제어시스템(발전시설, 전력시설, 교통시설 등)은 생산성, 가용성, 안전성을 목적으로 다양한 제어기기들로 구성되며, 물리적으로 다양한 위치에 분산되어 운영되고 있다. 그리고 안전성과 가용성을 유지하기 위해 시스템 도입 시 기존 시스템에 영향을 미치지 않는지 검증을 수행 후 시스템을 도입한다. 이러한 이유로 신규 기술의 도입이나, 기기의 변경이 자유롭지 않다. 이와 같은 제어시스템의 특성으로 인해 현재 증가되고 있는 제어시스템 사이버공격에 대한 보안대책 또는 기술들의 적용이 쉽지 않아 사이버공격에 취약한 상황이다. 제어시스템은 상위 시스템의 제어 명령을 통해 하위 제어기기 또는 필드기기를 제어하는 형태로 제어 명령의 무결성 유지가 특히 중요하다. 이는 곧 제어시스템에 환경에 접근한 공격자가 인가되지 않은 장비를 제어시스템에 연결하고, 악성 제어명령을 전송하게 된다면 제어기기는 이를 인지하지 못하고 정지되거나 오작동을 유발 할 수 있다는 것을 의미한다.

본 논문에서는 제어시스템 내 제어명령의 무결성 유지를 위해 임베디드 Add-on 단말을 통해 OTP 값을 생성, 전달, 검증하는 방안을 제안한다. 해당 방안은 상위노드와 하위노드 사이에 Add-on 장치를 두어 상위노드에서 제어명령 발생 시, 제어명령에 OTP값을 통해 캡슐화하고 하위노드로 전달한다. Add-on 장비는 일반 IT시스템과 상이한 제어시스템의 특성에 맞게 고안되었으며 제어시스템 내에 발생되는 제어명령 위변조, 제어명령 재사용 공격 등을 차단 할 수 있다.

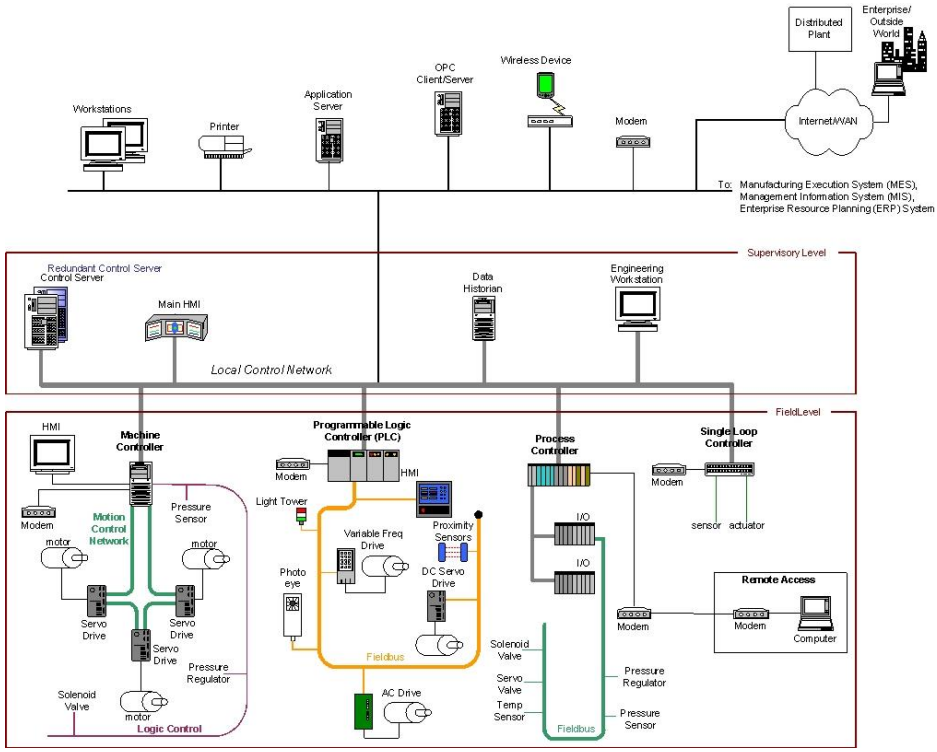
Ⅰ. 서 론

전 세계적으로 제어시스템에 대한 사이버 사고가 증가하고 있다. 2010년 제어시스템 전용 악성프로그램인 Stuxnet 발견을 시작으로 Duqu, Blackenergy와 같은 제어시스템 전용 악성코드들이 발견되고 있다[1][2]. 이러한 악성코드는 해커 개개인이 아닌 일련의 조직적 또는 국가적 차원으로 제작되었음이 분석가들로 인해 밝혀진 바 있다. 그리고 2016년 Blackhat에서 일반 상용 OS를 쓰는 컴퓨터가 아닌 제어시스템에서 사용되는 제어기기인 PLC에 대한 악성코드를 제작하여 발표한 바 있다[3]. 이는 보다 복잡하고 다양한 제어시스템을 대상으로 한 악성코드가 지속적으로 나올 수 있음을 의미한다.

본 논문에서는 공격자로부터 제어기기 운영을 위해 전달되는 제어명령에 대한 위변조 또는 허가되지 않은 기기로 부터 전송되는 제어명령을 차단하면서 기존 시스템에 영향을 최소화 할 수 있는 제어명령 무결성 보호 방안을 제안한다. 제안 방안은 제어시스템의 상위 노드에서 제어명령 전달 시 상위노드 혹은 Add-on 장치에서 OTP(One-Time Password)를 생성하고 이를 통해 제어명령을 캡슐화하여 하위노드에 전달한다. 그리고 전달된 상위노드의 OTP값과 하위 Add-on 장치 내부에서 생성된 OTP 값이 불일치하게 되면 문제 상황으로 인지, 문제 상황에 대해 주변 및 운전원에게 전달하는 구조이다. 이 때 제어시스템의 가용성에 대한 영향을 최소화하기 위해 Add-on방식의 임베디드 단말을 활용하여 OTP값을 생성, 검증, 전달하는 기능들을 수행하고 별도의 검증 서버를 설치하지 않는다.

본 논문은 2장에서 제어시스템의 특성과 제어명령 무결성과 관련된 배경들을 서술하고 3장에서는 제어명령 무결성 강화 방안에 대한 상세한 동작 방식에 대해 다루며, 4장에서 결론을 맺는다.

* 한국전자통신연구원 부설연구소(parfait@nsr.re.kr)
** 한국전자통신연구원 부설연구소(manhyun@nsr.re.kr)
*** 한국전자통신연구원 부설연구소(bgmin@nsr.re.kr)



〔그림 1〕 NIST SP 800-82 내 제어시스템 개괄도

Ⅱ. 배경설명

이 논문에서는 일반적인 IT시스템이 아닌 제어시스템의 보안성 향상에 대한 기술을 다룬다. 이를 위해 아래와 같은 제어시스템의 특징을 인지하여야 한다.

2.1. 제어시스템 특성

제어시스템은 일반적인 정보시스템과는 달리 [그림 2]처럼 다양한 제조사, OS, 통신방법, 펌웨어 버전들로 구성된 기기들로 구성되어 있다[4]. 이러한 제어시스템 고유의 특성들로 인해 OS나 전용 프로그램들에 일괄적으로 패치를 적용하기 어려우며, 제로데이나 원데이 취약점에 노출되기 쉽다. 다양한 기기로 구성된 제어시스템은 정보시스템으로 구성된(IT) 환경에 이용되는 방식인 NAC(Network Access Control)과 같은 Agent를 이용한 상시 감시 및 로그 전달 기술의 도입이 힘들다. 왜냐하면 제어시스템 내 사용되는 제어기기들의 운영체제는 일반적인 범용 운영체제(Linux, Windows) 뿐 아니라 RTOS (Real-Time Operation System) 또는 제조사 펌웨어로 구성되어 있어 일괄적인 Agent 설치가 어렵고, Agent를 설치하더라도 그 설치가 제어시스템의 가용성에 영향을 미치지 않는다는 보장이 없기 때문이다. 이러한 점들 때문에 별도의 보안관리를 목적으로 한 프로그램이나 백신은 물론 패치관리를 위한 PMS(Patch Management System) 등의 보안 기술 또한 적용이 어렵다.

제어시스템은 보안에 있어 중요한 3요소 가용성, 무결성, 기밀성 중 가용성을 제일 우선시한다. 가용성이 중요한 이유는 다음과 같다. 첫째, 제어시스템은 시스템 전체가 고장으로 인해 정지되거나 오동작 할 때를 제외하고 그 동작을 임의로 정지하지 않는다. 만일 제어시스템이 정지하게 되면 매시간 어마어마한 금전적 손실은 물론 다수의 사람들에게 불편을 주기 때문이다. 일례로 최근의 BlackEnergy 사고의 경우 발전소의 정지로 인해 약 3시간 동안 8만 명에 달하는 사람들이 전기를 사용하지 못하였다[5]. 둘째, 제어시스템은 한번 설치, 구동되면 그 시스템을 변경하지 않는다. 제어시스템을 구축할 때 사용되는 기기들은 구성 변화 없이10년 이상의 사용을 목적으로 선택되고 운영된다. 만일 일련의 이유

로 기기변경이 필요한 시점이 오면 사전에 그 변동사항이 적용되었을 때 끼치는 영향을 제어시스템 전체를 대상으로 재조사하고 도입한다. 임의로 추가한 기기가 제어시스템 오작동을 유발하면 치명적이기 때문에 제어시스템은 처음 설계되고 운영하던 상태에서 단순 편의를 이유로 추가 기기를 도입하거나 변경하는 데에 매우 보수적이다.

2.2. 사이버공격으로 인한 제어명령 위변조

제어시스템은 컴퓨터, 서버, 네트워크 장비들로 구성된 일반 IT시스템과는 달리 IT시스템의 장비들을 포함한 수많은 현장기기들과 제어기기로 구성되어 그 규모가 방대하다. 또한 운전원들이 작업하는 공간과 현장기기 간의 거리가 길어 장거리 통신 케이블 사용이 필요하다. 이러한 특성으로 외부 또는 내부자가 인가되지 않은 기기를 반입하거나 제어시스템 내부에 직접 연결할 수 있는 취약점이 발생 할 수 있다[6]. 해당 취약점을 예방하기 위해 CCTV 등을 이용한 시설 내 물리적 감시, 보안스티커 부착, 포트봉인 등의 방안을 사용할 수 있다. 하지만 실시간 현황파악 및 전 시스템에 적용이 힘들며 이로 인해 공격자의 공격 여부를 뒤늦게 파악할 가능성이 존재한다.

제어시스템 내부에 공격자가 접근하거나 임의의 기기를 연결할 수 있다면 제어네트워크에 스니핑, 스푸핑 등을 통해 제어명령을 위변조하거나 패킷 재사용 공격 등을 통해 제어시스템에 악영향을 미칠 수 있을 것이다.

2.3. 제어명령 무결성 확인 방법

기존 제어시스템에선 생성, 전달되는 패킷들의 무결성을 유지하기 위해 패킷의 헤더와 패킷 내부 데이터를 통해 무결성을 확인하고 있다. 패킷 헤더를 활용하는 경우로는 IP주소, 전송시간 등을 확인하는 방법이 있다. 만일 수신된 패킷의 송신자 IP주소가 사전에 등록된 주소가 아니거나 동기화된 시각에 어긋난 패킷이 수신된 경우에 이를 공격 혹은 이상으로 간주하고 관련 상황을 운전원에게 전달할 수 있다. 하지만 해당 방법은 공격자가 스니핑을 통해 패킷의 추이를 분석하여 패킷위변조 공격을 통해 우회할 수 있다. 패킷 내부 데이터를 활용하는 경우에는 데이터 내에 canary나 checksum 등을 포함시켜 전달하는 방식을 사용한다. 만일 수신된 패킷의 데이터에 존재하여야할 값이나 패킷의 checksum이 불일치할 경우 공격상황이 발생한 것으로 판단, 운전원에게 전달한다[7]. 이 보안 메커니즘은 헤더를 활용하는 방식보단 복잡하나 결국 공격자가 스니핑을 수행하여 그 규칙성을 파악할 수 있으며 Scapy[8] 등을 이용한 패킷 재사용 공격을 통해 관련 보안 메커니즘을 우회할 수 있다.

위에 언급된 기존 제어시스템에서 사용되고 있는 무결성 유지 방안들은 공격자가 제어시스템 내부에 접근하게 된다면 통신 프로토콜을 파악하고 이를 이용해 제어명령을 생성, 전달하게 되며 제어기기는 이에 대한 무결성을 판단할 수 없다는 공통적인 취약점이 존재한다. 이를 보완하기 위해 기존 IT시스템에서 사용하는 암호화 방안을 활용할 수 있는데, 이를 적용하기 위해서는 제어시스템의 특성을 고려하여야 한다, 일례로 개인키/공개키 방식의 경우 복호화에 시간이 많이 소요됨은 물론 암호를 사용하는 모든 장비들과 연결되어 암호키를 관리하는 CA(Certificated Authority)가 필요하다. 이는 곧 제어기기에 연결할 수 있는 새로운 접점이 될 수 있어 해당 방식은 사용할 수 없다. 그래서 본 논문에서는 2장의 배경정보들을 기반으로 제어시스템의 특징을 고려한 제어명령 무결성 보장을 위한 필수 요구사항을 다음과 같이 정리하였다.

- 다양한 OS, 통신환경에도 적용 가능한 기술
- 제어시스템의 변경을 최소화하는 기술
- 제어명령의 위변조 및 패킷 재사용 공격을 방지하는 기술

Ⅲ. 제안 방법

2장의 제어명령 무결성 보장 요구사항에 따라 본 논문에서는 제어시스템의 가용성을 확보하고 시스템의 변경을 최소화하며 다양한 환경에서도 운영 가능한 데이터 위변조와 재사용 공격을 방지할 수 있는 Add-on 형태의 장비를 제안하고, 장비에 적용한 암호화 방식은 상대적으로 속도가 빠르고 키 관리가 용이한 대칭키의 한 방식인 OTP를 적용하는 방안을 제안한다. 본 장에서는 이 논문에서 제시하는 방안에 대한 상세한 동작 방식을 서술한다.

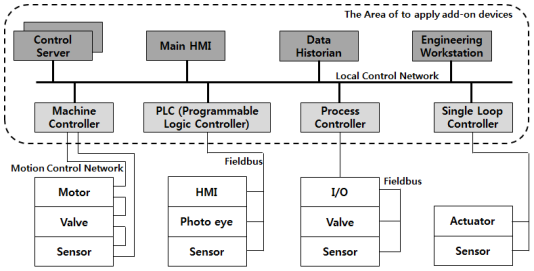
3.1. 시간 동기화 방식 OTP

OTP는 One-Time Password의 줄임말로 일정한 규칙을 피인증자와 인증서버 간에 공유하고, 일정 주기마다 그 값을 변경하는 방식이다[9]. 일반적으로 사용되는 OTP는 질의응답 방식, 이벤트 동기화 방식, 시간 동기화 방식이 존재한다[10][11]. 질의응답 방식의 경우 서버와 클라이언트가 서로 통신 할 수 있는 양방향 통신이 필요하다. 그러나 제어시스템의 경우 중요 시스템과 연결된 구간에는 단방향 통신 장비를 이용하여 사용하고 있으며, 질의응답 방식 절차를 통해 발생 되는 트래픽이 제어시스템 가용성에 영향을 미칠 수도 있다. 이벤트 동기화 방식의 경우 특정 이벤트가 발생할 때마다 OTP의 seed 값을 증가시키는 방식으로 모든 통신구간의 중요도 유무와는 상관없이 반드시 독립적인 seed를 사용해야하고, 이로 인한 연산이 증가하는 단점이 존재한다. 시간 동기화 방식은 피인증자와 인증서버 간에 동일한 시각 seed 값을 사용하여 OTP를 생성하는 방식으로 많은 제어시스템이 GPS나 NTP 서버를 통해 주요 시스템 간 시각을 동기화하고 있어 제어시스템에 활용하기 용이하다.

3.2. OTP 메커니즘 적용 대상

제어시스템 내부에서 발생되는 트래픽은 크게 세 종류의 데이터로 분류할 수 있다. 첫째, 제어시스템 내 운전원들이 제어기기 상태 및 운영 상황 확인을 위해 필요한 제어기기들의 상태정보나 공정값 현황을 전송하는 데이터로 해당 데이터는 하위노드들에서 상위노드로 전달된다. 둘째, 제어시스템 운영 및 제어를 위해 운전원이 제어기기 제어 및 제어시스템 긴급 정지 등의 제어명령 데이터를 전송하는 것으로 해당 데이터는 상위노드에서 하위노드로 전송된다. 마지막으로 제어시스템을 구성하는 제어기기 간의 유기적인 동작을 위한 바인딩 데이터가 있다. 제어시스템 내부에서 발생하는 모든 트래픽의 무결성을 검증하기에는 제어기기들의 연산능력이 부족하여 의도치 않은 지연이 발생할 수 있기에 제어기기를 제어하는 제어 명령에 한해서만 제안된 OTP를 통한 무결성 보호 방안을 적용한다.

[그림 2]는 제어시스템 내 기기들에 제안된 OTP Add-on 장치의 설치 위치를 나타낸다. [그림 2]는

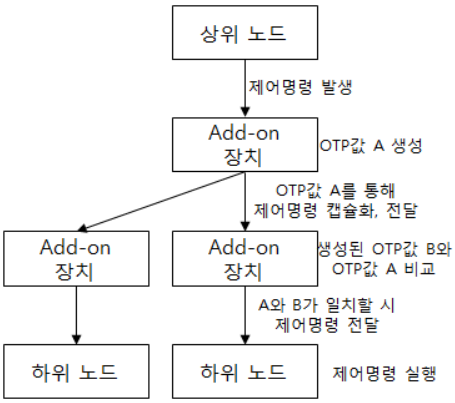


〔그림 2〕 제어시스템 내 Add-on 장치가 적용될 영역의 개괄도

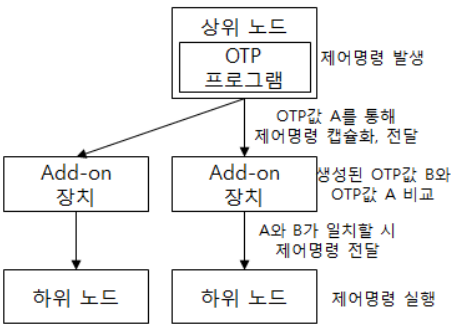
NIST SP 800-82에서 기술한 제어시스템 개괄도를 운전원이 제어하는 기기들 기준으로 간략화한 것으로 제일 상위 노드는 운전원이 제어를 수행하는 Control Server, Main HMI, Engineering Workstation으로 구성된 영역이며, 중간 노드는 상위노드의 제어명령을 실제 동작할 제어기기에 전달하는 Machine Controller, PLC, Process Controller 등으로 구성된 영역이다. 제어명령은 상위 노드 시스템에서 전송되어 중간 노드의 시스템을 거쳐 하위 노드의 제어기기 들로 전송된다. 하위노드는 모터, 밸브, 센서 등의 장치로 중간 노드에서 전기적 신호 받아 동작하고 있고 별도의 IT/제어시스템의 통신트래픽이 발생하지 않기 때문에 제안된 Add-on 장치의 설치가 불필요하다. 제안하는 OTP Add-on 장치는 상위와 중간노드의 연계 구간에 설치한다.

3.3. OTP를 통한 무결성 유지 방안

[그림 3], [그림 4]는 제안된 제어명령 무결성 유지 방안이 어떻게 동작하는지 제어기기를 상위, 하위노드로 구분하여 설명한다. 제어시스템에서 제어명령이 발생하면 [그림 3]의 경우 상위노드와 연결된 Add-on 장치에서 OTP를 생성, 포함하여 하위노드에 전달하고, [그림 4]의 경우 상위노드 내에 OTP 프로그램을 설치하여 제어명령 발생 시 OTP를 생성, 포함하여 하위노드에 전달한다. 만일 공격자가 제어시스템 내 스위치에 임의로 연결하거나 네트워크 탭핑 장비를 이용하여 제어명령을 전달하게 되면 전달된 공격자 제어명령이 하위노드 Add-on 장치에서 임의의 제어명령으로 판단 될 것이다. 이데 대하여 Add-on 장치는 문제 상황으로 인지, 관련 트래픽을 모두 거부하고 주위에 비프음이나 물리적 전기신호로 운전원에게 이상상황을 전달한다. 만일 공격자의 악성행위 없이 상위노드에서 제어명령이



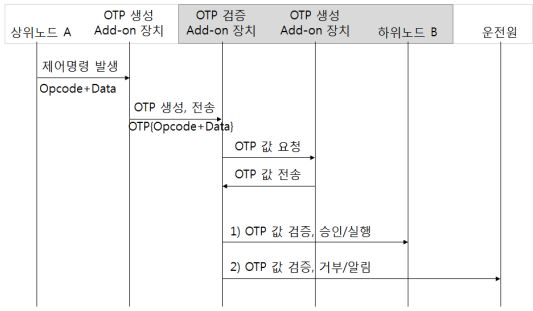
〔그림 3〕 제어명령 발생 시 상위노드, 하위노드 Add-on 장치를 통한 동작 메커니즘



〔그림 4〕 제어명령 발생 시 하위노드 Add-on 장치를 통한 동작 메커니즘

생성되고 하위노드로 전달하게 되면 상위노드 Add-on 장치와 하위노드 Add-on 장치 간의 OTP값이 일치하게 되어 정상적으로 제어명령이 전달, 실행된다.

시퀀스 다이어그램인 [그림 5]는 제안하는 방안 절차를 내타낸다. [그림 5]의 주요노드는 크게 상위노드 A, 하위노드 B, 운전원으로 구성되어 있으며 각각의 노드에는 OTP를 생성하는 Add-on장치 혹은 프로그램이 연결되어 있다. 운전원에 의해 상위노드 A에서 제어명령 생성되어 전달되면 상위노드 A와 연결된 Add-on 장치에서 OTP를 생성, 캡슐화하여 전달된다. 하위노드 B 이전에 설치된 OTP Add-on 장치는 캡슐화 된 제어명령을 수신하고 내부에 생성된 OTP와 외부의 OTP를 비교, 검증한다. 이 때 정상적으로 제어명령이 전달된 경우 하위노드 B로 전달되어 제어명령이 실행되며, 만일 외부 공격으로 인해 패킷이 변조된 경우 지연으로 인하



〔그림 5〕 동작 메커니즘에 대한 시퀀스 다이어그램

여 OTP값이 서로 불일치하여 해당 제어명령을 거부하고 관련 상황을 운전원에게 알린다.

제안된 무결성 보호 방안은 연산 능력이 제한적이거나(하위노드의 임베디드 기기의 경우) 가용성 유지가 매우 중시되는 노드의 경우 별도의 OTP 생성을 담당하는 Add-on 장치를 통신케이블 사이에 연결한다. 이 때 연산능력이 충분하고 가용성에 크게 제약되지 않는 노드(상위, 중간 단계의 상용 OS를 사용하고 있는 경우)에는 내부에 OTP 생성, 교환, 검증을 수행하는 프로그램을 탑재하여도 무방하다.

OTP Add-on 장치는 [표 1]과 같은 기능을 가지며, 필요한 기능들의 경우 시중의 저가, 소형 임베디드 기기로 충분히 구현될 수 있다. 또한 제안된 메커니즘은 별도의 통신방식, 구현방식의 단일화 없이 기존 제어시스템에서 사용하던 다양한 통신 방식을 유지한 채 OTP 정보를 생성, 전달, 검증하므로 제어시스템 구성의 변경이나 가용성에 심각한 영향을 주지 않고 무결성을 만족시킬 수 있다.

제안 방안 동작을 위해 필요한 OTP seed의 개수는 일반적인 대칭키 구조의 암호를 기준으로 전체 노드 n

〔표 1〕 OTP Add-on 장치 주요 기능

번호	기능 이름	설명
1	OTP 생성 모듈	특정 seed를 가지고 일정주기로 새로운 OTP 생성
2	OTP 비교 모듈	외부에서 입력받은 OTP값과 내부에서 생성된 OTP 값 비교
3	ALARM 모듈	OTP 불일치 및 fail-safe 동작과 같은 이상 발생 시 hard-wire로 운전원에 알리거나 비프음 발생
4	fail-safe 기능	이상발생, 전원 문제로 OTP 장치가 꺼지면 자동으로 기존 통신 케이블 연결

에 대하여 n(n-1)/2의 쌍이 필요하다. 앞서 설명한 것처럼 하위의 센서, 모터, 밸브와 같은 기기는 제외하여도 많은 기기를 사용하는 제어시스템의 특성을 고려하면 OTP seed의 개수의 필요치를 줄여야할 것이다. 이를 위해 제안되는 방안은 하나의 상위노드와 다수의 하위노드들 간 동일한 seed를 사용하는 것이다. 즉, 필요한 seed의 총 개수는 제어시스템 내에 존재하는 제어명령을 수신하는 하위 노드들을 제외한 개수와 동일하다. 만일 다수 대 다수의 쌍으로 이루어진 경우에는 관련 노드에 한 해 n(n-1)/2개의 seed를 사용할 수 있으며, 중요도에 따라 seed를 추가하거나 통합할 수도 있다. 이러한 방법을 사용한다면 모든 통신구간에 개별적인 seed를 사용하지 않아 대개 계층구조로 이루어져 있는 제어시스템에서 필요한 Add-on 장치의 개수를 줄일 수 있다. 줄어드는 seed의 개수는 최대 최하위 노드의 개수와 같다.

Ⅳ. 결 론

본 논문은 제어시스템의 무결성 보호를 위해 임베디드 OTP Add-on 장치를 활용하는 방안을 제시하였다. 제어시스템은 일반 IT시스템과는 달리 그 구성방식이 다양하고 가용성 유지를 위해 많은 제약사항이 존재한다. 이 때 내부의 공격자로 인해 임의의 제어명령이 제어시스템 내부에 전송되게 되면 기존 제어시스템의 무결성을 보호하기 위한 방법들이 쉽게 우회되어 제어시스템의 정지 또는 오작동이 유발 될 수 있다. 본 논문은 각 주요 제어기기에 소형 임베디드 Add-on 장치를 사용하여 제어명령이 발생되면 OTP를 통해 캡슐화하고 전달한다. 대상 제어기기의 다른 임베디드 Add-on 장치는 전달받은 제어명령의 OTP 값과 내부 OTP 값을 비교함으로써 제어시스템 내 제어명령의 무결성을 검증할 수 있다.

참 고 문 헌

[1] 최승오, 김우년, “제어시스템 침입탐지 시스템 기술 연구 동향”, 정보보호학회지, 24(5), pp.7-14, 2014

[2] Khan, Rafiullah, et al. "Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid." 4th Int'l Symposium ICS & SCADA Cyber Security Research. BCS. 2016.

[3] R. Spenneberg, M. Br□uggemann, and H. Schwartke, “PLC-blaster: A worm living solely in the PLC“, In Black Hat Asia, Marina Bay Sands, Singapore, 2016

[4] NIST, “Guide to Industrial Control Systems (ICS) Security”, SP 800-82 Revision2, May 2015

[5] ICS-CERT, “ICS-ALERT-14-281-01E – Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)“, 2016

[6] 전덕조, 박동규, “산업 제어시스템 보안관제 모델”, 한국정보기술학회논문지, 13(7), pp 1-16, 2015

[7] Fulton, Temple L., Lothar Trapp, and Heiner Fuchs. "Devices, systems, and methods regarding a PLC system fault." U.S. Patent No. 7,752,511. 6 Jul. 2010.

[8] Scapy Project, “http://www.secdev.org/projects/scapy/“

[9] N. Haller, C. Netz, P. Nesser, M. Straw, A One-Time Password System, RFC 2289, IETF, February 1998

[10] 송성현, 김근옥, “국내외 OTP 표준화 동향”, 정보보호학회지, 22(2), pp. 30-36, 2012

[11] 최동현, 김승주, 원동호, “일회용 패스워드(OTP: One-Time Password) 기술 분석 및 표준화 동향”, 정보보호학회지, 17(3), pp. 12-17, 2007

〈저 자 소 개〉

사 진

이 찬 영 (Chanyoung Lee) 정회원

2012년 2월 : 고려대학교 컴퓨터통신공학부 졸업

2014년 2월 : 고려대학교 컴퓨터·전파통신공학부 석사

2014년 3월～현재 : 한국전자통신연구원 부설연구소 연구원

관심분야 : 제어시스템 보안, 취약점 분석

사 진

정 만 현 (Manhyun Chung)
정회원

2009년 2월 : 고려대학교 정보보호 대학원 석사
2012년 8월 : 고려대학교 정보보호 대학원 박사 수료
2012년 9월~현재 : 한국전자통신연구원 부설연구소 선임 연구원

관심분야 : 제어시스템 보안, 침입탐지 시스템

사 진

민 병 길 (Byunggil Min)
정회원

2002년 2월 : 충북대학교 컴퓨터공학과 학사
2004년 2월 : 포항공과대학교 컴퓨터공학과 석사
2004년 3월~현재 : 한국전자통신연구원 부설연구소 선임연구원

관심분야 : `제어시스템 보안, 침입탐지 시스템, 취약성 분석