정 보 보 호 학 회 지
제24권 제5호, 2014. 10

# 제어시스템 ICCP 프로토콜 사이버 보안 현황

김 성 진*, 손 태 식**

요 약

전력시스템에 IT를 결합한 스마트그리드에 대한 연구가 최근 활발히 진행되고 있다. 스마트그리드 중 전력시스템의 핵심이라 할 수 있는 전력시스템 제어센터 간 통신을 담당하는 것이 ICCP 프로토콜이며, 주로 중앙급전소와 지역급전소간의 전력망 정보들을 교환하는데 사용되고 있다. 이 프로토콜은 단지 전력망의 정보교환 뿐 아니라 전력기기제어 기능도 가지고 있다. ICCP 프로토콜은 TCP/IP 프로토콜을 기반으로 동작하기 때문에 잠재적으로 다양한 형태의 사이버 공격이 가능하다. 또한 이 프로토콜을 사용하는 중앙급전소의 경우 주요 국가기반시설로써 사이버테러에 더욱더 공고한 대응체계를 갖추어야 할 필요가 있다. 현재 ICCP 프로토콜을 사용하는 통신 구간은 일반적으로 외부 네트워크와 분리되어 그 안전성을 담보하고 있지만, 네트워크 분리를 통한 보안성 향상 기법이 체계적인 관리와 함께 수반되지 않으면 인적 취약성이나 새로운 형태의 모바일 기기를 통한 물리적 취약성에 지속적으로 노출 될 수 있는 잠재적 위험을 내포하고 있다. 따라서 이러한 보안 사고의 잠재적 발생 가능성으로 인해 외부네트워크와 분리된 제어센터들도 향후 더욱더 높은 수준의 보안 기술을 적용할 필요성이 강조되고 있다. 본 논문에서는 전력 제어센터 사이에서 사용되고 있는 ICCP 프로토콜의 사이버 보안 현황에 대해 살펴보고 해당 프로토콜의 보안 위험성과 이에 대한 대응방안을 고찰한다.

## Ⅰ. 서 론

최근 전력시스템에 IT를 결합한 스마트그리드에 대한 연구가 활발히 진행되고 있다. 스마트그리드 중 전력시스템의 핵심이라 할 수 있는 전력제어센터 사이의 통신을 담당하는 프로토콜이 ICCP(Inter-Control Center Communication Protocol)이며, 주로 중앙급전소와 지역급전소가 전력망의 정보들을 교환하는데 사용되고 있다. 두 시설은 전력망 전체에 영향을 줄 수 있는 제어명령을 내릴 수 있어 한 번의 보안 사고에도 대규모의 자산피해가 일어 날 수 있다. 특히 중앙급전소의 경우 국가기반시설로써 보안사고 발생 시 국가적인 피해를 야기 할 수 있다. 따라서 중앙급전소와 지역급전소 같은 전력제어센터에 높은 수준의 보안이 필요함은 자명하다.

전통적으로 제어센터는 외부네트워크와 내부 네트워크의 분리가 원칙이다. 현재 국내 전력시스템의 경우 네트워크 분리의 중요성을 인지하여 네트워크 분리가 잘 이루어져 있다. 네트워크 분리를 통해 보안 위협을 원천적으로 제거할 수 있을 것처럼 보이지만, 2010년에 일어난 스턱스넷(Stuxnet)과 같은 APT(Advanced Persistent Threat) 형태의 공격이 발생함에 따라 네트워크 분리는 더 이상 제어시스템의 보안성을 보장하지 못한다. 이와 같이 기존에는 없던 새로운 공격방법의 출현과 2013년 발생한 320 사이버 테러와 같은 국가적인 피해를 야기하는 사이버테러의 발생의 발생은 사이버전 시대의 도래를 암시하며, 국가기반시설에 대한 공고한 대응체계의 필요성을 시사한다. 국가 전력망을 제어하는 전력시스템 제어센터에 높은 수준의 보안성이 필요함은 많은 전문가들이 인지하고 있지만, 제어 센터 간 통신에 사용되는 ICCP에 보안 기법이 적용되지 않는 등 보안 취약성을 내포하고 있다. 본 논문에서는 전력 제어센터 사이 통신에 사용되고 있는 ICCP 프로토콜의 표준화 동향과 알려진 취약성 및 대응방안에 대해 분석하고, 잠재적인 보안 이슈에 대해 논의한다.

2장에서는 ICCP 프로토콜의 개요와 일반적인 특징에 대해 설명하고 3장은 해당 프로토콜이 가지고 있는 보안위험에 대해 기술하였다. 4장에서 ICCP 프로토콜에 보안 기능을 추가한 Secure ICCP에 대해 언급하고

* 아주대학교 컴퓨터공학과 (ksjskyblue@ajou.ac.kr)
** 아주대학교 정보컴퓨터공학과 (tsshon@ajou.ac.kr)

5장에서는 Secure ICCP가 가지고 있는 잠재적인 위험성과 그 대응방안을 논의한다.

## Ⅱ. ICCP

본 장에서는 전력 제어센터 사이 통신에 사용되고 있는 ICCP 프로토콜의 표준화 동향과 구조 및 특징에 대해 다룬다.

### 2.1. ICCP 개요

ICCP는 전력제어센터 간 실시간통신에 사용되는 프로토콜로 한 지점의 상태 정보, 아날로그 정보, 전력 디바이스 제어명령의 전송에 사용된다. 이 프로토콜은 EMS(Energy Management System) 와 SCADA (Supervisory Control and Data Acquisition)의 통신에 주로 사용되고 있다.

ICCP 프로토콜은 EPRI(Electric Power Research Institute)에서 주도한 UCA(Utility Communication Architecture) 프로젝트에서 개발되어 1997년에 IEC (International Electrotechnical Commission) 표준이 되었다. UCA는 전체 전력시스템 전반에 실시간 통신을 포함한 여러 요구사항을 만족시키기 위해 진행된 프로젝트로 ICCP 프로토콜은 제어센터와 발전소, 제어센터와 변전소, 제어센터와 관계기관(Corporate)간의 통신에 사용되었다.[1]

이 프로토콜과 관련된 표준으로는 IEC 60870-6의 파트 503, 505, 702, 802가 존재한다. 503의 경우 서비스와 프로토콜 스택, 505는 유저 가이드, 702는 애플리케이션 서비스, 802는 객체모델에 관해 서술하고 있다.

유저 가이드인 505를 제외한 세 표준들은 새로운 에디션이 2014년 7월에 발간되었다. 새로운 에디션들은 다음과 같은 내용이 변경되었다.

○ 몇 가지의 객체를 추상객체로 변경
○ 추상객체와 관련된 서비스를 추상서비스로 변경
○ 사용되지 않는 Conformance Block의 삭제

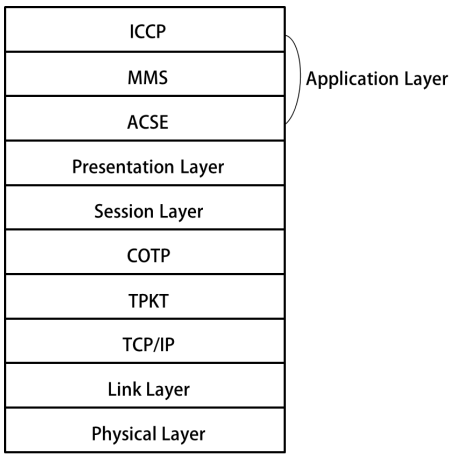
또한 새로운 에디션에는 포함되지 않았지만 전력제어시스템들에 동일한 정보모델을 제공하기 위한 공통정보 모델인 CIM(Common Information Model)을 ICCP 프로토콜에 적용하기 위한 연구가 진행 중에 있다.[2] 이 외에도 MOS(Market Operating System)와 EMS 구간에 ICCP 프로토콜 사용을 위한 연구가 진행되고 있다.

### 2.2. ICCP 프로토콜 스택 및 특징

ICCP 프로토콜은 OSI 7계층의 최상위에 해당하는 애플리케이션 계층의 프로토콜로써 하위에 MMS (Manufactoring Message Specification)와 ACSE (Association Control Service Element)를 사용한다. 그 아래 계층은 표준에서 정의되어 있지 않기 때문에 TCP/IP 계층위에서 MMS를 사용할 때와 마찬가지로 TPKT(Transport Packet)프로토콜과 COTP(Connection Oriented Transport Protocol)프로토콜을 활용한다. 이러한 하위 계층을 포함하여 나타낸 ICCP의 프로토콜 스택은 [그림 1]과 같다.

ICCP 프로토콜은 서비스에 대해 정의하고 이를 MMS의 서비스로 매핑하여 사용하고 있어 MMS의 장점인 뛰어난 상호운용성을 상속받는다. 또한 MMS를 사용하여 통신하기 때문에 서버 - 클라이언트 기반의 통신을 한다. 실제로 RCC(Regional Control Center)가 서버 역할을 수행하고, 중앙 EMS가 클라이언트 역할을 수행하고 있다.[3]

데이터 전송 방법은 One shot, Periodic, Event, Exception으로 총 네 가지 방법이 있다. 이 중 Periodic이 주로 데이터 획득을 위해 자주 사용되고 있다. RCC




〔그림 1〕 ICCP Protocol Stack

가 중앙 EMS로 주기적인(Periodic) 데이터 전송을 하는 경우에 대해 살펴보면, 우선 중앙 EMS에서 RCC로 주기적인 데이터 전송을 요구한다. 전달받은 요구사항에 따라 RCC는 보고 메커니즘을 생성하고, 이후 RCC는 메커니즘에 따라 EMS에서 요청하지 않아도 데이터를 전송한다.

ICCP 프로토콜의 또 다른 특징은 객제 지향 방법론(object oriented methodology)을 사용하는 것이다. 가장 대표적인 객체는 서버 객체이고, 이 객체에 존재하는 Method는 클라이언트의 요청에 대한 응답인 Operation과 서버에서 설정된 메커니즘에 따라 보내는 보고를 나타내는 Action이 있다. 내부에 추가적으로 Association, Data value등 여러 종류의 객체를 가질 수 있다. 추가적으로 가지는 객체들은 서버가 하는 역할에 따라서 다른 종류의 객체들을 가진다.[4,5]

표준에서 서버의 역할에 따라 객체들을 그룹핑하여 Conformance Block을 제공한다. Conformance Block은 특정 서버 유형을 만들기 위해 ICCP 프로토콜에 존재하는 객체들을 그룹핑 한 것으로 총 6개의 Block이 존재한다. 이 중 첫 번째 블록은 기본적인 통신에 대한 부분으로써 모든 ICCP 서버가 필수적으로 가져야 하는 항목이고, 나머지 항목들의 경우 서버가 수행하는 역할에 따라 선택 가능하다. [표 1]은 올해 새롭게 개정된 IEC 표준의 Conformance Block에 대해 설명하였다.

## Ⅲ. ICCP 보안 위협

본 장에서는 앞서 살펴본 ICCP 프로토콜이 지니고 있는 보안요소에 대해 설명한 후 추가적인 보안 기술 적용의 필요성에 대해 살펴본다.

〔표 1〕 ICCP Protocol Conformance Block

| Conformance Block | Supported Feature |
|---|---|
| Block 1 | Basic Service |
| Block 2 | Extended Data Set and Condition Monitoring |
| Block 3 | Blocked Transfer |
| Block 4 | Information Message |
| Block 5 | Device Control |
| Block 6 | Program |

### 3.1. ICCP 접근제어 테이블

ICCP 프로토콜은 통신 대상에 따라 객체별로 접근불가, 읽기, 읽기/쓰기 세 가지의 접근제어를 BLT(Bilateral Table)을 이용하여 실시한다. 클라이언트가 어떠한 데이터에 대한 정보에 접근할 경우 매번 서버는 BLT를 활용하여 접근제어 기능을 수행한다. BLT는 연결이 맺어지는 시점에서 사용되는 객체 및 도메인에 대한 정보와 함께 서버에서 클라이언트로 전송된다. 해당 테이블의 내용은 통신 도중 변경 될 수 있으며, 변경 될 경우 상대측에 바로 전송하도록 되어있다. 이러한 접근제어 기능을 가지고 있음에도 불구하고 ICCP 프로토콜은 취약하다고 알려져 있다. 다음 절에서는 ICCP 보안의 필요성에 대해 설명한다.

### 3.2. 보안 적용의 필요성

일반적인 IT환경과는 달리 전력시스템은 그 특성상 한 번의 사고로도 국가 전체적인 피해가 발생할 수 있기 때문에 높은 수준의 보안 기술 적용이 필요하다. 최근 사이버 공격으로 인해 피해의 빈도수가 급격히 증가하였다. 전력시스템에도 2013년 미국의 한 원자력발전소 네트워크에 슬래머 웜(Slammer worm)의 침투로 인한 안전감시 시스템 정지, 2014년 일본의 핵발전소 악성코드 감염으로 인한 문서 유출 등 전력시설을 대상으로 하는 공격으로 인한 피해들이 발생하고 있다. 피해뿐만 아니라 공격의 횟수도 크게 증가하고 있다. 2013년 미국 시의원은 미국 전력 시스템 중 몇몇이 끊임없는 사이버 공격에 시달리고 있다는 보고서를 제출하였고, ICS-CERT의 발표에 따르면 제어시스템 침해사고는 2011년 140건에서 2013년 257건으로 크게 상승하였다.

대부분의 사이버 공격은 외부 네트워크와의 연결로 인해 발생하기 때문에 원칙적으로 제어센터들은 내부 네트워크와 외부 네트워크를 분리하여 사용하고 있다. 네트워크 분리를 통해 사이버 공격의 위험성을 원천적으로 제거할 수 있어 보이지만, 2010년 이란 원자력발전소 제어시스템을 공격한 스턱스넷은 새로운 종류의 APT공격으로 인해 네트워크 분리가 더 이상 보안성을 제공하지 못한다는 것을 입증하였다. 이후 2011년 듀큐(Duqu), 2012년 플레임(Flame)등 신종 APT 공격은 기반시설을 대상으로 한 공격은 아니었지만, 계속해서 새로운 APT공격들이 발견됨에 따라 스턱스넷 사건이 다

시 상기 되었다.

전력제어센터에서 사용되고 있는 ICCP 프로토콜은 현재 존재하는 보안 기술들의 적용이 되어있지 않다. 하위 계층을 통해 보안 기술을 적용 할 수는 있지만 앞서 언급한데로 하위 계층에 대한 내용이 언급되어 있지 않기 때문에 실제로 많은 전력 회사들은 암호화나 인증과 같은 보안기능 없이 ICCP 프로토콜을 사용하고 있다. 보안 기능이 없는 프로토콜을 사용 될 경우 공격자가 손쉽게 데이터가 위/변조할 수 있어 보안 기술의 적용이 필수적이다.

### 3.3. 보안위협 및 취약점

2000년 초 EPRI는 ICCP 프로토콜을 사용하는 전력제어센터 간 통신에서 일어날 수 있는 보안위협에 대해 정리한 보고서를 발행하였다. 이후 2008년과 2014년에 걸쳐 ICCP 프로토콜 표준이 다시 등장하였지만 해당문제는 주로 ICCP 하위 계층의 문제점이기 때문에 여전히 문제점들을 가지고 있다. 보고서에서 언급된 보안위협은 다음과 같다.[6]

○ MMS로 직접 접근하여 ICCP 프로토콜이 사용하는 데이터에 접근 권한을 취득할 수 있다. 이 방법은 접근제어 테이블을 우회하기 때문에 ICCP 프로토콜이 가지고 있는 보안요소인 접근제어를 피해 갈 수 있다.
○ 허가되지 않은 유저가 잘못된 정보를 EMS에 전송할 경우 문제가 생길 수 있다. 잘못된 정보를 이용하여 중앙 EMS가 잘못된 제어명령을 내리도록 유도할 수 있다.
○ 인증되지 않은 사용자가 데이터 혹은 소프트웨어의 접근이 가능할 수 있다. 제어센터의 여러 요소는 물리적 보안 혹은 사이버 보안이 적용되어 있으며 인증을 필요로 하지만, ICCP 프로토콜은 접근제어 테이블이 보안요소의 전부이기 때문에 인증 없이 접근할 수 있는 경로가 될 수 있다.
○ 직원의 실수로 인해 시스템 운영과 네트워크의 안정성이 문제가 될 수 있다. 가령 데이터를 잘못 입력하거나, 잘못된 명령을 입력한 경우 시스템이 잘못된 정보를 수행하기 때문에 문제가 생길 수 있다.

최근 새롭게 밝혀진 ICCP 프로토콜의 취약점은 존재하지 않지만 2007년 이전에는 ICCP 벤더들의 취약점이 보고되었다. [표 2]에 언급된 취약점들은 보고된 ICCP 제품들의 취약점으로 모두 제품들의 프로토콜 스택에 관련된 것으로 하위 계층에서 일어난 문제점들이다.

[표 2]에서 기술된 취약점 이외에도 ICCP는 암호화되지 않은 메시지를 그대로 전송하기 때문에 정보 유출 및 위/변조에 대한 위험이 존재한다. 또한 TPKT 프로토콜과 COTP프로토콜의 경우 일반적인 상황에서는 많이 사용되고 있지 않기 때문에 현재까지 발견되지 않은 취약점들의 존재 가능성도 배제할 수 없다.[7]

취약성 검사 도구인 Nessus의 SCADA plug-in에서는 ICCP 사용 자체를 시스템 취약점으로 평가하고 있을 만큼 ICCP 프로토콜은 보안에 취약하다.

## Ⅳ. 대응 현황

본 장에서는 앞서 살펴본 취약점들에 대한 대응방안인 Secure ICCP에 대해 살펴본다. 또한 Secure ICCP 표준과 각 기관에서 제공하는 가이드라인에 대해 다루고 여전히 해결되지 않은 이슈들에 대해 다룬다.

### 4.1. Secure ICCP 개요

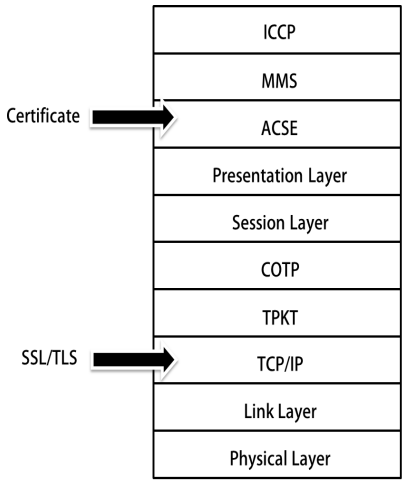
ICCP 프로토콜의 취약성에 대해서는 2000년대 초반부터 논의되었다. 이러한 문제점의 해결을 위해 등장한 것이 Secure ICCP이다. Secure ICCP는 TLS(Transport Layer Security)를 사용하여 암호화 기능을 제공한다. 이를 통해 데이터 유출, 위/변조 등과 같은 위협에 효과적인 대응할 수 있다. 또한 ACSE에 인증서를 이용한

〔표 2〕 보고된 ICCP 취약점〔8〕

| CVE Number | CVSS | 내용 |
|---|---|---|
| CVE-2005-4812 | 7.8 | SISCO OSI 스택이 특정 네트워크 트래픽에 DoS(process crash)를 유발 |
| CVE-2006-0059 | 7.5 | LiveData ICCP 서버의 RFC 1006 부분이 Heap-based buffer overflow 유발 |
| CVE-2006-6489 | 5.0 | SISCO OSI스택이 잘못된 패킷에 DoS(애플리케이션 종료 및 재부팅) 유발 |

인증을 사용하여 정상적이지 않은 대상이 해당 서버에 접속하는 것을 막는다.[9] [그림 2]는 ICCP의 프로토콜 스택에 위에 언급한 보안 기능을 추가한 Secure ICCP를 나타낸 것이다.

현재 SISCO, Simens, LiveData, ACS등 여러 업체에서 Secure ICCP 제품들을 출시하고 있지만, 각기 다른 보안 수준을 제공하고 있다. 이는 Secure ICCP 표준에서 세부적인 보안 기능에 대해 서술하고 있지 않아 암호화 알고리즘, 키 길이 등을 각 업체에서 자율적으로 선택하고 있기 때문에 생겨난 문제점이다. 일례로 Sisco 社의 ICCP Lite PLUS+의 경우 1024 bits의 공개키를 사용하고 있지만 Siemens 社의 ICCP NT의 경우 2048 bit 길이의 키를 사용하고 있다. 하나의 제품이 높은 수준의 보안을 가지고 있어도 통신대상이 낮은 수준의 보안 기능만을 제공할 경우 해당 통신 구간은 높은 수준의 보안이 불가능하다. 따라서 여러 국가와 단체들은 일정 수준이상의 보안을 제공하기 위해 가이드라인들을 제작하여 배포하고 있다.




〔그림 2〕 Secure ICCP protocol stack

### 4.2. 표준 및 가이드라인

전력시스템에서 사용되는 프로토콜들의 보안권고사항은 IEC 62351에 서술되어 있다. 표준은 총 9개의 파트로 구성되어 있으며 ICCP에 적용 가능한 보안 권고사항은 파트 3과 4에 존재한다. 파트 3은 TCP/IP를 사용하는 프로토콜들에 대한 보안권고사항으로 TLS의 사용을 권고하고 있다.[10] 파트 4의 경우 MMS를 사용하는 프로토콜들에 대한 보안권고사항으로 ACSE에서 인증서를 이용하는 인증을 권고하고 있다.

ICCP에 보안을 적용하기 위한 노력은 여러 단체들도 진행하고 있다. 대표적으로 EPRI는 2000년대 초 부터 ICCP 프로토콜의 취약성에 대한 보고서를 발행하였다. 2010년에는 Secure ICCP의 표준의 허점인 전자 인증서 관리와 관련된 문서를 발행하였고, 2012년에는 “Secure ICCP Implementation Guide”를 출간하였다.

국가적으로 Secure ICCP에 대한 가이드라인도 발행되고 있는데 대표적으로 뉴질랜드와 미국이 해당 문서를 웹에서 발행하고 있다. 미국 에너지부는 Secure ICCP의 동작과 구현에 발생할 수 있는 이슈들과 보안 권고사항을 다룬 “Secure ICCP Integration Considerations and Recommendations”를 발행하였다. 뉴질랜드의 경우 국가 전력회사인 Transposer 社에서 Secure ICCP를 소개하는 “Secure ICCP Customer Implementation Guide”를 출간하였다.

## Ⅴ. 잠재적인 보안 이슈

Secure ICCP는 ICCP 프로토콜에 존재하지 않던 인증 및 암호화를 추가하였다. 이를 통해 충분한 보안기능이 적용 된 것으로 보이지만 Secure ICCP는 몇 가지 잠재적인 문제점들을 가지고 있다. 본 장에서 ICCP의 보안권고사항을 담은 IEC 62351을 토대로 한 Secure ICCP에 잠재된 보안 이슈에 대해 다룬다.

### 5.1. 오래된 기술의 사용

현재 출간된 IEC 62351 문서들은 TLS 1.0 버전에 관한 내용을 다루는 RFC 2246을 참고하고 있다. TLS 1.0은 2012년에 CBC모드 기반 공격의 한 예인 BEAST(Browser Exploit Against SSL/TLSS) 공격 등 여러 취약점들이 발견되어 NIST에서 철회되었다. NIST는 이와 동시에 내년부터는 TLS 1.2 이상 버전을 사용할 것을 권고하고 있지만 해당 내용은 표준에는 반영이 되고 있지 않기 때문에 안전하지 않은 보안기술을 사용함으로써 생기는 보안사고가 발생할 수 있다.

이러한 문제는 공개키 암호화 알고리즘 및 해시함수에서도 나타난다. CA/Browser Forum에서는 올해부터

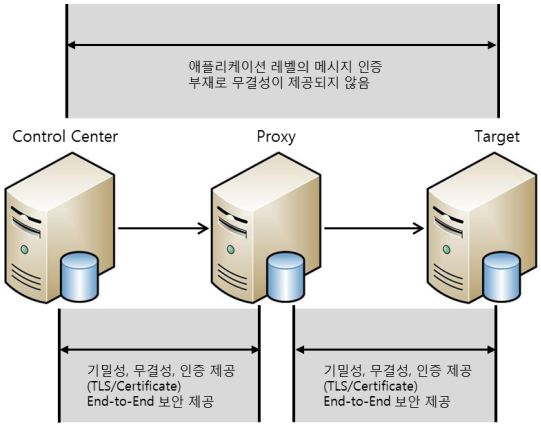
해시함수는 SHA-1, SHA-256, SHA-384, SHA-512를 사용할 것을 권고하고 있다. 또한 공개키 알고리즘으로 RSA 사용 시 RSA 계수의 크기를 기존 1024 bits에서 2048bits로 늘릴 것을 권장한다.[11] 이렇듯 보안과 관련된 기술들은 빠르게 변화하고 있지만 표준에서는 변동사항을 제시간 내에 수용하고 있지 못하다.

### 5.2. 표준에 존재하는 허점

인증서와 관련된 IEC 62351-4는 인증서 관리 및 갱신, 인증서 분배 등 인증서에 대한 규정이 미흡하다.[12] EPRI에서 2008년과 2010년에 이와 관련된 내용에 대한 보고서를 출간하였으나 해당 내용은 아직 표준에 추가되지 않았다. IEC 62351의 파트 3과 4의 경우 올해 초에 새로운 에디션이 출간될 예정이었으나 예상보다 출간일이 늦어져 위의 문제점들의 수정이 늦춰지고 있다.

또한 [그림 3]과 같이 프록시 서버를 사용한 통신을 할 경우 IEC 62351은 애플리케이션 레벨에서의 메시지 인증이 없기 때문에 End-to-End 보안에 허점이 생길 수 있다.[13] 제어센터와 프록시, 프록시와 통신대상 사이에는 TLS와 인증서를 통해 기밀성, 무결성, 인증이 모두 보장되지만 제어센터와 통신대상 사이에는 무결성이 보장되지 않아 End-to-End 보안이 재대로 이루어지지 못한다.

언급한 문제점 이 외에도 통신 구간의 추가로 인한 문제점이 발생 할 수 있다. 기존에 사용되던 EMS - SCADA구간은 이미 많은 연구가 이루어지고 있지만, 앞으로 추가될 MOS와 EMS의 통신의 경우 새로운 종류의 문제점이 발생할 수 있다.




〔그림 3〕 Proxy 사용 시 통신

## Ⅵ. 결 론

전력시스템 제어센터에서 사용되는 ICCP 프로토콜은 접근제어 테이블을 기반으로 하는 보안 기능 외에 부가적인 보안기능을 지원하지 않고 있다. 따라서 ICCP 프로토콜이 TLS와 같은 TCP 계층 보안 프로토콜과 함께 사용되지 않는 경우 단순한 위/변조 공격이나, 정상적이지 않은 대상이 해당 서버에 접속하는 것과 같은 공격들에 취약성을 가지게 된다. 이러한 보안 취약성들을 해결하기 위한 방안으로 TLS를 적용하고, ACSE에서 인증서 기반의 인증을 진행하는 Secure ICCP가 고려되고 이미 일부 활용되고 있다. 또한 IEC에서 발행한 보안관련 표준들 중 ICCP에 적용되는 부분들은 업계 활용 기술들을 기반으로 새롭게 표준화가 진행 중이고, 여러 업체와 관련 기관에서 ICCP의 보안성을 향상시킬 수 있는 TLS기반의 기술 문서들을 제공하고 있다. 하지만 기존 Secure ICCP 는 최근의 급변하는 사이버 공격에 대비하기에는 적절한 수준의 보안 기능을 제공하지 못하고 있고, 또한 인증서 관리와 같은 표준에서 언급하지 않는 부분에 대한 고려도 부족한 실정이다. 따라서 전력시스템 전반을 고려하고 제어센터 간 통신의 보안 중요성을 고려한 보다 체계적인 전력시스템의 제어 센터 간 보안 연구가 필요하다.

## 참 고 문 헌

[1] IEEE, IEEE-SA Technical Report on Utility Communications Architecture (UCA) Version 2.0, 1999.

[2] R. Mackiewicz, IEC Standards Status, http://www.emmos.org/prevconf/2012/6.Current%20Status%20of%20ICCP-TASE.2,%20Secure%20ICCP,%20and%20Other%20IEC%20Standards.pdf.

[3] IEC TC57, IEC 60870-6-503, Telecontrol protocols compatible with ISO standards and ITU-T recommendations – TASE.2 Service and protocol, 2008.

[4] IEC TC57, IEC 60870-6-505, Telecontrol equipment and systems - Part 6-505: Telecontrol proto-

cols compatible with ISO standards and ITU-T recommendations - TASE.2 User guide, 2006.

[5] C.A.S. da cunha Jr., O.Rein Jr., J.A. Jardini, L. C. Magrini, Electrical utilities control center data exchange with ICCP and CIM/XML, *2004 IEEE/PES*, pp.260-265, 2004.

[6] EPRI, Inter-Control Center Communications Protols (ICCP, TASE.2): Threats to Data Security and Potential Solutions, 2001.

[7] Matthew F., ICCP Exposed: Accessing the attack surface of the utility stack, *Proceeding of SCADA Security Scientific Symposium*, 2007.

[8] National Vulnerability Database, nvd.nist.gov

[9] John T. Michalski, Andrw L., Jason T., Sammy S., Secure ICCP Integration Considerations and Recommendations, 2007.

[10] IEC TC 57, IEC/TS 62351-3, Power systems management and associated information exchange - Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP, 2007.

[11] CA/Broswer Forum, Baseline Requirements for the issuance and management of publicly-trusted certificates, v.1.1.9, 2014.

[12] EPRI, Secure Inter Control Center Protocol Digital Certificate management, 2010.

[13] Fries, S., Hof, H. J., Seewald, M., Enhancing IEC 62351 to improve security for energy automation in smart grid environments, *Internet and Web Applications and Services (ICIW), 2010 Fifth International Conference on, IEEE*, 2010.

## 〈저자소개〉

**김 성 진 (SungJin Kim)**
비회원

2014년 2월 : 아주대학교 정보컴퓨터공학과 졸업
2014년 3월~현재 : 아주대학교 컴퓨터공학과 석사과정
<관심분야> 전력제어시스템 보안, 비정상행위탐지

**손 태 식 (Taeshik Shon)**
정회원

2000년 2월 : 아주대학교 정보컴퓨터공학부 졸업
2002년 2월 : 아주대학교 정보통신공학과 공학석사
2005년 8월 : 고려대학교 정보보호학과 공학박사
2004년 2월~2005년 2월 : Research Scholar, University of Minnesota
2005년 8월~2011년 2월 : 삼성전자 DMC 연구소 책임연구원
2011년 3월~현재 : 아주대학교 정보컴퓨터공학과 조교수
<관심분야> 전력제어시스템 보안, 디지털 포렌식, 비정상행위탐지, 융합보안