스마트그리드 환경에서 ICCP 통신 취약점 및 보안기술 동향 연구

김성진, 손태식
아주대학교 컴퓨터공학과
e-mail: ksjskyblue@ajou.ac.kr, tsshon@ajou.ac.kr

A study on Trend of ICCP Communication Vulnerability and Security Technology in SmartGrid Environment

SungJin Kim, Taseshik Shon
Dept of Computer Engineering, AJOU University

요 약

스마트그리드에서 가장 중요한 것 중 하나로 제어센터를 뽑을 수 있다. 이러한 제어센터에서 사용되는 대표적인 프로토콜은 ICCP가 있다. ICCP는 제어센터 사이의 데이터 통신에 적합한 프로토콜로써 전력망 전체의 정보들을 다룰 수 있도록 설계되었다. 하지만 해당 프로토콜은 데이터에 대한 접근제어만을 보안요소로 가지고 있기 때문에 매우 취약한 프로토콜이다. 일반적인 ICCP는 보안이 취약하기 때문에 실제 제품들 중 일부는 Secure ICCP를 제공한다. Secure ICCP는 ICCP가 가지고 있는 보안위협에 대한 대응책으로 암호화와 인증을 제공한다. 하지만 Secure ICCP는 한계점이 존재하고, 실제 대부분의 ICCP 서버에서는 기존 ICCP만 사용하고 않기 때문에 전력제어센터 사이에 주고받는 데이터는 여전히 취약하다. 따라서 ICCP 서버에서 Secure ICCP의 사용을 권장하고, Secure ICCP가 해결하지 못하는 문제점에 대한 연구가 추가적으로 필요하다.

1. 서론

최근 전력망에 IT기술을 접목시킨 스마트그리드에 관한 연구가 활발하게 진행되고 있다. 스마트그리드에서 다양한 전력망의 정보들은 제어센터들로 들어간다. 제어센터는 이러한 정보들을 바탕으로 전력망을 모니터링하고 제어하는 역할을 한다. 따라서 제어센터는 스마트그리드의 중요한 부분이 되었고 그로 인해 기존보다 높은 레벨의 보안이 필요하게 되었다. 제어센터는 여러 프로토콜을 사용하지만 가장 대표적으로 사용되는 프로토콜이 ICCP(Inter Control-Centre Communication Protocol)이다. ICCP는 전력 제어센터간 통신에 사용하는 프로토콜로 여러 종류의 데이터 통신에 적합하다. 본 논문에서는 ICCP를 보안의 관점에서 살펴보고, 존재하는 보안 위협에 대해 다룬다.

2. ICCP 특징 및 보안 취약점

위에 언급한 것과 같이 제어센터는 스마트그리드 시스템에서 주요 역할을 하는 요소이다. 제어센터는 전력망 전반에 관련된 정보를 전달 받고, 그 상황에 따라 적절한 명령을 내려 전력망을 안전한 상태로 유지 하는 역할을 한다. 이러한 전력 제어센터들 사이 통신에 사용하는 프로토콜이 ICCP이다. 따라서 ICCP는 전력망과 관련된 모든 데이터 교환(실시간 모니터링 정보, 실시간 제어 명령, 회계 자료, 측정 값 등)에 사용 할 수 있다.

2.1 관련 표준

1990년대 EPRI(Electric Power Research institute)의 주도하에 ICCP는 전력시스템에 사용되도록 설계되었다. 이후 1997년 IEC 60870-6의 503과 802파트, 그리고 그 다음해인 1998년에는 702파트가 IEC 표준이 되었다. 추가로 2002년에 유저 가이드인 505파트가 추가되었고 503과 802 파트는 다음 에디션2가 출간되었다. 현재 유저 가이드를 제외한 세 표준은 2014년에 새로운 에디션이 나올 예정이다. 다음 표는 각 다음과 같은 정보를 다루고 있다.

<표 1> IEC Standard for ICCP

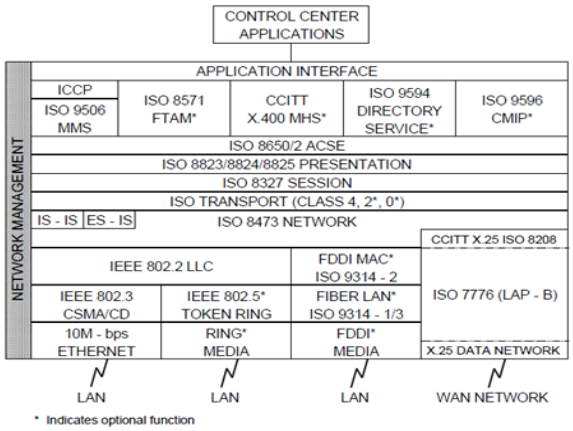
IEC 60870-6-503	서비스와 프로토콜
IEC 60870-6-505	유저 가이드
IEC 60870-6-702	어플리케이션 서비스
IEC 60870-6-802	객체 모델

본 연구는 2013년도 산업통상자원부의 재원으로 한국에너지기술평가원 (KETEP)의 지원을 받아 수행한 연구과제입니다. (No. 20131020402090)

2.2 ICCP 특징

표준에 따르면 ICCP는 OSI 7Layer의 어플리케이션 계층에서 동작한다. 그 하단에는 MMS(Manufacturing Message Specification)와 ACSE(Association Control Service Element)를 필요로 한다. ICCP의 서비스는 그 하단의 MMS의 서비스로 매핑된다. 따라서 MMS가 서버-클라이언트 모델을 사용하기 때문에 ICCP 또한 서버-클라이언트 모델을 사용하여 통신한다. 이처럼 MMS의 통신을 이용하기 때문에 ICCP는 상호 운용성, 통합의 편리성 등 MMS의 장점을 얻을 수 있다. 그 하단에 존재하는 ACSE의 경우 하나의 클라이언트와 여러 서버들 간에 다중 연결을 위해 사용된다. 이를 통해 전송되는 데이터의 중요도에 따라 다른 서비스 품질을 적용할 수 있다.

TCP/IP 스택에서 OSI 7계층구조에서 사용해야하는 ICCP를 사용하기 위해 ICCP는 하위에 COTP와 TPKT 두 계층을 추가하여 사용한다. COTP는 TCP와 기능이 거의 유사하지만 TCP는 스트림 기반의 통신을 제공하는 반면 COTP는 패킷 기반의 통신을 제공한다. TPKT의 경우 TCP/IP 스택 위에서 COTP를 사용하기 위해 사용된다. 이 두 프로토콜을 이용하여 현재 사용되고 있는 TCP/IP 스택위에서도 ICCP프로토콜은 동작 할 수 있다.



(그림 1) ICCP Stack[2)]

ICCP는 Object Oriented Methodology를 사용한다. 따라서 클래스를 정의하고 클래스의 Attributes와 Methods를 이용해 서비스를 제공한다. 이러한 클래스는 Bilateral Table을 통해 접근제어를 한다. 이 테이블은 서버에 존재하는 정보들에 대해 '실행', '읽기와 쓰기', '읽기', 혹은 '접근불가' 네 가지 종류의 설정이 가능하다. ICCP에서는 각 클라이언트마다 접근권한을 다르게 설정 가능하기 때문에 클라이언트별로 차별화된 접근제어도 가능하다. 또한 ICCP 통신 연결 도중 정책의 변경으로 인해 다른 내용의 접근제어가 필요한 경우 서버에서 테이블을 변경하여 클라이언트에게 전송해주는 것만으로 접근제어의 변경이 가능하다.

클래스의 Method중 가장 기본적인 것은 ICCP서버 클래스에 있는 클라이언트에서 서버로 요청하는 Operation(운영)과 운영과는 달리 서버 측에서 시작하는 Action(동작)이 있다. Operation은 클라이언트에서 서버의 ICCP 버전을 요청하는 것과 같은 데이터 통신을 의미하고, Action(동작)은 어떠한 이벤트의 발생으로 인한 서버에서 클라이언트로 보고하는 것과 같은 데이터 통신을 뜻한다.

또 다른 특징으로는 Conformance Block이 있다. 이것은 특정 역할을 하는 서버를 만들기 위해 TASE2 클래스를 그룹핑한 것이다. 첫 번째 블록은 통신연결과 관련된 기본 서비스에 관련된 내용을 다루고 있기 때문에 ICCP 서버는 모두 최소한 블록 1(Basic Service)을 지원해야한다. 현재 블록 6(Programs), 블록 7(Event), 블록 8(Account), 그리고 블록 9(Time Series)의 경우 사용되고 있지 않다. 현재 진행 중인 다음 표준은 해당 블록을 의미있게 만들기 위해 Conformance Block을 변경 중이다.

<표 2> 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
Block 7	Event
Block 8	Accounts
Block 9	Time Series

2.3 ICCP 보안 취약점

이와 같이 여러 종류의 데이터를 다루고, 많은 서비스를 제공 하는 ICCP는 그 기능에 비해 초라한 보안요소들을 가지고 있다. 앞서 언급한 Bilateral Table을 이용한 접근제어가 전부라고 할 정도로 보안기능이 제공되어 있지 않아 다양한 보안 위협을 가지고 있다. 특히 데이터 위/변조, 데이터 유출과 같은 문제에 대한 대응책이 전혀 없다.

이 외에도 TCP/IP 스택위에서 ICCP을 구현할 때 생길 수 있는 문제점도 존재한다. 앞서 언급한 COTP와 TPKT의 보안 취약점은 곧 ICCP의 보안 취약점이 된다. 2007년 M. Franz는 ICCP 하위 프로토콜의 취약점으로 인한 ICCP 취약점에 관한 논문을 발표하였다.[3] 이 논문에서 소개된 두 개의 취약점(CVE-2006-0059, CVE-2005-4812)

1) Matthew Franz, ICCP Exposed : Assessing the Attack Surface of the "Utility Stack", 2007

은 실제 ICCP서버 장치에 퍼징기법을 적용하여 찾아낸 취약점이다.[3] 이처럼 표준에서는 찾아 낼 수 없는 취약점이 존재하기 때문에 실제 ICCP제품은 많은 취약점을 가지고 있다고 볼 수 있다. ICCP 제품들의 취약점이 대규모 정전과 같은 사회 전반에 문제를 야기할 수 있기 때문에 강력한 보안 대책이 필요하다.

3. ICCP 보안 기술 동향

다행히 ICCP 제품들을 제조하는 산업계에서는 위의 보안 위협들을 이전부터 인지하고 있었다. ICCP가 표준으로 출간되기 전인 1997년부터 Secure ICCP가 사용가능하였다. 또 비교적 최근에 표준이 된 IEC/TS 62541의 파트 3과 4에는 TCP/IP 보안에 관련된 내용과 MMS 보안 내용이 포함되는 등 ICCP에 적용 가능한 보안에 관한 연구가 진행되고 있다.

3.1 Secure ICCP

앞서 언급한 데이터의 위/변조 혹은 데이터 유출과 같은 보안 위협에 대한 대응책으로 Secure ICCP에서 제공하는 보안 기술은 SSL/TLS, 공개키를 이용한 키 교환, 그리고 어플리케이션 계층에서의 인증이 있다. 출시되는 모든 제품들이 세 기술을 모두 적용한 것이 아니기 때문에 일반적으로 지원하는 내용에 대해 다룬다.

<표 3> Secure ICCP Stack

7	ICCP(TASE.2)
	MMS
	ACSE(Certificate)
6	Presentation
5	Session
4	Transport(SSL/TLS)
3	Network
2	Data Link
1	Physical

앞서 언급한 데이터의 위/변조 혹은 데이터 유출과 같은 보안 위협에 대한 대응책으로 Secure ICCP는 SSL/TLS를 사용하여 암호화를 제공한다. SSL/TLS는 대칭키 알고리즘을 사용하여 상위 계층들의 정보를 암호화한다. 암호화된 패킷은 키를 알고 있는 수신자만 복호화할 수 있기 때문에 정상적인 수신자만이 키를 가지고 있는 경우 송신자와 수신자 사이 안전한 채널을 형성할 수 있게 된다. 이러한 채널을 형성하기 위해서는 수신자가 키를 알고 있어야 한다는 제약사항이 존재하기 때문에 키 교환에 대한 문제점이 존재한다. 만약 공격자가 사용된 키를 알게 되면 이를 이용해 복호화가 가능해 지기 때문에 안전한 키 교환이 SSL/TLS에서는 필수적이다.

이러한 키 교환을 위한 방안으로 공개키-개인키를 사용한다. 개인키로 암호화 한 정보는 공개키로 복화화 할 수 있기 때문에 키 교환과정에서 사용된다. A와 B사이 공개키와 개인키를 이용한 키 교환 과정을 살펴보면 다음과 같다. 공개키는 이름처럼 외부에 공개되어있기 때문에 A는 B의 공개키를 이용하여 키를 암호화하여 전송한다. 개인키는 B만 소유하고 있기 때문에 키는 B만이 복호화 할 수 있다. 이러한 방식을 이용하여 키 교환을 성공적으로 이루었다면 이후 A와 B는 SSL/TLS를 이용한 안전한 통신 채널을 형성하여 통신이 가능하게 된다. 현재 Secure ICCP제품에서는 1024비트의 비대칭 키가 주로 사용되고 일부에서는 2048비트의 비대칭 키를 사용한다.

정상적인 제어센터인지 파악하기 위한 인증서가 마지막으로 추가된다. 정상적이지 않은 제어센터와 통신 채널을 형성하게 될 경우 통신채널의 안전성과는 관련 없이 정보의 유출 혹은 잘못된 정보를 받아들일 위험이 있다. 이 문제를 해결하기 위해 X.509를 적용한 인증서 기반의 인증을 Secure ICCP는 제공한다.

3.2 실제 Secure ICCP 제품의 문제점

Secure ICCP는 이처럼 보안요소들을 ICCP에 추가하였다. 하지만 이러한 내용을 추가하였다고 하여도 제어센터 사이의 데이터 교환이 안전하다고 할 수 없다. 위의 문제점 이외에도 2장에서 다룬 ICCP의 구현과정에서 사용되는 하위계층도 문제가 될 수 있다. COTP, TPKT와 같은 하위 계층의 보안 취약점은 Secure ICCP에서 예상하지 못한 보안 위협이 될 수 있다. 또한 키 관리의 어려움과 같은 적용된 보안기술이 가지고 있는 문제점도 존재한다.

실제 출시되는 ICCP 제품들의 경우 위에 언급한 Secure ICCP 전체를 지원하는 것이 아니라 일부를 지원하는 경우도 많고, Secure ICCP를 지원하지 않는 경우도 있다. 일부분만 Secure ICCP를 지원하는 경우 다른 보안요소들이 정상적으로 동작하여도 안전성을 보장 받을 수 없다. 예를 들어 SSL/TLS 만 지원하는 장치의 경우 인증을 거치지 않기 때문에 접속을 시도하는 대상이 정상적인 제어센터인지 판별이 불가능하다. 또한 적용하고 있는 보안기술이 구 버전의 보안기술일 경우 문제점이 있을 수 있다. 따라서 실제 ICCP를 사용한 통신 메시지들의 보안은 재대로 이루어지고 있지 않다고 볼 수 있다.

3.3 대응책과 보안기술 동향

ICCP의 보안에 관련된 IEC 62351이 존재하지만 Secure ICCP 제품들은 제품마다 조금씩 다른 보안기술을 적용중이다. 위에 언급한 세 가지 보안기술인 SSL/TLS, 인증서, 공개키-개인키를 ICCP에 적용하는 구체적인 표준을 제공하고 제품들이 해당 보안기술들을 적용하도록 하는 정책이 필요하다.

또한 적용하고 있는 보안기술을 최신기술로 변경하는

것도 필요하다. TLS 1.0 버전의 경우 중간자 공격(Man in the Middle Attack)에 취약한 모습을 보였다. 계속하여 TLS의 취약점이 발견되고 해당 버전에서 사용하는 알고리즘인 3DES, MD5은 더 이상 안전성을 보장할 수 없기 때문에 2013년 3월 철회되었다. 따라서 구 버전의 TLS를 사용하던 제품들은 TLS 1.2 버전으로 변경하여 사용하는 것이 권장된다.

인증의 경우 해당 인프라의 구축이 우선 필요하다. 일부 장치에서 해당 내용을 지원하다 하여도 해당 인프라의 부재 시 사용할 수 없기 때문에 인프라 구축이 필요하다. 또한 장치의 경우 인증서 규격에 관련된 X.509와 인증서 요청에 관련된 PKCS#10을 기반으로 하는 인증시스템을 구축하여야 한다.

그리고 하위 계층인 COTP와 TPKT의 경우 2006년 이후 새롭게 밝혀진 취약점은 존재하지 않는다. 그 당시 발견한 취약점은 퍼징기법을 Live Data의 ICCP장치에 적용하여 찾아낸 취약점이다. 하위 계층의 표준만으로는 파악하기 힘든 취약점이기 때문에 지속적인 확인이 필요하다.

4. 결론

현재 출시되는 많은 제품들이 Secure ICCP를 지원하고 있지만 정작 제어센터들은 보안이 추가되지 않은 기존 ICCP를 사용 하고 있다. 이러한 제어센터의 ICCP 통신의 경우 기본적인 보안조차 제공되고 있지 않기 때문에 위/변조, 데이터 유출과 관련된 문제에 직접적으로 노출되어 있다. Secure ICCP를 사용한다고 보안위협이 모두 사라지는 것은 아니지만, 기존의 ICCP에 비해 높은 수준의 보안을 제공하기 때문에 Secure ICCP를 사용하는 것을 권장한다. 제어센터는 여러 프로토콜을 사용하고 있기 때문에 타 프로토콜과의 연계 시 일어날 수 있는 보안상의 문제점이 존재할 수 있다. 이 부분에 관해서는 진행된 연구가 많지 않기 때문에 추가적인 연구가 필요하다. 향후 전력망은 지금 보다 더 밀접하게 IT기술과 융합하게 될 것이고, 그로 인해 제어센터는 더욱 많은 정보를 주고받게 될 것이다. 제어센터간의 정보교환에 일어나는 보안 사고는 사회 전반에 큰 영향을 미칠 수 있기 때문에 ICCP 프로토콜 보안에 관련된 연구가 지속적으로 필요할 것이다.

참고문헌

[1] Muhammad S. Malik "SECURITY ANALYSIS OF INTER CONTROL CENTER COMMUNICATION PROTOCOL USING MODEL CHECKING“ 2013

[2] da C Jr, C. A. S. “Electrical Utility Control Center Data Exchange with ICCP and CIM/XML” 2004 IEEE/PES. 2004

[3] Matthew F. “ICCP Exposed: Accessing the Attack Surface of the Utility Stack.” Proceedings of SCADA Security Scientific Symposium 2007

[4] John T. Michalski, Andrw L., Jason T., Sammy S. “Secure ICCP Integration Considerations and Recommendations” SANDIA report 2007

[5] IEC Std. 60870-6-503, "Telecontrol equipment and systems - Part 6-503: Telecontrol protocols compatible with ISO standards and ITU-T recommendations - TASE.2 Services and protocol". International Electro technical Commission, ed2. 2002

[6] IEC Std. 60870-6-505, "Telecontrol equipment and systems - Part 6-505: Telecontrol protocols compatible with ISO standards and ITU-T recommendations - TASE.2 User guide". International Electro technical Commission, ed1. 2002